111TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
111–493

GRID RELIABILITY AND INFRASTRUCTURE DEFENSE ACT

MAY 25, 2010.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. WAXMAN, from the Committee on Energy and Commerce, submitted the following

R E P O R T

[To accompany H.R. 5026]

[Including cost estimate of the Congressional Budget Office]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 5026) to amend the Federal Power Act to protect the bulk-power system and electric infrastructure critical to the defense of the United States from cybersecurity and other threats and vulnerabilities, having considered the same, report favorably thereon with amendments and recommend that the bill as amended do pass.

CONTENTS

89–006

AMENDMENT

The amendments are as follows:
Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Grid Reliability and Infrastructure Defense Act" or the "GRID Act".

SEC. 2. AMENDMENT TO THE FEDERAL POWER ACT.

(a) CRITICAL ELECTRIC INFRASTRUCTURE SECURITY.—Part II of the Federal Power Act (16 U.S.C. 824 et seq.) is amended by adding after section 215 the following new section:

"SEC. 215A. CRITICAL ELECTRIC INFRASTRUCTURE SECURITY.

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

"(1) BULK-POWER SYSTEM; ELECTRIC RELIABILITY ORGANIZATION; REGIONAL ENTITY.—The terms 'bulk-power system', 'Electric Reliability Organization', and 'regional entity' have the meanings given such terms in paragraphs (1), (2), and (7) of section 215(a), respectively.

"(2) DEFENSE CRITICAL ELECTRIC INFRASTRUCTURE.—The term 'defense critical electric infrastructure' means any infrastructure located in the United States (including the territories) used for the generation, transmission, or distribution of electric energy that—

"(A) is not part of the bulk-power system; and

"(B) serves a facility designated by the President pursuant to subsection (d)(1), but is not owned or operated by the owner or operator of such facility.

"(3) DEFENSE CRITICAL ELECTRIC INFRASTRUCTURE VULNERABILITY.—The term 'defense critical electric infrastructure vulnerability' means a weakness in defense critical electric infrastructure that, in the event of a malicious act using electronic communication or an electromagnetic pulse, would pose a substantial risk of disruption of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of defense critical electric infrastructure.

"(4) ELECTROMAGNETIC PULSE.—The term 'electromagnetic pulse' means 1 or more pulses of electromagnetic energy emitted by a device capable of disabling, disrupting, or destroying electronic equipment by means of such a pulse.

"(5) GEOMAGNETIC STORM.—The term 'geomagnetic storm' means a temporary disturbance of the Earth's magnetic field resulting from solar activity.

"(6) GRID SECURITY THREAT.—The term 'grid security threat' means a substantial likelihood of—

"(A)(i) a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of the bulk-power system or of defense critical electric infrastructure; and

"(ii) disruption of the operation of such devices or networks, with significant adverse effects on the reliability of the bulk-power system or of defense critical electric infrastructure, as a result of such act or event; or

"(B)(i) a direct physical attack on the bulk-power system or on defense critical electric infrastructure; and

"(ii) significant adverse effects on the reliability of the bulk-power system or of defense critical electric infrastructure as a result of such physical attack.

"(7) GRID SECURITY VULNERABILITY.—The term 'grid security vulnerability' means a weakness that, in the event of a malicious act using electronic communication or an electromagnetic pulse, would pose a substantial risk of disruption to the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of the bulk-power system.

"(8) LARGE TRANSFORMER.—The term 'large transformer' means an electric transformer that is part of the bulk-power system.

"(9) PROTECTED INFORMATION.—The term 'protected information' means information, other than classified national security information, designated as protected information by the Commission under subsection (e)(2)—

"(A) that was developed or submitted in connection with the implementation of this section;

"(B) that specifically discusses grid security threats, grid security vulnerabilities, defense critical electric infrastructure vulnerabilities, or plans, procedures, or measures to address such threats or vulnerabilities; and

"(C) the unauthorized disclosure of which could be used in a malicious manner to impair the reliability of the bulk-power system or of defense critical electric infrastructure.

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

"(11) SECURITY.—The definition of 'security' in section 3(16) shall not apply to the provisions in this section.

"(b) EMERGENCY RESPONSE MEASURES.—

"(1) AUTHORITY TO ADDRESS GRID SECURITY THREATS.—Whenever the President issues and provides to the Commission (either directly or through the Secretary) a written directive or determination identifying an imminent grid security threat, the Commission may, with or without notice, hearing, or report, issue such orders for emergency measures as are necessary in its judgment to protect the reliability of the bulk-power system or of defense critical electric infrastructure against such threat. As soon as practicable but not later than 180 days after the date of enactment of this section, the Commission shall, after notice and opportunity for comment, establish rules of procedure that ensure that such authority can be exercised expeditiously.

"(2) NOTIFICATION OF CONGRESS.—Whenever the President issues and provides to the Commission (either directly or through the Secretary) a written directive or determination under paragraph (1), the President (or the Secretary, as the case may be) shall promptly notify congressional committees of relevant jurisdiction, including the Committee on Energy and Commerce of the House of Representatives and the Committee on Energy and Natural Resources of the Senate, of the contents of, and justification for, such directive or determination.

"(3) CONSULTATION.—Before issuing an order for emergency measures under paragraph (1), the Commission shall, to the extent practicable in light of the nature of the grid security threat and the urgency of the need for such emergency measures, consult with appropriate governmental authorities in Canada and Mexico, entities described in paragraph (4), the Secretary, and other appropriate Federal agencies regarding implementation of such emergency measures.

"(4) APPLICATION.—An order for emergency measures under this subsection may apply to—

"(A) the Electric Reliability Organization;

"(B) a regional entity; or

"(C) any owner, user, or operator of the bulk-power system or of defense critical electric infrastructure within the United States.

"(5) DISCONTINUANCE.—The Commission shall issue an order discontinuing any emergency measures ordered under this subsection, effective not later than 30 days after the earliest of the following:

"(A) The date upon which the President issues and provides to the Commission (either directly or through the Secretary) a written directive or determination that the grid security threat identified under paragraph (1) no longer exists.

"(B) The date upon which the Commission issues a written determination that the emergency measures are no longer needed to address the grid security threat identified under paragraph (1), including by means of Commission approval of a reliability standard under section 215 that the Commission determines adequately addresses such threat.

"(C) The date that is 1 year after the issuance of an order under paragraph (1).

"(6) COST RECOVERY.—If the Commission determines that owners, operators, or users of the bulk-power system or of defense critical electric infrastructure have incurred substantial costs to comply with an order under this subsection and that such costs were prudently incurred and cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners, operators, or users, the Commission shall, after notice and an opportunity for comment, establish a mechanism that permits such owners, operators, or users to recover such costs.

"(c) MEASURES TO ADDRESS GRID SECURITY VULNERABILITIES.—

"(1) COMMISSION AUTHORITY.—If the Commission, in consultation with appropriate Federal agencies, identifies a grid security vulnerability that the Commission determines has not adequately been addressed through a reliability standard developed and approved under section 215, the Commission shall, after notice and opportunity for comment and after consultation with the Secretary, other appropriate Federal agencies, and appropriate governmental au-

thorities in Canada and Mexico, promulgate a rule or issue an order requiring implementation, by any owner, operator, or user of the bulk-power system in the United States, of measures to protect the bulk-power system against such vulnerability. Before promulgating a rule or issuing an order under this paragraph, the Commission shall, to the extent practicable in light of the urgency of the need for action to address the grid security vulnerability, request and consider recommendations from the Electric Reliability Organization regarding such rule or order. The Commission may establish an appropriate deadline for the submission of such recommendations.

"(2) CERTAIN EXISTING CYBERSECURITY VULNERABILITIES.—Not later than 180 days after the date of enactment of this section, the Commission shall, after notice and opportunity for comment and after consultation with the Secretary, other appropriate Federal agencies, and appropriate governmental authorities in Canada and Mexico, promulgate a rule or issue an order requiring the implementation, by any owner, user, or operator of the bulk-power system in the United States, of such measures as are necessary to protect the bulk-power system against the vulnerabilities identified in the June 21, 2007, communication to certain 'Electricity Sector Owners and Operators' from the North American Electric Reliability Corporation, acting in its capacity as the Electricity Sector Information and Analysis Center.

"(3) RESCISSION.—The Commission shall approve a reliability standard developed under section 215 that addresses a grid security vulnerability that is the subject of a rule or order under paragraph (1) or (2), unless the Commission determines that such reliability standard does not adequately protect against such vulnerability or otherwise does not satisfy the requirements of section 215. Upon such approval, the Commission shall rescind the rule promulgated or order issued under paragraph (1) or (2) addressing such vulnerability, effective upon the effective date of the newly approved reliability standard.

"(4) GEOMAGNETIC STORMS.—Not later than 1 year after the date of enactment of this section, the Commission shall, after notice and an opportunity for comment and after consultation with the Secretary and other appropriate Federal agencies, issue an order directing the Electric Reliability Organization to submit to the Commission for approval under section 215, not later than 1 year after the issuance of such order, reliability standards adequate to protect the bulk-power system from any reasonably foreseeable geomagnetic storm event. The Commission's order shall specify the nature and magnitude of the reasonably foreseeable events against which such standards must protect. Such standards shall appropriately balance the risks to the bulk-power system associated with such events, including any regional variation in such risks, and the costs of mitigating such risks.

"(5) LARGE TRANSFORMER AVAILABILITY.—Not later than 1 year after the date of enactment of this section, the Commission shall, after notice and an opportunity for comment and after consultation with the Secretary and other appropriate Federal agencies, issue an order directing the Electric Reliability Organization to submit to the Commission for approval under section 215, not later than 1 year after the issuance of such order, reliability standards addressing availability of large transformers. Such standards shall require entities that own or operate large transformers to ensure, individually or jointly, adequate availability of large transformers to promptly restore the reliable operation of the bulk-power system in the event that any such transformer is destroyed or disabled as a result of a reasonably foreseeable physical or other attack or geomagnetic storm event. The Commission's order shall specify the nature and magnitude of the reasonably foreseeable attacks or events that shall provide the basis for such standards. Such standards shall—

"(A) provide entities subject to the standards with the option of meeting such standards individually or jointly; and

"(B) appropriately balance the risks associated with a reasonably foreseeable attack or event, including any regional variation in such risks, and the costs of ensuring adequate availability of spare transformers.

"(d) CRITICAL DEFENSE FACILITIES.—

"(1) DESIGNATION.—Not later than 180 days after the date of enactment of this section, the President shall designate, in a written directive or determination provided to the Commission, facilities located in the United States (including the territories) that are—

"(A) critical to the defense of the United States; and

"(B) vulnerable to a disruption of the supply of electric energy provided to such facility by an external provider.

The number of facilities designated by such directive or determination shall not exceed 100. The President may periodically revise the list of designated fa-

cilities through a subsequent written directive or determination provided to the Commission, provided that the total number of designated facilities at any time shall not exceed 100.

"(2) COMMISSION AUTHORITY.—If the Commission identifies a defense critical electric infrastructure vulnerability that the Commission, in consultation with owners and operators of any facility or facilities designated by the President pursuant to paragraph (1), determines has not adequately been addressed through measures undertaken by owners or operators of defense critical electric infrastructure, the Commission shall, after notice and an opportunity for comment and after consultation with the Secretary and other appropriate Federal agencies, promulgate a rule or issue an order requiring implementation, by any owner or operator of defense critical electric infrastructure, of measures to protect the defense critical electric infrastructure against such vulnerability. The Commission shall exempt from any such rule or order any specific defense critical electric infrastructure that the Commission determines already has been adequately protected against the identified vulnerability. The Commission shall make any such determination in consultation with the owner or operator of the facility designated by the President pursuant to paragraph (1) that relies upon such defense critical electric infrastructure.

"(3) COST RECOVERY.—An owner or operator of defense critical electric infrastructure shall be required to take measures under paragraph (2) only to the extent that the owners or operators of a facility or facilities designated by the President pursuant to paragraph (1) that rely upon such infrastructure agree to bear the full incremental costs of compliance with a rule promulgated or order issued under paragraph (2).

"(e) PROTECTION OF INFORMATION.—

"(1) PROHIBITION OF PUBLIC DISCLOSURE OF PROTECTED INFORMATION.—Protected information—

"(A) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and

"(B) shall not be made available pursuant to any State, local, or tribal law requiring disclosure of information or records.

"(2) INFORMATION SHARING.—

"(A) IN GENERAL.—Consistent with the Controlled Unclassified Information framework established by the President, the Commission shall promulgate such regulations and issue such orders as necessary to designate protected information and to prohibit the unauthorized disclosure of such protected information.

"(B) SHARING OF PROTECTED INFORMATION.—The regulations promulgated and orders issued pursuant to subparagraph (A) shall provide standards for and facilitate the appropriate sharing of protected information with, between, and by Federal, State, local, and tribal authorities, the Electric Reliability Organization, regional entities, and owners, operators, and users of the bulk-power system in the United States and of defense critical electric infrastructure. In promulgating such regulations and issuing such orders, the Commission shall take account of the role of State commissions in reviewing the prudence and cost of investments within their respective jurisdictions. The Commission shall consult with appropriate Canadian and Mexican authorities to develop protocols for the sharing of protected information with, between, and by appropriate Canadian and Mexican authorities and owners, operators, and users of the bulk-power system outside the United States.

"(3) SUBMISSION OF INFORMATION TO CONGRESS.—Nothing in this section shall permit or authorize the withholding of information from Congress, any committee or subcommittee thereof, or the Comptroller General.

"(4) DISCLOSURE OF NON-PROTECTED INFORMATION.—In implementing this section, the Commission shall protect from disclosure only the minimum amount of information necessary to protect the reliability of the bulk-power system and of defense critical electric infrastructure. The Commission shall segregate protected information within documents and electronic communications, wherever feasible, to facilitate disclosure of information that is not designated as protected information.

"(5) DURATION OF DESIGNATION.—Information may not be designated as protected information for longer than 5 years, unless specifically redesignated by the Commission.

"(6) REMOVAL OF DESIGNATION.—The Commission may remove the designation of protected information, in whole or in part, from a document or electronic communication if the unauthorized disclosure of such information could no longer

be used to impair the reliability of the bulk-power system or of defense critical electric infrastructure.

"(7) JUDICIAL REVIEW OF DESIGNATIONS.—Notwithstanding subsection (f) of this section or section 313, a person or entity may seek judicial review of a determination by the Commission concerning the designation of protected information under this subsection exclusively in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in the District of Columbia. In such a case the court shall determine the matter de novo, and may examine the contents of documents or electronic communications designated as protected information in camera to determine whether such documents or any part thereof were improperly designated as protected information. The burden is on the Commission to sustain its designation.

"(f) JUDICIAL REVIEW.—The Commission shall act expeditiously to resolve all applications for rehearing of orders issued pursuant to this section that are filed under section 313(a). Any party seeking judicial review pursuant to section 313 of an order issued under this section may obtain such review only in the United States Court of Appeals for the District of Columbia Circuit.

"(g) PROVISION OF ASSISTANCE TO INDUSTRY IN MEETING GRID SECURITY PROTECTION NEEDS.—

"(1) EXPERTISE AND RESOURCES.—The Secretary shall establish a program, in consultation with other appropriate Federal agencies, to develop technical expertise in the protection of systems for the generation, transmission, and distribution of electric energy against geomagnetic storms or malicious acts using electronic communications or electromagnetic pulse that would pose a substantial risk of disruption to the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of such systems. Such program shall include the identification and development of appropriate technical and electronic resources, including hardware, software, and system equipment.

"(2) SHARING EXPERTISE.—As appropriate, the Secretary shall offer to share technical expertise developed under the program under paragraph (1), through consultation and assistance, with owners, operators, or users of systems for the generation, transmission, or distribution of electric energy located in the United States and with State commissions. In offering such support, the Secretary shall assign higher priority to systems serving facilities designated by the President pursuant to subsection (d)(1) and other critical-infrastructure facilities, which the Secretary shall identify in consultation with the Commission and other appropriate Federal agencies.

"(3) SECURITY CLEARANCES AND COMMUNICATION.—The Secretary shall facilitate and, to the extent practicable, expedite the acquisition of adequate security clearances by key personnel of any entity subject to the requirements of this section to enable optimum communication with Federal agencies regarding grid security threats, grid security vulnerabilities, and defense critical electric infrastructure vulnerabilities. The Secretary, the Commission, and other appropriate Federal agencies shall, to the extent practicable and consistent with their obligations to protect classified and protected information, share timely actionable information regarding grid security threats, grid security vulnerabilities, and defense critical electric infrastructure vulnerabilities with appropriate key personnel of owners, operators, and users of the bulk-power system and of defense critical electric infrastructure.".

(b) CONFORMING AMENDMENTS.—

(1) JURISDICTION.—Section 201(b)(2) of the Federal Power Act (16 U.S.C. 824(b)(2)) is amended by inserting "215A," after "215," each place it appears.

(2) PUBLIC UTILITY.—Section 201(e) of the Federal Power Act (16 U.S.C. 824(e)) is amended by inserting "215A," after "215,".

Amend the title so as to read:

A bill 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.

PURPOSE AND SUMMARY

H.R. 5026, the Grid Reliability and Infrastructure Defense Act, or "GRID Act", was introduced by Reps. Edward J. Markey (D–MA) and Fred Upton (R–MI) on April 14, 2010. The purpose of H.R. 5026 is to provide the Federal Energy Regulatory Commission with

new authorities under the Federal Power Act to protect the electric grid against cybersecurity and other threats and vulnerabilities.

BACKGROUND AND NEED FOR LEGISLATION

The U.S. electric grid consists of interconnected transmission lines, local distribution systems to deliver electricity to end-users, generation facilities, and related communications systems. The bulk-power system in the United States and Canada has more than 200,000 miles of transmission lines, has more than 800,000 megawatts of generating capacity, is valued at over $1 trillion, and serves more than 300 million people.[1] The components of the grid are highly interdependent, such that a line outage or system condition problems in one area can lead to reliability concerns in other areas. In addition, the operations controls over the transmission grid and generators are increasingly managed by computer systems (notably Supervisory Control and Data Acquisition, or SCADA, systems) linked to the Internet or other communications systems and to each other. The grid's increasing reliance on automation and two-way communications increases its vulnerability to remote cyber attacks.

Public reports relating to cyber vulnerabilities of and threats to the electric grid have increased in recent years and have been the subject of several hearings in the 110th and 111th Congresses. Especially noteworthy are reports on what is known as the "Aurora" vulnerability. In 2006, the Department of Homeland Security's Control Systems Security Program conducted an analysis—performed by the Department of Energy's Idaho National Laboratory—that came to be known as Aurora. This analysis demonstrated that an attacker could hack into the control system of an electric generator or other rotating equipment connected to the grid and throw the equipment out of phase, causing severe physical damage to the equipment.

In addition, it has been reported that actors based in China, Russia, and other nations have conducted cyber "probes" of U.S. grid systems, and that cyber attacks have been conducted against critical infrastructure in other countries. Cyber attacks may create instant effects at very low cost, and are very difficult to positively attribute back to the attacker. These features could make such attacks attractive not only for criminal purposes, but also as a possible element of future national hostilities.[2] Utilization of cyber attacks on civilian critical infrastructure has reportedly become an important element of Chinese military strategy.[3]

There also has been growing attention to physical vulnerabilities of the grid. For example, large transformers essential to the reliable operation of the grid are manufactured outside of the United States and replacement may require two years or longer. A limited number of spare, large transformers are available within the United States, and industry has developed a voluntary program

---

[1] U.S. Government Accountability Office, Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain, at 22 (Oct. 2007) (GAO–07–1036).

[2] U.S. Government Accountability Office, Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats, at 4, Table 1 (Nov. 17, 2009) (GAO–10–230T).

[3] Bryan Krekel et al., *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* prepared by Northrop Grumman Corporation for The US-China Economic and Security Review Commission, at 22–26 (Oct. 9, 2009).

(the spare transformer equipment program, or "STEP") providing for sharing of such assets in the event of a terrorist attack.

A special subset of physical vulnerabilities and threats is associated with electromagnetic pulse (EMP), of which there are three general categories: (1) geomagnetic storms resulting from solar activity; (2) intentional electromagnetic interference from portable equipment that uses high-power radio frequency or microwave or other electromagnetic pulses to destroy or temporarily disable electronic equipment; and (3) EMP caused by a high-altitude detonation of a nuclear weapon.

Solar coronal mass ejections emit electromagnetic particles that can disrupt the Earth's magnetic field. Such geomagnetic storms in turn can induce voltages in transmission lines, particularly in the northern-latitudes, which can damage electric transformers and other infrastructure. There are several historical examples of electric transformers being damaged or destroyed by geomagnetic storms, including the storms of 1859, 1921, and 1989. A recent National Academy of Sciences report estimated the effects of a geomagnetic storm of the magnitude of the 1921 storm on the current electrical grid, concluding that such a storm could cause permanent damage to more than 350 transformers, leaving as many as 130 million people without power. Impacts from a large geomagnetic storm could last for several years and cost in the range of several trillion dollars per year.[4]

Portable electromagnetic weapons can be used to disrupt or disable the control systems that operate the electric grid. Such weapons can vary in size from a hand-held device to a large vehicle-borne device, can be used at a distance from a target, and can penetrate walls or other obstacles—making detection and attribution of an attack to a specific source difficult. More than a dozen countries have conducted research on such weapons, and the Department of Defense (DOD) has demonstrated that such weapons can be developed with modest financial resources and technical capability. Such weapons have been used to defeat security systems, commit robberies, disable police communications, induce fires, and disrupt banking computers.[5]

In 2001, Congress established a commission to assess the threat of electromagnetic pulse from a high-altitude nuclear detonation, vulnerabilities of military and civilian infrastructure to such an attack, and the feasibility and cost of protecting such infrastructure. The commission issued a first report in 2004 and a second report in 2008. The 2004 report concluded that the risks from high-altitude EMP to the U.S. electric grid are substantial and recommended that measures be taken to protect high-value transmission assets that would require a long lead time to replace, key electric generation capability, and critical communication channels.[6]

---

[4] National Research Council, S*evere Space Weather Events—Understanding Societal and Economic Impacts,* Workshop Report, Committee on the Societal and Economic Impacts of Severe Space Weather Events: A Workshop, at 77–79 (2008).

[5] Technical Support Working Group and Directed Energy Technology Office, *The Threat of Radio Frequency Weapons to Critical Infrastructure Facilities,* at p. 1, 6–7 (Aug. 2005).

[6] Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Volume 1: Executive Report, at pp. 17–23 (2004).

The vulnerabilities of the electric grid present substantial risks to U.S. defense assets. A 2008 report by the Defense Science Board's Task Force on DOD Energy Strategy concluded that:

> critical missions . . . are almost entirely dependent on the national transmission grid. About 85% of the energy infrastructure upon which DoD depends is commercially owned, and 99% of the electric energy DoD installations consume originates outside the fence. . . . In most cases, neither the grid nor on-base backup power provides sufficient reliability to ensure continuity of critical national priority functions and oversight of strategic missions in the face of a long term (several months) outage.[7]

An October 2009 report by the Government Accountability Office concluded that of the Department of Defense's 34 most critical global assets, 31 of which rely on commercially operated electricity grids for their primary source of electricity.[8]

All of the threats to and vulnerabilities of the U.S. electric grid described above have been addressed in multiple hearings in the 110th and 111th Congresses, both in the Subcommittee on Energy and Environment of the Committee on Energy and Commerce, as well as in other committees. In addition, these threats and vulnerabilities were the subject of classified briefings on grid security, provided jointly by multiple federal agencies to the members of the Committee on Energy and Commerce, during both the 110th Congress and the 111th Congress.

Section 215 of the Federal Power Act, enacted as part of the Energy Policy Act of 2005, provides for the establishment of mandatory reliability standards for the bulk-power system, including standards addressing cybersecurity threats. Under section 215, the Federal Energy Regulatory Commission (FERC) has designated the North American Electric Reliability Corporation (NERC) as the electric reliability organization. NERC is responsible for proposing, for FERC review and approval, reliability standards to protect and enhance the reliability of the bulk-power system, including cybersecurity standards. NERC is a not-for-profit corporation, the principal members of which are owners, operators, and users of the bulk-power system. More than 1,800 different entities own or operate components of the bulk-power system that is subject to the NERC standard-setting process. NERC develops standards on an open basis through its standards committee, which is composed of member representatives. Approval of a reliability standard requires a quorum of 75% of the stakeholder ballot pool and support from a supermajority of at least two-thirds of the votes. The process of developing reliability standards is lengthy; for example, the critical infrastructure protection (CIP) standards approved by FERC in January 2008 took three years for NERC to develop. NERC procedures approved in February 2010 allow for an accelerated process

[7] Department of Defense, Report of the Defense Science Board Task Force on DoD Energy Strategy, More Fight—Less Fuel, at 18 (Feb. 2008).

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

for developing standards in case of a "national security emergency situation," but these procedures have not yet been used.[9]

The Canadian and Mexican electric grids are directly linked to the U.S. bulk-power system, and Canadian (and to a lesser extent Mexican) utilities participate in NERC and have agreed to be subject to NERC-adopted standards. They are not, however, subject to FERC jurisdiction.

Reliability standards developed by NERC and approved by FERC under section 215 apply to the users, owners, and operators of the bulk-power system and are mandatory and subject to enforcement by FERC with respect to U.S. entities. FERC cannot prescribe standards under section 215, but it has authority to direct NERC to develop standards or to modify existing standards. Importantly, the scope of these 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 normally serve critical defense facilities and other end-users of electricity. In addition, the provisions of section 215 do not apply to Alaska or Hawaii, where a number of important defense facilities are located.

To date, FERC has approved nine CIP reliability standards developed by NERC. With regard to cybersecurity, the CIP standards address critical cyber asset identification, security management controls, personnel and training, electronic security perimeters, physical security of critical cyber assets, systems security management, incident reporting and response planning, and recovery plans for critical cyber assets. In approving these standards, FERC directed that NERC develop revised standards—including a first phase of high-priority modifications and a second phase. On September 30, 2009, FERC approved phase I of the modifications to the standards. The second phase is currently under development. With regard to malicious physical attacks on the bulk-power system, the sole NERC standard is one that requires reporting within industry and to government of disturbances or unusual occurrences, suspected or determined to be caused by sabotage.

NERC's record with regard to grid security vulnerabilities and threats has raised concerns. For example, three years after the identification of the Aurora vulnerability discussed above, NERC still has not proposed any reliability standard directly addressing that vulnerability. In addition, NERC's current CIP standards apply only to "critical assets and associated critical cyber assets," as self-identified by owners and operators of such assets. In a December 2008 NERC survey of self-certification of critical assets and critical cyber assets, only 31% of respondents to the survey, and only 29% of owners and operators of electric generation, identified even a single critical asset. Only 63% of transmission owners identified even a single critical asset. Consequently, a substantial proportion of bulk-power system assets are not actually covered by any CIP standard. NERC expressed its concern with these results in a letter to industry stakeholders dated April 7, 2009, but an April 2010 survey does not indicate any improvement in coverage. Fi-

[9] North American Electric Reliability Corporation, *Reliability Standards Development Procedure,* Version 7 (Feb. 5, 2010).

nally, in testimony before the Committee, FERC raised concerns about whether NERC's open stakeholder process is capable of addressing rapidly emerging grid security vulnerabilities with sufficient speed and protection of sensitive information.

LEGISLATIVE HISTORY

H.R. 2165, the Bulk Power System Protection Act of 2009, was introduced by Rep. John Barrow (with Reps. Henry A. Waxman and Edward J. Markey as co-sponsors) on April 29, 2009. On October 27, 2009, the Subcommittee on Energy and Environment held a legislative hearing on this bill and related legislation. In preparation for that hearing, the Subcommittee convened a classified briefing on grid security vulnerabilities and threats for members of the full Committee on Energy and Commerce and staff with appropriate clearances.

After the hearing, the majority and minority staffs of the Subcommittee and full Committee joined in a bipartisan effort to develop grid security legislation. The results of this effort were embodied in a Committee print, considered in markup by the Subcommittee on Energy and Environment on March 24, 2010. The Subcommittee approved by voice vote the Committee print for consideration by the full Committee with the recommendation that the legislation pass. The text of H.R. 5026, which was introduced by Reps. Edward J. Markey and Fred Upton on April 14, 2010, is identical in substance to the text of the Committee print forwarded by the Subcommittee. On April 15, 2010, the Committee on Energy and Commerce held a markup to consider H.R. 5026 and, after approving a manager's amendment in the nature of a substitute by voice vote, unanimously agreed to a motion for final passage of the bill.

COMMITTEE CONSIDERATION

The Subcommittee on Energy and Environment met in open markup session on March 24, 2010, to consider a Committee Print dated March 22, 2010, on H.R. _____, to amend the Federal Power Act to protect the bulk-power system and electric infrastructure critical to the defense of the United States from cybersecurity and other threats and vulnerabilities. Subsequently, the Subcommittee approved the text of the Committee Print to be forwarded to the full Committee without amendments by a voice vote. H.R. 5026 was introduced on April 14, 2010, with the identical language of the Committee Print as approved by the Subcommittee, and was referred to the Committee on Energy and Commerce.

The full Committee met in open markup session on April 15, 2010, to consider H.R. 5026. A manager's amendment by Mr. Waxman was adopted by a voice vote. Subsequently, the Committee ordered H.R. 5026 favorably reported to the House, amended, by a roll call vote of 47 yeas and 0 nays.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the motion to report legislation and amendments thereto. The Committee agreed to a motion by Mr. Waxman to order H.R. 5026 favorably reported to the House, amended, by a record vote of 47 yeas and

0 nays. The following is the recorded vote taken during Committee consideration, including the names of those Members voting for and against:

COMMITTEE ON ENERGY AND COMMERCE – 111TH CONGRESS
ROLL CALL VOTE # 148

BILL: **H.R. 5026,** the "Grid Reliability and Infrastructure Defense Act" or the "GRID Act".

MOTION: A motion by Mr. Waxman to order H.R. 5026 favorably reported to the House, amended. (Final Passage)

DISPOSITION: **AGREED TO** by a roll call vote of 47 yeas to 0 nays.

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Mr. Waxman	X			Mr. Barton	X		
Mr. Dingell	X			Mr. Hall	X		
Mr. Markey	X			Mr. Upton	X		
Mr. Boucher				Mr. Stearns	X		
Mr. Pallone	X			Mr. Whitfield			
Mr. Gordon				Mr. Shimkus			
Mr. Rush	X			Mr. Shadegg	X		
Ms. Eshoo	X			Mr. Blunt			
Mr. Stupak	X			Mr. Buyer	X		
Mr. Engel				Mr. Radanovich	X		
Mr. Green	X			Mr. Pitts	X		
Ms. DeGette	X			Ms. Bono Mack	X		
Mrs. Capps	X			Mr. Terry	X		
Mr. Doyle				Mr. Rogers			
Ms. Harman				Mrs. Myrick			
Ms. Schakowsky				Mr. Sullivan	X		
Mr. Gonzalez				Mr. Murphy of PA	X		
Mr. Inslee	X			Mr. Burgess	X		
Ms. Baldwin	X			Ms. Blackburn	X		
Mr. Ross	X			Mr. Gingrey	X		
Mr. Weiner	X			Mr. Scalise	X		
Mr. Matheson	X			Mr. Griffith	X		
Mr. Butterfield	X			Mr. Latta	X		
Mr. Melancon	X						
Mr. Barrow	X						
Mr. Hill	X						
Ms. Matsui	X						
Mrs. Christensen	X						
Ms. Castor	X						
Mr. Sarbanes	X						
Mr. Murphy of CT	X						
Mr. Space	X						
Mr. McNerney	X						
Ms. Sutton	X						
Mr. Braley	X						
Mr. Welch	X						

04/15/2010

COMMITTEE OVERSIGHT FINDINGS AND RECOMMENDATIONS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the findings and recommendations of the Committee are reflected in the descriptive portions of this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

Regarding compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the estimate of budget authority and revenues regarding H.R. 5026 prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974. The Committee finds that H.R. 5026 would result in no new or increased entitlement authority or tax expenditures.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

In accordance with clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the Committee's performance goals and objectives are reflected in the descriptive portions of this report.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds that the constitutional authority for H.R. 5026 is provided in Article I, section 8, clauses 3 and 18.

EARMARKS AND TAX AND TARIFF BENEFITS

H.R. 5026 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9 of rule XXI of the Rules of the House of Representatives.

ADVISORY COMMITTEE STATEMENT

No advisory committees were created by H.R. 5026 within the meaning of section 5 U.S.C. App., 5(b) of the Federal Advisory Committee Act.

APPLICABILITY OF LAW TO THE LEGISLATIVE BRANCH

The Committee finds that H.R. 5026 does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act of 1985.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimates of federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandate Reform Act.

COMMITTEE COST ESTIMATE

Pursuant to clause 3(d) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the cost estimate

on H.R. 5026 prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate on H.R. 5026 provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

MAY 19, 2010.

Hon. HENRY A. WAXMAN,
Chairman, Committee on Energy and Commerce,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 5026, the Grid Reliability and Infrastructure Defense Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Kathleen Gramp,

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

H.R. 5026—Grid Reliability and Infrastructure Defense Act

Summary: H.R. 5026 would amend existing law regarding the regulation of electric power transmission facilities. Under current law, most of the standards governing the reliability of the bulk-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 set deadlines for FERC to issue standards regarding the security of computer networks used in electric power transmission (known as cybersecurity) and other risks to the electric power transmission grid, subject to certain conditions. In addition, both FERC and ERO would be directed to ensure that utilities maintain adequate supplies of large electrical transformers and implement measures to protect their systems against geomagnetic storms (incidents involving solar radiation). Other provisions would authorize a new technical assistance program related to grid security and establish terms and procedures for responding to emergencies, protecting information, and identifying strategically important electric facilities.

CBO estimates that implementing this bill would increase net direct spending by about $5 million over the 2011–2015 period and $40 million over the 2011–2020 period.[1] Implementing the bill would increase discretionary spending by $219 million over the 2011–2015 period. CBO estimates that enacting this bill would not affect revenues.

Pay-as-you-go procedures apply because enacting the legislation would affect direct spending.

H.R. 5026 would impose intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), on owners and operators of electric infrastructure and a private-sector mandate on ERO. Because of uncertainty about the

[1] Enacting H.R. 5026 would not increase direct spending over the 2010–2014 period and would increase direct spending by $33 million over the 2010–2019 period.

number of entities affected, the scope of future regulations, and the implementation timeline, CBO cannot determine whether the aggregate cost of the mandates in the bill would exceed the annual thresholds established in UMRA for intergovernmental or private-sector mandates ($70 million and $141 million in 2010, respectively, adjusted annually for inflation).

CBO has not reviewed a provision that would provide FERC with emergency authority to protect the electric transmission grid from security threats for intergovernmental or private-sector mandates. Section 4 of UMRA excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined that the provision falls within that exclusion.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 5026 is shown in the following table. The costs of this legislation fall within budget function 270 (energy).

	By fiscal year, in millions of dollars—					
	2011	2012	2013	2014	2015	2011–2015
CHANGES IN DIRECT SPENDING [1]						
Estimated Budget Authority	0	0	0	0	5	5
Estimated Outlays	0	0	0	0	5	5
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Federal Power Agencies:						
Estimated Authorization Level	0	0	0	4	10	14
Estimated Outlays	0	0	0	4	10	14
Department of Energy:						
Estimated Authorization Level	50	51	51	52	52	256
Estimated Outlays	19	39	45	50	52	205
Total Changes:						
Estimated Authorization Level	50	51	51	56	62	270
Estimated Outlays	19	39	45	54	62	219

[1] CBO estimates that enacting the bill would increase direct spending by $40 million over the 2011–2020 period.

Basis of estimate: For this estimate, CBO assumes that the legislation will be enacted near the end of fiscal year 2010, that the necessary funds will be appropriated each year, and that spending patterns will be consistent with historical trends for similar activities.

Background

Taken together, four federal agencies own and operate about 15 percent of the nation's electric power grid, providing much of the transmission service in certain regions of the country. Capital expenditures for the federally owned transmission grid totaled about $645 million in 2009. Most of those costs were incurred by the Tennessee Valley Authority (TVA) and Bonneville Power Administration (BPA). Spending by TVA and BPA affects 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. In contrast, the Western Area Power Administration (WAPA) and Southwestern Power Administration (SWPA) rely on annual appropriations for capital investments in transmission reliability measures. Regardless of the method of financing, the federal power agencies are required by law to set electricity prices high enough to recoup capital investments over the useful life of the assets.

CBO estimates that H.R. 5026 would increase both direct spending and spending subject to appropriation for additional capital investments by federal power agencies. CBO estimates that other provisions of the bill would further increase spending subject to appropriation.

Additional capital spending by federal power agencies (Direct spending and spending subject to appropriation)

The budgetary impacts of this legislation on the federal power agencies would depend on the scope and substance of future regulations that are developed to implement it. FERC and ERO would be directed to require utilities to address various threats, taking into consideration the likelihood of those events and the cost-effectiveness of any mitigation measures. Given the lead times involved in changing standards for electric utilities, CBO expects that most of the budgetary impacts resulting from those rules would occur after 2014 and would involve only modest changes in performance standards through 2020.

Assuming appropriation of the necessary amounts, CBO estimates that implementing H.R. 5026 would increase discretionary spending by WAPA and SWPA by $14 million over the 2011–2015 period, and additional amounts thereafter. In addition, we estimate that additional capital spending by TVA and BPA would increase direct spending by about $40 million, net of recoveries from ratepayers, over the 2011–2020 period.

Acquiring Additional Transformer Capacity. CBO expects that the regulations developed under this bill for large transformers would initially mirror the requirements of the industry's existing voluntary program for sharing spare transformers in the event of a terrorist attack. CBO estimates that complying with those benchmarks would have a negligible effect on spending by TVA, BPA, and SWPA because those agencies have sufficient spare transformers to meet the voluntary guidelines. In contrast, we estimate that WAPA would spend about $12 million over the 2011–2015 period to acquire additional transformers, assuming appropriation of the necessary amounts. Additional costs would occur after 2015 for WAPA. Costs for all of the agencies could be higher if the new rules require utilities to increase the number of spare transformers, which cost between $1 million and $15 million each.

Mitigating Other Risks to Transmission Systems. Currently, there are no standards that address risks posed by natural or malicious disruptions to the grid, such as geomagnetic storms and electromagnetic pulses from weapons. As a result, CBO expects that directives addressing those threats would increase capital spending by the federal power agencies. Government reports have identified various actions that could be taken to mitigate those risks, with costs for the entire industry estimated to range from a few hundred million dollars (for example, for equipment that protects generators or transformers) to over a billion dollars (for example, for comprehensive strategies for the utility industry). For this estimate, CBO assumes that near-term measures would primarily involve small upgrades to equipment and facilities and would increase capital spending on bulk power facilities by less than 1 percent annually. On that basis, CBO estimates that those investments would increase net direct spending by TVA and BPA by about $40 million

over the 2011–2020 period, and discretionary spending for WAPA and SWPA by about $2 million over the 2011–2015 period.

Finally, CBO estimates that other provisions in the bill concerning the security of computer networks used by the federal power agencies would have a negligible budgetary impact because the new standards would be similar to those followed by federal agencies as a result of other statutory directives.

Other impacts on spending subject to appropriation

H.R. 5026 would direct the Secretary of Energy to establish a new technical assistance program related to grid security. According to the Department of Energy (DOE), the proposed program would build on existing efforts related to cybersecurity (currently funded at around $40 million annually) and would focus in particular on developing technologies to mitigate risks associated with geomagnetic storms or certain malicious acts. The bill would direct DOE to establish an outreach program to share expertise developed through those activities. Finally, H.R. 5026 would establish new requirements related to security clearances and sharing sensitive information on grid security among federal agencies.

Based on information from DOE, CBO estimates that those activities would cost about $200 million over the 2011–2015 period, with additional spending occurring in later years. That estimate is based on the cost of similar programs and reflects historical spending patterns for activities related to research, development, and technical assistance.

In addition, CBO expects that implementing H.R. 5026 would expand FERC's workload and increase the agency's administrative costs, which are controlled through annual appropriation acts. Because FERC recovers 100 percent of its costs through user fees, any such increases in its costs would be offset by an equal change in fees that the commission charges, resulting in no net budgetary impact.

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. The net changes in outlays that are subject to those pay-as-you-go procedures are shown in the following table.

CBO ESTIMATE OF PAY-AS-YOU-GO EFFECTS FOR H.R. 5026 AS ORDERED REPORTED BY THE HOUSE COMMITTEE ON ENERGY AND COMMERCE ON APRIL 15, 2010

	By fiscal year, in millions of dollars—												
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2010–2015	2010–2020
NET INCREASE OR DECREASE (−) IN THE DEFICIT													
Statutory Pay-As-You-Go Impact	0	0	0	0	0	5	7	7	7	7	7	5	40

Intergovernmental and private-sector impact: H.R. 5026 would impose intergovernmental and private-sector mandates, as defined in UMRA, on owners and operators of electric infrastructure and a private-sector mandate on the Electric Reliability Organization. Because of uncertainty about the number of entities affected, the scope of future regulations, and the implementation timeline, CBO cannot determine whether the aggregate cost of the mandates in

the bill would exceed the annual thresholds established in UMRA for intergovernmental and private-sector mandates ($70 million and $141 million in 2010, respectively, adjusted annually for inflation).

CBO has not reviewed a provision that would provide FERC with emergency authority to protect the electric transmission grid from security threats for intergovernmental or private-sector mandates. Section 4 of UMRA excludes from the application of that act any legislative provisions that are necessary for national security. CBO has interpreted that exclusion to encompass provisions dealing with activities that are immediately necessary to protect vital national security interests. CBO has determined that the provision dealing with emergency authority falls within the exclusion for national security.

Mandates that apply to both public and private entities

By requiring ERO and FERC to issue new standards to address vulnerabilities in the nation's energy grid, the bill would impose mandates on public and private owners and operators of electric infrastructure. The standards would address vulnerabilities related to cybersecurity, disruptions related to geomagnetic or electromagnetic events and unexpected losses of large transformers. Based on information from FERC and industry sources, the cost of complying with each of the mandates could equal tens of millions of dollars annually, depending on the scope and implementation timeline of future regulations. Because of those uncertainties, however, CBO cannot estimate the total costs of the mandates.

Cybersecurity. The bill would require owners and operators of electric infrastructure to implement measures to mitigate the risk to the power grid from cybersecurity vulnerabilities. FERC would establish the standards for cybersecurity and implementation timelines after an assessment of current standards.

Geomagnetic Storms and Electromagnetic Pulse Events. The bill would require owners and operators of electric infrastructure to protect against risks posed by natural or malicious disruptions to the grid resulting from geomagnetic storms or electromagnetic pulse events. Based on information from government reports, potential mitigation measures could involve significant capital investments in equipment and facilities.

Large Transformers. The bill would require owners and operators of large transformers to maintain an adequate supply of spare transformers in order to restore the reliability of the power grid if any transformer is disabled. The number of spare transformers required by the bill would depend on future regulations.

Mandate that applies to public entities only

The bill would preempt state, local, and tribal laws relating to the disclosure of information or records. Those preemptions would be intergovernmental mandates as defined in UMRA, but CBO estimates that they would impose no duty on states that would result in additional spending.

Mandate that applies to private entities only

Under current law, FERC has the authority to require the ERO to develop reliability standards. The bill would impose a private-

sector mandate by requiring ERO to develop standards earlier than it would have under current law. Based on information from ERO, CBO estimates that the cost to develop the standards would be small in relation to the annual threshold for private-sector mandates.

Estimate prepared by: Federal Costs: Kathleen Gramp (federal power agencies), Megan Carroll (FERC, DOE); 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.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section provides that the short title of the bill is the "Grid Reliability and Infrastructure Defense Act" or the "GRID Act".

Section 2. Amendment to the Federal Power Act

Subsection (a) of this section would amend the Federal Power Act to add a new section 215A, providing FERC new authorities to protect the electric grid against cyber and other threats and vulnerabilities, as well as from geomagnetic storms created by coronal mass ejections and other solar activity.

Subsection (a) of the new section 215A provides a number of definitions. The definition of "bulk-power system" is the same as in the existing section 215 of the Federal Power Act. As a result, except with regard to electric infrastructure serving critical defense facilities, the new authorities established by the bill would extend to matters affecting the reliability of the "bulk-power system"—providing the same coverage as the existing section 215 of the Federal Power Act, enacted as part of the Energy Policy Act of 2005, which provides authority to establish mandatory reliability standards for the bulk-power system. As the agency charged with administering section 215A, FERC has the authority to interpret this and the other definitions included in subsection (a).

Subsection (b) of the new section 215A gives FERC authority to issue emergency orders to protect against a "grid security threat," with or without notice, if the President notifies the Commission (either directly or through the Secretary of Energy) that an imminent "grid security threat" exists. The term "imminent" in this context means that the grid security threat is urgent, impending, or near at hand, but does not necessarily require that it be immediate in time. A grid security threat is defined under subsection (a) as a substantial likelihood of one of the following acts or events, provided there is a substantial likelihood the act or event would have a significant adverse effect on the reliability of the bulk-power system or of defense critical electric infrastructure:

- a malicious act using electronic communication (i.e., a cyber attack) or an electromagnetic pulse (i.e., one or more pulses of electromagnetic energy, such as radio frequency or microwave, emitted by a device capable of disabling, disrupting, or destroying electronic equipment by means of such a pulse);
- a geomagnetic storm (i.e., a solar storm); or

• a direct physical attack on the bulk power infrastructure or on defense critical electric infrastructure.

A malicious act "using electronic communication" is intended to refer to an act using the electronic communication as an actual vector for the attack (i.e., a cyber attack), as opposed to an act in which electronic communications are used only incidentally, such as the use of electronic communication to plan or execute a physical attack.

Subsection (b) requires the President or Secretary of Energy to promptly notify the relevant congressional committees whenever the President provides a written directive or determination of a grid security threat to FERC under the subsection. Subsection (b) provides for the discontinuance of an order issued under this subsection whenever any of the following first occurs: the President determines the grid security threat no longer exists, FERC determines the emergency measures are no longer needed to protect against the threat, or one year elapses from the date the order was issued.

Subsection (b) also provides FERC with authority to establish a mechanism for owners, operators, or users of the bulk-power system to recover prudently incurred costs of complying with an order under subsection (b) if FERC determines that such entities cannot otherwise recover such costs through market prices or rates. Nothing in this provision is intended to prevent or affect use of other existing mechanisms for the recovery of costs incurred in compliance with this subsection or the remainder of the new section 215A under existing procedures or mechanisms, whether under the Federal Power Act or state law.

Subsection (c)(1) of the new section 215A provides FERC authority to promulgate a rule or issue an order, after notice and comment, requiring implementation of measures to protect against any "grid security vulnerability" that FERC determines has not been adequately addressed by a NERC reliability standard developed and approved under section 215. Subsection (a) defines a grid security vulnerability as a weakness that, in the event of a malicious act using electronic communication (i.e., a cyber attack) or an electromagnetic pulse, would pose a substantial risk of disruption to the operation of those electronic devices or communication networks that are essential to the reliability of the bulk-power system. Before promulgating a rule or issuing an order to address a grid security vulnerability under subsection (c)(1), FERC, to the extent practicable in light of the urgency of the need for action, is required to request and consider recommendations from NERC regarding such a rule or order. FERC may establish an appropriate deadline for NERC's submission of such recommendations.

Subsection (c)(2) specifically requires FERC, within 180 days of enactment, to promulgate a rule or issue an order requiring measures to address the "Aurora vulnerability" to cyber attack that was identified three years ago.

Subsection (c)(3) directs FERC to approve a proposed NERC reliability standard (under section 215) that addresses a grid security vulnerability identified under subsection (c)(1) or (c)(2) unless FERC determines that the NERC standard does not adequately protect against the vulnerability. If FERC approves a proposed

NERC standard, the corresponding FERC rule or order must be rescinded.

Subsection (c)(4) requires FERC to direct NERC to submit for approval a reliability standard under section 215 to protect the bulk-power system against geomagnetic storms. FERC is directed to identify the nature and magnitude of the reasonably foreseeable geomagnetic storm events against which the standards should protect, similar to the identification of a "design basis threat." The standards must balance risks against the cost of protecting against those risks.

Subsection (c)(5) requires FERC to direct NERC to submit for approval a reliability standard under section 215 to require adequate availability of large transformers to ensure the reliability of the bulk-power system in the event of a reasonably foreseeable physical or other attack or a geomagnetic storm. FERC is directed to identify the nature and magnitude of the attack or event against which the standard must protect, similar to the identification of a "design basis threat." The standard must allow entities required to comply with the standard the option of complying either individually or jointly (e.g., through a spare transformer sharing program), and must balance risks against the cost of protecting against those risks.

Subsection (d) of the new section 215A directs the President to designate not more than 100 facilities located in the United States that are critical to the defense of the United States and vulnerable to interruption of an external supply of electricity to the facility. The bill classifies electric infrastructure that is not part of the bulk-power system, that serves such a facility, and that is not owned or operated by the owner or operator of the designated facility, as "defense critical electric infrastructure." If FERC, in consultation with the owner or operator of a designated critical facility, identifies a vulnerability in such infrastructure to a cyber attack or attack using an electromagnetic pulse that has not adequately been addressed, FERC has authority to promulgate a rule or issue an order, after notice and opportunity for comment, to require measures to protect such infrastructure. Infrastructure can be exempted from such rules or orders, on a case-by-case basis, if FERC, in consultation with the owner or operator of the designated critical facility, determines that such infrastructure is adequately protected. An owner or operator of defense critical electric infrastructure shall be required to take such required measures only to the extent that the owners or operators of a facility designated by the President that rely on such infrastructure agree to bear the full incremental costs of compliance with such a rule or order.

Subsection (e) of the new section 215A addresses the treatment of "protected information," defined as information designated as such by FERC that is not classified national security information; that was developed or submitted in connection with the implementation of this section; that specifically discusses grid security threats, grid security vulnerabilities, or defense critical electric infrastructure vulnerabilities, or plans, procedures or measures to address such threats or vulnerabilities; and the unauthorized disclosure of which could be used in a malicious manner to impair the reliability of the bulk power system. The bill exempts such information from disclosure under the Freedom of Information Act or

under state, local, or tribal disclosure laws. The bill also requires FERC to promulgate regulations and issue orders necessary to designate protected information, prohibit unauthorized disclosure of such information, and facilitate appropriate sharing of such information with, between, and by governmental authorities, NERC, the regional reliability councils, and owners, operators, and users of the bulk-power system.

Subsection (f) of the new section 215A provides that any party seeking judicial review of an order issued under this section pursuant to section 313 of the Federal Power Act may obtain such review exclusively in the U.S. Court of Appeals for the District of Columbia Circuit.

Subsection (g) of the new section 215A directs the Secretary of Energy to develop technical expertise in the protection of the grid against attacks using electronic communication or electromagnetic pulse, and against geomagnetic storms, and to provide technical assistance in this area to owners, operators, and users of systems for the generation, transmission and distribution of electric energy—with priority given to systems serving critical defense and other critical-infrastructure facilities. The Secretary is directed to facilitate and, to the extent practicable, expedite acquisition of security clearances by key industry personnel to facilitate communication regarding grid security threats and vulnerabilities. In addition, the Secretary, FERC, and other federal authorities are directed, to the extent practicable, to share timely and actionable information regarding grid security threats and vulnerabilities and defense critical electric infrastructure vulnerabilities with appropriate key personnel of owners, operators, and users of the bulk-power system and defense critical electric infrastructure.

Section 2(b) of the GRID Act makes conforming amendments to section 201 of the Federal Power Act.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as 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

* * * * * * *

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

DECLARATION OF POLICY; APPLICATION OF PART; DEFINITIONS

SECTION 201. (a) * * *

(b)(1) * * *

(2) Notwithstanding section 201(f), the provisions of sections 203(a)(2), 206(e), 210, 211, 211A, 212, 215, *215A,* 216, 217, 218, 219, 220, 221, and 222 shall apply to the entities described in such provisions, and such entities shall be subject to the jurisdiction of the Commission for purposes of carrying out such provisions and for purposes of applying the enforcement authorities of this Act

with respect to such provisions. Compliance with any order of the Commission under the provisions of section 203(a)(2), 206(e), 210, 211, 211A, 212, 215, *215A,* 216, 217, 218, 219, 220, 221, or 222, shall not make an electric utility or other entity subject to the jurisdiction of the Commission for any purposes other than the purposes specified in the preceding sentence.

* * * * * * *

(e) The term "public utility" when used in this Part or in the Part next following means any person who owns or operates facilities subject to the jurisdiction of the Commission under this Part (other than facilities subject to such jurisdiction solely by reason of section 206(e), 206(f), 210, 211, 211A, 212, 215, *215A,* 216, 217, 218, 219, 220, 221, or 222).

* * * * * * *

SEC. 215A. CRITICAL ELECTRIC INFRASTRUCTURE SECURITY.

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

(1) BULK-POWER SYSTEM; ELECTRIC RELIABILITY ORGANIZATION; REGIONAL ENTITY.—The terms "bulk-power system", "Electric Reliability Organization", and "regional entity" have the meanings given such terms in paragraphs (1), (2), and (7) of section 215(a), respectively.

(2) DEFENSE CRITICAL ELECTRIC INFRASTRUCTURE.—The term "defense critical electric infrastructure" means any infrastructure located in the United States (including the territories) used for the generation, transmission, or distribution of electric energy that—

(A) is not part of the bulk-power system; and

(B) serves a facility designated by the President pursuant to subsection (d)(1), but is not owned or operated by the owner or operator of such facility.

(3) DEFENSE CRITICAL ELECTRIC INFRASTRUCTURE VULNERABILITY.—The term "defense critical electric infrastructure vulnerability" means a weakness in defense critical electric infrastructure that, in the event of a malicious act using electronic communication or an electromagnetic pulse, would pose a substantial risk of disruption of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of defense critical electric infrastructure.

(4) ELECTROMAGNETIC PULSE.—The term "electromagnetic pulse" means 1 or more pulses of electromagnetic energy emitted by a device capable of disabling, disrupting, or destroying electronic equipment by means of such a pulse.

(5) GEOMAGNETIC STORM.—The term "geomagnetic storm" means a temporary disturbance of the Earth's magnetic field resulting from solar activity.

(6) GRID SECURITY THREAT.—The term "grid security threat" means a substantial likelihood of—

(A)(i) a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of the

bulk-power system or of defense critical electric infrastructure; and

(ii) disruption of the operation of such devices or networks, with significant adverse effects on the reliability of the bulk-power system or of defense critical electric infrastructure, as a result of such act or event; or

(B)(i) a direct physical attack on the bulk-power system or on defense critical electric infrastructure; and

(ii) significant adverse effects on the reliability of the bulk-power system or of defense critical electric infrastructure as a result of such physical attack.

(7) GRID SECURITY VULNERABILITY.—The term "grid security vulnerability" means a weakness that, in the event of a malicious act using electronic communication or an electromagnetic pulse, would pose a substantial risk of disruption to the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of the bulk-power system.

(8) LARGE TRANSFORMER.—The term "large transformer" means an electric transformer that is part of the bulk-power system.

(9) PROTECTED INFORMATION.—The term "protected information" means information, other than classified national security information, designated as protected information by the Commission under subsection (e)(2)—

(A) that was developed or submitted in connection with the implementation of this section;

(B) that specifically discusses grid security threats, grid security vulnerabilities, defense critical electric infrastructure vulnerabilities, or plans, procedures, or measures to address such threats or vulnerabilities; and

(C) the unauthorized disclosure of which could be used in a malicious manner to impair the reliability of the bulk-power system or of defense critical electric infrastructure.

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

(11) SECURITY.—The definition of "security" in section 3(16) shall not apply to the provisions in this section.

(b) EMERGENCY RESPONSE MEASURES.—

(1) AUTHORITY TO ADDRESS GRID SECURITY THREATS.—Whenever the President issues and provides to the Commission (either directly or through the Secretary) a written directive or determination identifying an imminent grid security threat, the Commission may, with or without notice, hearing, or report, issue such orders for emergency measures as are necessary in its judgment to protect the reliability of the bulk-power system or of defense critical electric infrastructure against such threat. As soon as practicable but not later than 180 days after the date of enactment of this section, the Commission shall, after notice and opportunity for comment, establish rules of procedure that ensure that such authority can be exercised expeditiously.

(2) NOTIFICATION OF CONGRESS.—Whenever the President issues and provides to the Commission (either directly or through the Secretary) a written directive or determination

under paragraph (1), the President (or the Secretary, as the case may be) shall promptly notify congressional committees of relevant jurisdiction, including the Committee on Energy and Commerce of the House of Representatives and the Committee on Energy and Natural Resources of the Senate, of the contents of, and justification for, such directive or determination.

(3) CONSULTATION.—Before issuing an order for emergency measures under paragraph (1), the Commission shall, to the extent practicable in light of the nature of the grid security threat and the urgency of the need for such emergency measures, consult with appropriate governmental authorities in Canada and Mexico, entities described in paragraph (4), the Secretary, and other appropriate Federal agencies regarding implementation of such emergency measures.

(4) APPLICATION.—An order for emergency measures under this subsection may apply to—

(A) the Electric Reliability Organization;

(B) a regional entity; or

(C) any owner, user, or operator of the bulk-power system or of defense critical electric infrastructure within the United States.

(5) DISCONTINUANCE.—The Commission shall issue an order discontinuing any emergency measures ordered under this subsection, effective not later than 30 days after the earliest of the following:

(A) The date upon which the President issues and provides to the Commission (either directly or through the Secretary) a written directive or determination that the grid security threat identified under paragraph (1) no longer exists.

(B) The date upon which the Commission issues a written determination that the emergency measures are no longer needed to address the grid security threat identified under paragraph (1), including by means of Commission approval of a reliability standard under section 215 that the Commission determines adequately addresses such threat.

(C) The date that is 1 year after the issuance of an order under paragraph (1).

(6) COST RECOVERY.—If the Commission determines that owners, operators, or users of the bulk-power system or of defense critical electric infrastructure have incurred substantial costs to comply with an order under this subsection and that such costs were prudently incurred and cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners, operators, or users, the Commission shall, after notice and an opportunity for comment, establish a mechanism that permits such owners, operators, or users to recover such costs.

(c) MEASURES TO ADDRESS GRID SECURITY VULNERABILITIES.—

(1) COMMISSION AUTHORITY.—If the Commission, in consultation with appropriate Federal agencies, identifies a grid security vulnerability that the Commission determines has not adequately been addressed through a reliability standard developed and approved under section 215, the Commission shall,

after notice and opportunity for comment and after consultation with the Secretary, other appropriate Federal agencies, and appropriate governmental authorities in Canada and Mexico, promulgate a rule or issue an order requiring implementation, by any owner, operator, or user of the bulk-power system in the United States, of measures to protect the bulk-power system against such vulnerability. Before promulgating a rule or issuing an order under this paragraph, the Commission shall, to the extent practicable in light of the urgency of the need for action to address the grid security vulnerability, request and consider recommendations from the Electric Reliability Organization regarding such rule or order. The Commission may establish an appropriate deadline for the submission of such recommendations.

(2) CERTAIN EXISTING CYBERSECURITY VULNERABILITIES.—Not later than 180 days after the date of enactment of this section, the Commission shall, after notice and opportunity for comment and after consultation with the Secretary, other appropriate Federal agencies, and appropriate governmental authorities in Canada and Mexico, promulgate a rule or issue an order requiring the implementation, by any owner, user, or operator of the bulk-power system in the United States, of such measures as are necessary to protect the bulk-power system against the vulnerabilities identified in the June 21, 2007, communication to certain 'Electricity Sector Owners and Operators' from the North American Electric Reliability Corporation, acting in its capacity as the Electricity Sector Information and Analysis Center.

(3) RESCISSION.—The Commission shall approve a reliability standard developed under section 215 that addresses a grid security vulnerability that is the subject of a rule or order under paragraph (1) or (2), unless the Commission determines that such reliability standard does not adequately protect against such vulnerability or otherwise does not satisfy the requirements of section 215. Upon such approval, the Commission shall rescind the rule promulgated or order issued under paragraph (1) or (2) addressing such vulnerability, effective upon the effective date of the newly approved reliability standard.

(4) GEOMAGNETIC STORMS.—Not later than 1 year after the date of enactment of this section, the Commission shall, after notice and an opportunity for comment and after consultation with the Secretary and other appropriate Federal agencies, issue an order directing the Electric Reliability Organization to submit to the Commission for approval under section 215, not later than 1 year after the issuance of such order, reliability standards adequate to protect the bulk-power system from any reasonably foreseeable geomagnetic storm event. The Commission's order shall specify the nature and magnitude of the reasonably foreseeable events against which such standards must protect. Such standards shall appropriately balance the risks to the bulk-power system associated with such events, including any regional variation in such risks, and the costs of mitigating such risks.

(5) LARGE TRANSFORMER AVAILABILITY.—Not later than 1 year after the date of enactment of this section, the Commission

shall, after notice and an opportunity for comment and after consultation with the Secretary and other appropriate Federal agencies, issue an order directing the Electric Reliability Organization to submit to the Commission for approval under section 215, not later than 1 year after the issuance of such order, reliability standards addressing availability of large transformers. Such standards shall require entities that own or operate large transformers to ensure, individually or jointly, adequate availability of large transformers to promptly restore the reliable operation of the bulk-power system in the event that any such transformer is destroyed or disabled as a result of a reasonably foreseeable physical or other attack or geomagnetic storm event. The Commission's order shall specify the nature and magnitude of the reasonably foreseeable attacks or events that shall provide the basis for such standards. Such standards shall—

(A) provide entities subject to the standards with the option of meeting such standards individually or jointly; and

(B) appropriately balance the risks associated with a reasonably foreseeable attack or event, including any regional variation in such risks, and the costs of ensuring adequate availability of spare transformers.

(d) CRITICAL DEFENSE FACILITIES.—

(1) DESIGNATION.—Not later than 180 days after the date of enactment of this section, the President shall designate, in a written directive or determination provided to the Commission, facilities located in the United States (including the territories) that are—

(A) critical to the defense of the United States; and

(B) vulnerable to a disruption of the supply of electric energy provided to such facility by an external provider.

The number of facilities designated by such directive or determination shall not exceed 100. The President may periodically revise the list of designated facilities through a subsequent written directive or determination provided to the Commission, provided that the total number of designated facilities at any time shall not exceed 100.

(2) COMMISSION AUTHORITY.—If the Commission identifies a defense critical electric infrastructure vulnerability that the Commission, in consultation with owners and operators of any facility or facilities designated by the President pursuant to paragraph (1), determines has not adequately been addressed through measures undertaken by owners or operators of defense critical electric infrastructure, the Commission shall, after notice and an opportunity for comment and after consultation with the Secretary and other appropriate Federal agencies, promulgate a rule or issue an order requiring implementation, by any owner or operator of defense critical electric infrastructure, of measures to protect the defense critical electric infrastructure against such vulnerability. The Commission shall exempt from any such rule or order any specific defense critical electric infrastructure that the Commission determines already has been adequately protected against the identified vulnerability. The Commission shall make any such determination in consultation with the owner or operator of the facility designated by the

President pursuant to paragraph (1) that relies upon such defense critical electric infrastructure.

(3) COST RECOVERY.—An owner or operator of defense critical electric infrastructure shall be required to take measures under paragraph (2) only to the extent that the owners or operators of a facility or facilities designated by the President pursuant to paragraph (1) that rely upon such infrastructure agree to bear the full incremental costs of compliance with a rule promulgated or order issued under paragraph (2).

(e) PROTECTION OF INFORMATION.—

(1) PROHIBITION OF PUBLIC DISCLOSURE OF PROTECTED INFORMATION.—Protected information—

(A) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and

(B) shall not be made available pursuant to any State, local, or tribal law requiring disclosure of information or records.

(2) INFORMATION SHARING.—

(A) IN GENERAL.—Consistent with the Controlled Unclassified Information framework established by the President, the Commission shall promulgate such regulations and issue such orders as necessary to designate protected information and to prohibit the unauthorized disclosure of such protected information.

(B) SHARING OF PROTECTED INFORMATION.—The regulations promulgated and orders issued pursuant to subparagraph (A) shall provide standards for and facilitate the appropriate sharing of protected information with, between, and by Federal, State, local, and tribal authorities, the Electric Reliability Organization, regional entities, and owners, operators, and users of the bulk-power system in the United States and of defense critical electric infrastructure. In promulgating such regulations and issuing such orders, the Commission shall take account of the role of State commissions in reviewing the prudence and cost of investments within their respective jurisdictions. The Commission shall consult with appropriate Canadian and Mexican authorities to develop protocols for the sharing of protected information with, between, and by appropriate Canadian and Mexican authorities and owners, operators, and users of the bulk-power system outside the United States.

(3) SUBMISSION OF INFORMATION TO CONGRESS.—Nothing in this section shall permit or authorize the withholding of information from Congress, any committee or subcommittee thereof, or the Comptroller General.

(4) DISCLOSURE OF NON-PROTECTED INFORMATION.—In implementing this section, the Commission shall protect from disclosure only the minimum amount of information necessary to protect the reliability of the bulk-power system and of defense critical electric infrastructure. The Commission shall segregate protected information within documents and electronic communications, wherever feasible, to facilitate disclosure of information that is not designated as protected information.

(5) DURATION OF DESIGNATION.—Information may not be designated as protected information for longer than 5 years, unless specifically redesignated by the Commission.

(6) REMOVAL OF DESIGNATION.—The Commission may remove the designation of protected information, in whole or in part, from a document or electronic communication if the unauthorized disclosure of such information could no longer be used to impair the reliability of the bulk-power system or of defense critical electric infrastructure.

(7) JUDICIAL REVIEW OF DESIGNATIONS.—Notwithstanding subsection (f) of this section or section 313, a person or entity may seek judicial review of a determination by the Commission concerning the designation of protected information under this subsection exclusively in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in the District of Columbia. In such a case the court shall determine the matter de novo, and may examine the contents of documents or electronic communications designated as protected information in camera to determine whether such documents or any part thereof were improperly designated as protected information. The burden is on the Commission to sustain its designation.

(f) JUDICIAL REVIEW.—The Commission shall act expeditiously to resolve all applications for rehearing of orders issued pursuant to this section that are filed under section 313(a). Any party seeking judicial review pursuant to section 313 of an order issued under this section may obtain such review only in the United States Court of Appeals for the District of Columbia Circuit.

(g) PROVISION OF ASSISTANCE TO INDUSTRY IN MEETING GRID SECURITY PROTECTION NEEDS.—

(1) EXPERTISE AND RESOURCES.—The Secretary shall establish a program, in consultation with other appropriate Federal agencies, to develop technical expertise in the protection of systems for the generation, transmission, and distribution of electric energy against geomagnetic storms or malicious acts using electronic communications or electromagnetic pulse that would pose a substantial risk of disruption to the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of such systems. Such program shall include the identification and development of appropriate technical and electronic resources, including hardware, software, and system equipment.

(2) SHARING EXPERTISE.—As appropriate, the Secretary shall offer to share technical expertise developed under the program under paragraph (1), through consultation and assistance, with owners, operators, or users of systems for the generation, transmission, or distribution of electric energy located in the United States and with State commissions. In offering such support, the Secretary shall assign higher priority to systems serving facilities designated by the President pursuant to subsection (d)(1) and other critical-infrastructure facilities, which the Secretary shall identify in consultation with the Commission and other appropriate Federal agencies.

(3) SECURITY CLEARANCES AND COMMUNICATION.—The Secretary shall facilitate and, to the extent practicable, expedite the

acquisition of adequate security clearances by key personnel of any entity subject to the requirements of this section to enable optimum communication with Federal agencies regarding grid security threats, grid security vulnerabilities, and defense critical electric infrastructure vulnerabilities. The Secretary, the Commission, and other appropriate Federal agencies shall, to the extent practicable and consistent with their obligations to protect classified and protected information, share timely actionable information regarding grid security threats, grid security vulnerabilities, and defense critical electric infrastructure vulnerabilities with appropriate key personnel of owners, operators, and users of the bulk-power system and of defense critical electric infrastructure.

* * * * * * *

○