I

111TH CONGRESS
1ST SESSION

H. R. 2165

To amend Part II of the Federal Power Act to address known cybersecurity threats to the reliability of the bulk power system, and to provide emergency authority to address future cybersecurity threats to the reliability of the bulk power system, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 29, 2009

Mr. BARROW (for himself, Mr. MARKEY of Massachusetts, and Mr. WAXMAN) introduced the following bill; which was referred to the Committee on Energy and Commerce

---

A BILL

To amend Part II of the Federal Power Act to address known cybersecurity threats to the reliability of the bulk power system, and to provide emergency authority to address future cybersecurity threats to the reliability of the bulk power system, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Bulk Power System Protection Act of 2009''.

SEC. 2. FINDINGS.

The Congress finds that—

(1) it is in the public interest to require the Federal Energy Regulatory Commission to promptly order measures to address known cybersecurity threats to the reliability of the electric bulk power system; and

(2) the Commission must have the necessary emergency authority to respond promptly to future cybersecurity threats that could compromise reliability of the bulk power system.

SEC. 3. PROTECTION OF BULK POWER SYSTEM FROM CYBERSECURITY THREATS.

(a) IN GENERAL.—Part II of the Federal Power Act is amended by adding the following new section after section 215:

"SEC. 215A. EMERGENCY AUTHORITY TO ADDRESS CYBERSECURITY THREATS TO THE BULK POWER SYSTEM.

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

''(1) The terms 'reliability standard', 'bulk power system', 'reliable operation', 'cybersecurity incident', 'Electric Reliability Organization', 'regional entity', and 'owners, users or operators' shall have the same meaning as when used in section 215.

''(2) The term 'cybersecurity threat' means that there is credible information or evidence of—

"(A) a likelihood of a malicious act that could disrupt the operation of those programmable electronic devices and communications networks including hardware, software and data that are essential to the reliable operation of the bulk power system; and

"(B) a substantial possibility of disruption to the operation of such devices and networks in the event of such a malicious act.

"(3) CLASSIFIED INFORMATION.—The term 'classified information' means any information that has been determined pursuant to Executive Order 12958, as amended, or successor orders, or the Atomic Energy Act of 1954, to require protection against unauthorized disclosure and that is so designated.

"(4) SENSITIVE CYBERSECURITY INFORMATION.—The term 'sensitive cybersecurity information' means unclassified information that, if an unauthorized disclosure is made, could be used in a malicious manner to impair the reliability or operations of the bulk power system or the supply of electricity to the bulk power system.

"(5) The term 'Secretary' means the Secretary of Energy.

''(b) INTERIM AUTHORITY TO ADDRESS EXISTING CYBERSECURITY THREATS.—

''(1) IN GENERAL.—After notice and opportunity for comment, and after consultation with appropriate governmental authorities in Canada and Mexico (subject to adequate protections against inappropriate disclosure of security-sensitive information), the Commission shall establish, by rule or order, within 120 days after enactment of this section, such measures or actions as are necessary to protect the reliability of the bulk power system against the cybersecurity threats resulting from—

''(A) 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 Sharing and Analysis Center; and

''(B) related remote access issues.

Such measures or actions may be required of any owner, user, or operator of the bulk power system within the United States.

''(2) ADDITIONAL ORDERS.—Until such time as the interim reliability measures or actions ordered

under this subsection are replaced by cybersecurity reliability standards developed, approved, and implemented pursuant to section 215, the Commission may issue additional orders to supplement the initial rule or order issued under this subsection only if, based on subsequent information or petition from an affected entity, the Commission determines that clarification or refinements to the originally ordered measures or actions are necessary to ensure that the threats are adequately and appropriately addressed. Any such additional orders shall be preceded by notice and opportunity for comment.

''(c) FUTURE EMERGENCIES INVOLVING IMMINENT CYBERSECURITY THREATS.—

''(1) AUTHORITY TO ADDRESS IMMINENT CYBERSECURITY THREATS.—Whenever the President issues and provides to the Commission (either directly or through the Secretary) a written directive or determination that an imminent cybersecurity threat to the reliability of the bulk power system exists, the Commission may on its own motion, with or without notice, hearing, or report issue such orders for emergency measures or actions as are necessary in its judgment to protect the reliability of the bulk power system against such threat.

''(2) CONSULTATION.—Before acting under this subsection, to the extent feasible, taking into account the nature of the threat and urgency of need for action, the Commission shall consult with appropriate governmental authorities in Canada and Mexico (subject to adequate protections against inappropriate disclosure of security-sensitive information), entities described in paragraph (3), and officials at other Federal agencies, including the Secretary, as appropriate, regarding implementation of measures or actions that will effectively address the identified threat.

''(3) APPLICATION OF EMERGENCY MEASURES.—An order for emergency actions or measures under this subsection may apply to—

''(A) the Electric Reliability Organization referred to in section 215,

''(B) a regional entity with respect to the United States operations of the Electric Reliability Organization,

''(C) the regional entity, or

''(D) any owner, user, or operator of the bulk power system within the United States.

''(d) DISCONTINUANCE OF INTERIM MEASURES.—The Commission shall issue an order discontinuing any

measures or actions ordered under subsection (b) upon the earliest of the following:

''(1) When the President (either directly or through the Secretary of Energy) issues a written order or directive provided to the Commission to the effect that the threat to the bulk power system that requires such measures, or actions no longer exists.

''(2) When the Commission determines in writing that the ordered measures or actions are no longer needed to address the identified threat.

''(3) When a reliability standard developed and approved pursuant to section 215 is implemented to address the identified threat.

''(4) One year after the issuance of an order under subsections (b) unless the President (either directly or through the Secretary) issues a determination affirming the continuing nature of the threat. A determination issued under this paragraph shall expire upon the implementation of a standard under section 215 to address the identified threat.

The Commission shall issue such order to be effective within 30 days of the relevant triggering event set out in paragraphs (1) through (4).

''(e) DISCONTINUANCE OF EMERGENCY MEASURES.—The Commission shall issue an order dis-

continuing any measures or actions ordered under subsection (c) upon the earliest of the following:

''(1) When the President (either directly or through the Secretary of Energy) issues a written order or directive provided to the Commission to the effect that the threat to the bulk power system that requires such measures, or actions no longer exists.

''(2) When the Commission determines in writing that the ordered measures or actions are no longer needed to address the identified threat.

''(3) When a reliability standard developed and approved pursuant to section 215 is implemented to address the identified threat.

''(4) With respect to orders under subsection (c), one year after the issuance of an order unless the President (either directly or through the Secretary) issues a determination reaffirming the continuing nature of the threat. A determination issued under this paragraph shall expire upon the implementation of a standard under section 215 to address the identified threat.

The Commission shall issue such order to be effective within 30 days of the relevant triggering event set out in paragraphs (1) through (4).

''(f) PROTECTION OF UNCLASSIFIED SENSITIVE CYBERSECURITY INFORMATION.—

''(1) CONFIDENTIALITY PROCEDURES.—After notice and opportunity for comment, the Commission shall promulgate rules and procedures to prohibit the unauthorized disclosure of unclassified sensitive cybersecurity information—

''(A) which was developed or used in connection with the implementation of this section,

''(B) which specifically discusses cybersecurity threats, vulnerabilities, mitigation plans or security procedures, and

''(C) the unauthorized disclosure of which could be used in a malicious manner to impair the reliability or operations of the bulk power system or the supply of electricity to the bulk power system.

Such rules and procedures shall require the inventory and safeguarding of such information during its creation, storage and transmittal by the Commission or by any other entity, including any vendor, contractor or consultant.

''(2) LIMITED DISCLOSURE TO ENTITIES SUBJECT TO COMMISSION ACTION.—In the rules and procedures promulgated under paragraph (1), the

Commission shall authorize the release of sensitive cybersecurity information to entities subject to Commission action under this section and to their employees, contractors and third-party representatives, to the extent necessary to enable such entities to implement Commission rules, orders or measures. Entities originating, receiving or possessing such information shall comply with Commission rules and procedures to limit disclosure of such information to any other entities that have been determined to have a need to know, have executed non disclosure agreements, and have been deemed by the entity to be trustworthy and reliable. Any entity which signed such non disclosure agreement and was found by the Commission or by another entity subject to this section to have improperly disclosed sensitive cybersecurity information shall thereafter be denied access to such information, and the Commission shall suspend ability of the entity disclosing such information to appear before the Commission. The sanctions under this paragraph against any individual or other entity shall be in addition to, and not in lieu of, any other actions Commission is authorized to take pursuant to section 316A for failure to comply with the rules or procedures established by the Commission under

this section. Information designated sensitive cybersecurity information pursuant to this section shall not be subject to disclosure under the Freedom of Information Act (5 U.S.C. 552).

''(3) LIMITATIONS.—

''(A) The Commission shall consult with national security or national intelligence agencies, as appropriate, for purposes of designating certain information as sensitive cybersecurity information, but shall not designate as sensitive cybersecurity information any information that has been classified by another Federal agency.

''(B) Nothing in this section shall be construed to authorize the withholding of information from the committees of the Congress with jurisdiction over the Commission or the Comptroller General.

''(C) In promulgating and implementing rules and procedures under this section, the Commission shall protect from disclosure only the minimum amount of sensitive cybersecurity information necessary to protect the reliability or operations of the bulk power system or the supply of electricity to the bulk power system. The Commission shall segregate sensitive cyber-

security information within documents, electronic communications, and rules, orders or records associated with such rules and orders, wherever feasible, to facilitate disclosure of information which is not designated as sensitive cybersecurity information.

''(D) Information may not be designated as sensitive cybersecurity information for longer than 10 years, unless specifically redesignated by the Commission.

''(E) The Commission is authorized to remove the designation of sensitive cybersecurity information, in whole or in part, from a document or electronic communication if the unauthorized disclosure could not be used to impair the reliability or operations of the bulk power system or the supply of electricity to the bulk power system.

''(4) CONSISTENCY OF MARKINGS.—The Commission is authorized to place markings on documents, in whole or in part, which designate the degree of sensitivity and limitations on dissemination. Regulations and related procedures may be modified, as appropriate, to ensure consistency with applicable

Executive Orders or laws pertaining to controlled unclassified information.

''(5) NONDISCLOSURE OF SENSITIVE CYBERSECURITY INFORMATION IN RULES OR ORDERS.—If a rule or order issued pursuant to this section contains sensitive cybersecurity information or if information in the record associated with such rule or order constitutes sensitive cybersecurity information, the Commission may make the rule, order or information non-public in whole or in part. The Commission may disclose such non-public rule, order or information to entities other than the recipient of the rule or order, as the Commission deems necessary, to carry out the rule or order and protect the reliability of the bulk power system.

''(6) JUDICIAL REVIEW OF DESIGNATIONS.—Any determination by the Commission concerning the designation of sensitive cybersecurity information shall be subject to judicial review pursuant to subsection (a)(4)(B) of section 552 of title 5 of the United States Code.

''(g) REVIEW.—The Commission shall act expeditiously to resolve all applications for rehearing of orders issued pursuant to this section which are filed under section 313(a). Any person or other entity seeking judicial

review pursuant to section 313 may obtain such review only in the United States Court of Appeals for the District of Columbia Circuit. In the case of any petition for review involving rules or orders containing or relating to security-sensitive information, the Commission and parties shall develop with the court appropriate measures to ensure the confidentiality of such information, including, but not limited to, court filings under seal or otherwise in non-public form, or judicial review in camera.

''(h) ENFORCEMENT DISCRETION.—The Commission is authorized to impose penalties pursuant to section 316A for any violation of a rule or order of the Commission under this section. The Commission shall exercise its discretion in engaging in enforcement actions under this section to recognize good faith efforts to comply with directives of the Commission.

''(i) PAPERWORK REDUCTION.—Chapter 35 of title 44, United States Code (44 U.S.C. 3501 et seq.) (commonly referred to as the 'Paperwork Reduction Act') shall not apply to collections of information that relate to measures or actions described in this section.

''(j) PROVISION OF ASSISTANCE TO INDUSTRY IN MEETING CYBERSECURITY PROTECTION NEEDS.—

''(1) EXPERTISE AND RESOURCES.—The Secretary shall establish a program to develop expertise

and identify technical and electronic resources, including hardware, software and system equipment, helpful to cybersecurity protection of the electric grid and all electric systems, including distribution-level electric systems.

''(2) SHARING EXPERTISE.—The Secretary shall offer to share such expertise through consultation and assistance with any owner, operator, or user of the bulk power system, to any owner or operator of an electricity distribution system located in the United States whether or not connected to the bulk power system, and specifically to any owner or operator of an electricity distribution system that may provide electricity to national defense and other critical-infrastructure facilities of the United States.

''(3) PRIORITY.—The Secretary shall consult with the Commission, the Secretary of Defense, the Secretary of Homeland Security, and other Federal agencies to confirm the identity of States and electric systems serving such national defense and critical-infrastructure facilities, and shall assign higher priority to such States and systems in offering such support.

''(4) CLEARANCES.—The Secretary shall facilitate the acquisition by key security personnel of any

electric entity affected by this subsection of sufficient security clearances to allow such personnel access to information that would enable optimum understanding of cybersecurity threats and ability to respond.

''(5) DEFENSE FACILITIES.—Within one year of the date of enactment of this section, the States of Alaska and Hawaii and the Territory of Guam shall prepare, in consultation with the Secretary of Energy, the Secretary of Defense, and the electric utilities that serve national defense facilities in those jurisdictions, a comprehensive plan, to be implemented by the relevant State and territorial governmental authorities, identifying the emergency measures or actions that will be taken to protect the reliability of the electric power supply of the national defense facilities located in those jurisdictions in the event of an imminent cybersecurity threat. A copy of each such plan shall be provided to the Secretary of Energy and the Secretary of Defense.''.

(b) CONFORMING AMENDMENT.—Section 201(b)(2) of the Federal Power Act is amended by inserting ''215A'' after ''215''.

○