112TH CONGRESS
1ST SESSION

S. _____

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.

IN THE SENATE OF THE UNITED STATES

_____

_____ introduced the following bill; which was read twice and referred to the Committee on _____

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.

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

SECTION 1. CRITICAL ELECTRIC INFRASTRUCTURE.

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

"SEC. 224. CRITICAL ELECTRIC INFRASTRUCTURE.

''(a) DEFINITIONS.—In this section:

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

''(2) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—The term 'critical electric infrastructure information' means critical infrastructure information relating to critical electric infrastructure.

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

''(4) CYBER SECURITY THREAT.—The term 'cyber security threat' means the imminent danger of an act that disrupts, attempts to disrupt, or poses a significant risk of disrupting the operation of programmable electronic devices or communications net-

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

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

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

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

''(b) AUTHORITY OF COMMISSION.—

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

''(2) INITIAL ORDER.—Unless the Commission determines that the reliability standards established pursuant to section 215 are adequate to protect critical electric infrastructure from cyber security

vulnerabilities within _____ days after the date of enactment of this section, the Commission shall order the Electric Reliability Organization to submit to the Commission, not later than _____ days after the date of enactment of this section, a proposed reliability standard or a modification to a reliability standard that will provide adequate protection of critical electric infrastructure from cyber security vulnerabilities.

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

"(4) RELIABILITY STANDARDS.—Any proposed reliability standard or modification to a reliability standard submitted pursuant to paragraph (2) or

(3) shall be developed and approved in accordance with section 215(d).

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

''(6) INTERIM FINAL RULE.—

''(A) ISSUANCE.—If the Electric Reliability Organization fails to submit a proposed reliability standard or a modification to a reliability standard to the Commission that will provide adequate protection of critical electric infrastructure from a cyber security vulnerability within the time prescribed by paragraph (2) or (3) (including any additional time provided under paragraph (5)), the Commission shall issue an interim final rule that provides adequate protection of critical electric infrastructure from a cyber security vulnerability.

''(B) EFFECTIVE DATE.—If the Commission determines the interim final rule must be issued immediately to protect critical electric infrastructure from a cyber security vulnerability, the Commission may—

"(i) issue the interim final rule without prior notice or hearing; or

"(ii) make the interim final rule immediately effective or effective with less than 30 days notice.

"(C) DURATION OF INTERIM FINAL RULE.—An interim final rule issued under this paragraph shall terminate, in whole or in part, on the effective date of a reliability standard or a modification to a reliability standard developed and approved pursuant to section 215 that the Commission determines provides adequate protection to critical electric infrastructure from the cyber security vulnerability addressed by the interim final rule.

"(c) EMERGENCY AUTHORITY OF SECRETARY.—

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

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

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

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

''(d) DURATION OF EXPEDITED OR EMERGENCY RULES OR ORDERS.—Any order issued by the Secretary under subsection (c) shall remain effective for not more

than 90 days unless, during the 90 day-period, the Secretary—

''(1) gives interested persons an opportunity to submit written data, views, or arguments; and

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

''(e) JURISDICTION.—

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

''(2) COVERED ENTITIES.—

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

''(i) carrying out this section; and

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

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

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

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

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

''(1) IN GENERAL.—Section 214 of the Critical Infrastructure Information Act of 2002 (6 U.S.C. 133) shall apply to critical electric infrastructure information submitted to the Commission or the Secretary under this section to the same extent as that section applies to critical infrastructure information voluntarily submitted to the Department of Homeland Security under that Act (6 U.S.C. 131 et seq.).

''(2) RULES PROHIBITING DISCLOSURE.—Notwithstanding section 552 of title 5, United States Code, the Secretary and the Commission shall prescribe regulations prohibiting disclosure of informa-

tion obtained or developed in ensuring cyber security under this section if the Secretary or Commission, as appropriate, decides disclosing the information would be detrimental to the security of critical electric infrastructure.

''(3) PROCEDURES FOR SHARING INFORMATION.—

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

''(B) REQUIREMENTS.—The procedures shall—

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

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

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

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

"(h) ACCESS TO CLASSIFIED INFORMATION.—

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

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

SEC. 2. BUDGETARY EFFECTS.

The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go-Act of 2010, shall be determined by reference to the latest statement

titled ''Budgetary Effects of PAYGO Legislation'' for this Act, submitted for printing in the Congressional Record by the Chairman of the Senate Budget Committee, provided that such statement has been submitted prior to the vote on passage.