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.

---

**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.

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

2. **SECTION 1. SHORT TITLE.**

3. This Act may be cited as the “Grid Cyber Security Act”.

---

IN THE SENATE OF THE UNITED STATES

JULY 11, 2011

Mr. BINGAMAN, from the Committee on Energy and Natural Resources, reported the following original bill; which was read twice and placed on the calendar.
SEC. 2. 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 networks (including hardware, software, and data) essential to the reliable operation of critical electric infrastructure.

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

“(6) Electric reliability organization.—The term ‘Electric Reliability Organization’ has the meaning given the term in section 215(a).

“(7) Secretary.—The term ‘Secretary’ means the Secretary of Energy.

“(b) Authority of Commission.—

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

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

“(3) Subsequent determinations and orders.—If at any time following the issuance of the initial order under paragraph (2) the Commission determines that the reliability standards established pursuant to section 215 are inadequate to protect critical electric infrastructure from a cyber security vulnerability, the Commission shall order the Electric Reliability Organization to submit to the Commission, not later than 180 days after the date of the determination, a proposed reliability standard or a modification to a reliability standard that will pro-
vide adequate protection of critical electric infra-
structure 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 Organi-
zation reasonable additional time to submit a pro-
posed reliability standard or a modification to a reli-
ability standard under paragraph (2) or (3).

“(c) Emergency authority of Secretary.—

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

“(2) Coordination with Canada and Mex-
ico.—In exercising the authority granted under this
subsection, the Secretary is encouraged to consult
and coordinate with the appropriate officials in Can-
ada 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 ex-
tent practicable, taking into account the nature of
the threat and urgency of need for action, the Sec-
retary 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 imple-
ment 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 Sec-
retary—

“(1) gives interested persons an opportunity to
submit written data, views, or arguments; and
“(2) affirms, amends, or repeals the rule or order.

“(e) JURISDICTION.—

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

“(2) COVERED ENTITIES.—

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

“(i) carrying out this section; and

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

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

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

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

“(g) Protection of Critical Electric Infrastructure Information.—

“(1) In general.—Section 214 of the Critical Infrastructure Information Act of 2002 (6 U.S.C. 133) shall apply to critical electric infrastructure information submitted to the Commission or the Secretary under this section, or developed by a Federal power marketing administration or the Tennessee Valley Authority under this section or section 215, to the same extent as that section applies to critical infrastructure information voluntarily submitted to the Department of Homeland Security under that Act (6 U.S.C. 131 et seq.).

“(2) Rules prohibiting disclosure.—Notwithstanding section 552 of title 5, United States Code, the Secretary and the Commission shall prescribe regulations prohibiting disclosure of information obtained or developed in ensuring cybersecurity
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 obso-
lete or erroneous names and information.

“(h) ACCESS TO CLASSIFIED INFORMATION.—

“(1) AUTHORIZATION REQUIRED.—No person
shall be provided with access to classified informa-
tion (as defined in section 6.1 of Executive Order
13526 (50 U.S.C. 435 note; relating to classified na-
tional security information)) relating to cyber secu-

“(2) SECURITY CLEARANCES.—The appropriate
Federal agencies or departments shall cooperate
with the Secretary or the Commission, to the max-
imum extent practicable consistent with applicable
procedures and requirements, in expeditiously pro-

SEC. 3. LIMITED ADDITION OF ERO AUTHORITY FOR CRIT-

ICAL ELECTRIC INFRASTRUCTURE.

Section 215(a)(1) of the Federal Power Act (16
U.S.C. 824o(a)(1)) is amended—

S 1342 PCS
(1) in the first sentence—
   (A) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively, and indenting appropriately;
   (B) by striking “(1) The term” and inserting the following:
   “(1) BULK-POWER SYSTEM.—
      “(A) IN GENERAL.—The term”;
      (C) in clause (i) (as so redesignated), by striking “and” after the semicolon at the end;
      (D) in clause (ii) (as so redesignated), by striking the period at the end and inserting “; and”;
      (E) by adding at the end the following:
      “(iii) for purposes of section 224, facilities used for the local distribution of electric energy that the Commission determines to be critical electric infrastructure pursuant to section 224.”; and
   (2) in the second sentence, by striking “The term” and inserting the following:
      “(B) EXCLUSION.—Except as provided in subparagraph (A), the term”.

VerDate Mar 15 2010 23:22 Jul 11, 2011 Jkt 099200 PO 00000 Frm 00011 Fmt 6652 Sfmt 6201 E:\BILLS\S1342.PCS S1342emcdonald on DSK2BSOYB1PROD with BILLS
SEC. 4. LIMITATION.

Section 215(i) of the Federal Power Act (16 U.S.C. 824o(i)) is amended by adding at the end the following:

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

SEC. 5. TEMPORARY EMERGENCY ORDERS FOR CYBER SECURITY VULNERABILITIES.

Section 215(d) of the Federal Power Act (16 U.S.C. 824o(d)) is amended by adding at the end the following:

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

“(B) to make the temporary emergency order immediately effective; and

“(C) to keep the temporary emergency order in effect until—

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

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

SEC. 6. EMP STUDY.

(a) DOE REPORT.—Not later than 3 years after the date of enactment of this Act, the Secretary of Energy, in consultation with appropriate experts at the National Laboratories (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)), shall prepare and publish a report that assesses the susceptibility of critical electric infrastructure to electromagnetic pulse events and geomagnetic disturbances.

(b) CONTENTS.—The report under subsection (a) shall—
(1) examine the risk of electromagnetic pulse
events and geomagnetic disturbances, using both
computer-based simulations and experimental test-
ing;

(2) assess the full spectrum of possible events
and disturbances and the likelihood that the events
and disturbances would cause significant disruption
to the transmission and distribution of electric
power; and

(3) seek to quantify and reduce uncertainties
associated with estimates for electromagnetic pulse
events and geomagnetic disturbances.

(e) FERC ASSESSMENT.—Not later than 1 year after
publication of the report under subsection (a), the Federal
Energy Regulatory Commission, in coordination with the
Secretary of Energy and in consultation with electric utili-
ties and the ERO (as defined in section 215(a) of the Fed-
eral Power Act (16 U.S.C. 824o(a)), shall submit to Con-
gress an assessment of whether and to what extent infra-
structure affecting the transmission of electric power in
interstate commerce should be hardened against electro-
magnetic events and geomagnetic disturbances, including
an estimate of the costs and benefits of options to harden
the infrastructure.
SEC. 7. 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.
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.

A BILL

[Report No. 112-34]

S. 1342

112th CONGRESS

JULY 11, 2011

Read twice and placed on the calendar