

Calendar No. 101

112TH CONGRESS
1ST SESSION

S. 1342

[Report No. 112-34]

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

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

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 Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

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

1 **SEC. 2. CRITICAL ELECTRIC INFRASTRUCTURE.**

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

4 **“SEC. 224. CRITICAL ELECTRIC INFRASTRUCTURE.**

5 “(a) DEFINITIONS.—In this section:

6 “(1) CRITICAL ELECTRIC INFRASTRUCTURE.—

7 The term ‘critical electric infrastructure’ means sys-
8 tems and assets, whether physical or virtual, used
9 for the generation, transmission, or distribution of
10 electric energy affecting interstate commerce that, as
11 determined by the Commission or the Secretary (as
12 appropriate), are so vital to the United States that
13 the incapacity or destruction of the systems and as-
14 sets would have a debilitating impact on national se-
15 curity, national economic security, or national public
16 health or safety.

17 “(2) CRITICAL ELECTRIC INFRASTRUCTURE IN-
18 FORMATION.—The term ‘critical electric infrastruc-
19 ture information’ means critical infrastructure infor-
20 mation relating to critical electric infrastructure.

21 “(3) CRITICAL INFRASTRUCTURE INFORMA-
22 TION.—The term ‘critical infrastructure information’
23 has the meaning given the term in section 212 of the
24 Critical Infrastructure Information Act of 2002 (6
25 U.S.C. 131).

1 “(4) CYBER SECURITY THREAT.—The term
2 ‘cyber security threat’ means the imminent danger
3 of an act that disrupts, attempts to disrupt, or poses
4 a significant risk of disrupting the operation of pro-
5 grammable electronic devices or communications net-
6 works (including hardware, software, and data) es-
7 sential to the reliable operation of critical electric in-
8 frastructure.

9 “(5) CYBER SECURITY VULNERABILITY.—The
10 term ‘cyber security vulnerability’ means a weakness
11 or flaw in the design or operation of any program-
12 mable electronic device or communication network
13 that exposes critical electric infrastructure to a cyber
14 security threat.

15 “(6) ELECTRIC RELIABILITY ORGANIZATION.—
16 The term ‘Electric Reliability Organization’ has the
17 meaning given the term in section 215(a).

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

20 “(b) AUTHORITY OF COMMISSION.—

21 “(1) INITIAL DETERMINATION.—Not later than
22 120 days after the date of enactment of this section,
23 the Commission shall determine whether reliability
24 standards established pursuant to section 215 are

1 adequate to protect critical electric infrastructure
2 from cyber security vulnerabilities.

3 “(2) INITIAL ORDER.—Unless the Commission
4 determines that the reliability standards established
5 pursuant to section 215 are adequate to protect crit-
6 ical electric infrastructure from cyber security
7 vulnerabilities within 120 days after the date of en-
8 actment of this section, the Commission shall order
9 the Electric Reliability Organization to submit to the
10 Commission, not later than 180 days after the date
11 of issuance of the order, a proposed reliability stand-
12 ard or a modification to a reliability standard that
13 will provide adequate protection of critical electric
14 infrastructure from cyber security vulnerabilities.

15 “(3) SUBSEQUENT DETERMINATIONS AND OR-
16 DERS.—If at any time following the issuance of the
17 initial order under paragraph (2) the Commission
18 determines that the reliability standards established
19 pursuant to section 215 are inadequate to protect
20 critical electric infrastructure from a cyber security
21 vulnerability, the Commission shall order the Elec-
22 tric Reliability Organization to submit to the Com-
23 mission, not later than 180 days after the date of
24 the determination, a proposed reliability standard or
25 a modification to a reliability standard that will pro-

1 vide adequate protection of critical electric infra-
2 structure from the cyber security vulnerability.

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

8 “(5) ADDITIONAL TIME.—The Commission
9 may, by order, grant the Electric Reliability Organi-
10 zation reasonable additional time to submit a pro-
11 posed reliability standard or a modification to a reli-
12 ability standard under paragraph (2) or (3).

13 “(c) EMERGENCY AUTHORITY OF SECRETARY.—

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

22 “(2) COORDINATION WITH CANADA AND MEX-
23 ICO.—In exercising the authority granted under this
24 subsection, the Secretary is encouraged to consult
25 and coordinate with the appropriate officials in Can-

1 ada and Mexico responsible for the protection of
2 cyber security of the interconnected North American
3 electricity grid.

4 “(3) CONSULTATION.—Before exercising the
5 authority granted under this subsection, to the ex-
6 tent practicable, taking into account the nature of
7 the threat and urgency of need for action, the Sec-
8 retary shall consult with the entities described in
9 subsection (e)(1) and with officials at other Federal
10 agencies, as appropriate, regarding implementation
11 of actions that will effectively address the identified
12 cyber security threat.

13 “(4) COST RECOVERY.—The Commission shall
14 establish a mechanism that permits public utilities to
15 recover prudently incurred costs required to imple-
16 ment immediate actions ordered by the Secretary
17 under this subsection.

18 “(d) DURATION OF EXPEDITED OR EMERGENCY
19 RULES OR ORDERS.—Any order issued by the Secretary
20 under subsection (e) shall remain effective for not more
21 than 90 days unless, during the 90 day-period, the Sec-
22 retary—

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

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

3 “(e) JURISDICTION.—

4 “(1) IN GENERAL.—Notwithstanding section
5 201, this section shall apply to any entity that owns,
6 controls, or operates critical electric infrastructure.

7 “(2) COVERED ENTITIES.—

8 “(A) IN GENERAL.—An entity described in
9 paragraph (1) shall be subject to the jurisdic-
10 tion of the Commission for purposes of—

11 “(i) carrying out this section; and

12 “(ii) applying the enforcement au-
13 thorities of this Act with respect to this
14 section.

15 “(B) JURISDICTION.—This subsection
16 shall not make an electric utility or any other
17 entity subject to the jurisdiction of the Commis-
18 sion for any other purpose.

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

22 “(f) DEFENSE FACILITIES.—Not later than 1 year
23 after the date of enactment of this section, the Secretary
24 of Defense shall prepare, in consultation with the Sec-
25 retary, the States of Alaska and Hawaii, the Territory of

1 Guam, and the electric utilities that serve national defense
2 facilities in those States and Territory, a comprehensive
3 plan that identifies the emergency measures or actions
4 that will be taken to protect the reliability of the electric
5 power supply of the national defense facilities located in
6 those States and Territory in the event of an imminent
7 cybersecurity threat.

8 “(g) PROTECTION OF CRITICAL ELECTRIC INFRA-
9 STRUCTURE INFORMATION.—

10 “(1) IN GENERAL.—Section 214 of the Critical
11 Infrastructure Information Act of 2002 (6 U.S.C.
12 133) shall apply to critical electric infrastructure in-
13 formation submitted to the Commission or the Sec-
14 retary under this section, or developed by a Federal
15 power marketing administration or the Tennessee
16 Valley Authority under this section or section 215,
17 to the same extent as that section applies to critical
18 infrastructure information voluntarily submitted to
19 the Department of Homeland Security under that
20 Act (6 U.S.C. 131 et seq.).

21 “(2) RULES PROHIBITING DISCLOSURE.—Not-
22 withstanding section 552 of title 5, United States
23 Code, the Secretary and the Commission shall pre-
24 scribe regulations prohibiting disclosure of informa-
25 tion obtained or developed in ensuring cyber security

1 under this section if the Secretary or Commission,
2 as appropriate, decides disclosing the information
3 would be detrimental to the security of critical elec-
4 tric infrastructure.

5 “(3) PROCEDURES FOR SHARING INFORMA-
6 TION.—

7 “(A) IN GENERAL.—The Secretary and the
8 Commission shall establish procedures on the
9 release of critical infrastructure information to
10 entities subject to this section, to the extent
11 necessary to enable the entities to implement
12 rules or orders of the Commission or the Sec-
13 retary.

14 “(B) REQUIREMENTS.—The procedures
15 shall—

16 “(i) limit the redissemination of infor-
17 mation described in subparagraph (A) to
18 ensure that the information is not used for
19 an unauthorized purpose;

20 “(ii) ensure the security and confiden-
21 tiality of the information;

22 “(iii) protect the constitutional and
23 statutory rights of any individuals who are
24 subjects of the information; and

1 “(iv) provide data integrity through
2 the timely removal and destruction of obso-
3 lete or erroneous names and information.

4 “(h) ACCESS TO CLASSIFIED INFORMATION.—

5 “(1) AUTHORIZATION REQUIRED.—No person
6 shall be provided with access to classified informa-
7 tion (as defined in section 6.1 of Executive Order
8 13526 (50 U.S.C. 435 note; relating to classified na-
9 tional security information)) relating to cyber secu-
10 rity threats or cyber security vulnerabilities under
11 this section without the appropriate security clear-
12 ances.

13 “(2) SECURITY CLEARANCES.—The appropriate
14 Federal agencies or departments shall cooperate
15 with the Secretary or the Commission, to the max-
16 imum extent practicable consistent with applicable
17 procedures and requirements, in expeditiously pro-
18 viding appropriate security clearances to individuals
19 that have a need-to-know (as defined in section 6.1
20 of that Executive Order) classified information to
21 carry out this section.”.

22 **SEC. 3. LIMITED ADDITION OF ERO AUTHORITY FOR CRIT-**
23 **ICAL ELECTRIC INFRASTRUCTURE.**

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

1 (1) in the first sentence—

2 (A) by redesignating subparagraphs (A)
3 and (B) as clauses (i) and (ii), respectively, and
4 indenting appropriately;

5 (B) by striking “(1) The term” and insert-
6 ing the following:

7 “(1) BULK-POWER SYSTEM.—

8 “(A) IN GENERAL.—The term”;

9 (C) in clause (i) (as so redesignated), by
10 striking “and” after the semicolon at the end;

11 (D) in clause (ii) (as so redesignated), by
12 striking the period at the end and inserting “;
13 and”;

14 (E) by adding at the end the following:

15 “(iii) for purposes of section 224, fa-
16 cilities used for the local distribution of
17 electric energy that the Commission deter-
18 mines to be critical electric infrastructure
19 pursuant to section 224.”; and

20 (2) in the second sentence, by striking “The
21 term” and inserting the following:

22 “(B) EXCLUSION.—Except as provided in
23 subparagraph (A), the term”.

1 **SEC. 4. LIMITATION.**

2 Section 215(i) of the Federal Power Act (16 U.S.C.
3 824o(i)) is amended by adding at the end the following:

4 “(6) **LIMITATION.**—The ERO shall have au-
5 thority to develop and enforce compliance with reli-
6 ability standards and temporary emergency orders
7 with respect to a facility used in the local distribu-
8 tion of electric energy only to the extent the Com-
9 mission determines the facility is so vital to the
10 United States that the incapacity or destruction of
11 the facility would have a debilitating impact on na-
12 tional security, national economic security, or na-
13 tional public health or safety.”.

14 **SEC. 5. TEMPORARY EMERGENCY ORDERS FOR CYBER SE-**
15 **CURITY VULNERABILITIES.**

16 Section 215(d) of the Federal Power Act (16 U.S.C.
17 824o(d)) is amended by adding at the end the following:

18 “(7) **TEMPORARY EMERGENCY ORDERS FOR**
19 **CYBER SECURITY VULNERABILITIES.**—Notwith-
20 standing paragraphs (1) through (6), if the Commis-
21 sion determines that immediate action is necessary
22 to protect critical electric infrastructure for a cyber
23 security vulnerability, the Commission may, without
24 prior notice or hearing, after consulting the ERO,
25 require the ERO—

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

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

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

8 “(i) the ERO develops, and the Com-
9 mission approves, a final reliability stand-
10 ard under this section; or

11 “(ii) the Commission authorizes the
12 ERO to withdraw the temporary emer-
13 gency order.”.

14 **SEC. 6. EMP STUDY.**

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

23 (b) CONTENTS.—The report under subsection (a)
24 shall—

1 (1) examine the risk of electromagnetic pulse
2 events and geomagnetic disturbances, using both
3 computer-based simulations and experimental test-
4 ing;

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

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

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

1 **SEC. 7. BUDGETARY EFFECTS.**

2 The budgetary effects of this Act, for the purpose of
3 complying with the Statutory Pay-As-You-Go-Act of 2010,
4 shall be determined by reference to the latest statement
5 titled “Budgetary Effects of PAYGO Legislation” for this
6 Act, submitted for printing in the Congressional Record
7 by the Chairman of the Senate Budget Committee, pro-
8 vided that such statement has been submitted prior to the
9 vote on passage.

Calendar No. 101

112TH CONGRESS
1ST Session

S. 1342

[Report No. 112-34]

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.

JULY 11, 2011

Read twice and placed on the calendar