

113TH CONGRESS
2^D SESSION

S. 2158

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 physical and other threats and vulnerabilities.

IN THE SENATE OF THE UNITED STATES

MARCH 26, 2014

Mr. MARKEY introduced the following bill; which was read twice and referred to the Committee on Energy and Natural Resources

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 physical 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 Reliability and
5 Infrastructure Defense Act” or the “GRID Act”.

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

2 (a) IN GENERAL.—Part II of the Federal Power Act
3 is amended by inserting after section 215 (16 U.S.C.
4 824o) the following:

5 **“SEC. 215A. CRITICAL ELECTRIC INFRASTRUCTURE SECUR-**
6 **RITY.**

7 “(a) DEFINITIONS.—In this section:

8 “(1) BULK-POWER SYSTEM; ELECTRIC RELI-
9 ABILITY ORGANIZATION; REGIONAL ENTITY.—The
10 terms ‘bulk-power system’, ‘Electric Reliability Or-
11 ganization’, and ‘regional entity’ have the meanings
12 given those terms in section 215(a).

13 “(2) DEFENSE CRITICAL ELECTRIC INFRA-
14 STRUCTURE.—The term ‘defense critical electric in-
15 frastructure’ means any infrastructure located in the
16 United States (including the territories) used for the
17 generation, transmission, or distribution of electric
18 energy that—

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

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

25 “(3) DEFENSE CRITICAL ELECTRIC INFRA-
26 STRUCTURE VULNERABILITY.—The term ‘defense

1 critical electric infrastructure vulnerability’ means a
2 weakness in defense critical electric infrastructure
3 that, in the event of—

4 “(A) a malicious act using electronic com-
5 munication or an electromagnetic pulse, would
6 pose a substantial risk of disruption of those
7 electronic devices or communications networks,
8 including hardware, software, and data, that
9 are essential to the reliability of defense critical
10 electric infrastructure; or

11 “(B) a direct physical attack on the de-
12 fense critical electric infrastructure, would pose
13 a substantial risk of significant adverse effects
14 on the reliability of defense critical electric in-
15 frastructure.

16 “(4) ELECTROMAGNETIC PULSE.—The term
17 ‘electromagnetic pulse’ means 1 or more pulses of
18 electromagnetic energy emitted by any device or
19 weapon capable of generating a pulse that would
20 pose a substantial risk of disruption to the operation
21 of those electronic devices or communications net-
22 works, including hardware, software, and data, that
23 are essential to the reliability of systems necessary
24 for the generation, transmission, and distribution of
25 electric energy.

1 “(5) GEOMAGNETIC STORM.—The term ‘geo-
2 magnetic storm’ means a temporary disturbance of
3 the magnetic field of the Earth resulting from solar
4 activity.

5 “(6) GRID SECURITY THREAT.—The term ‘grid
6 security threat’ means a substantial likelihood of—

7 “(A)(i) a malicious act using electronic
8 communication or an electromagnetic pulse, or
9 a geomagnetic storm event, that could disrupt
10 the operation of those electronic devices or com-
11 munications networks, including hardware, soft-
12 ware, and data, that are essential to the reli-
13 ability of the bulk-power system or of defense
14 critical electric infrastructure; and

15 “(ii) disruption of the operation of those
16 devices or networks, with significant adverse ef-
17 fects on the reliability of the bulk-power system
18 or of defense critical electric infrastructure, as
19 a result of the act or event; or

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

23 “(ii) significant adverse effects on the reli-
24 ability of the bulk-power system or of defense

1 critical electric infrastructure as a result of the
2 physical attack.

3 “(7) GRID SECURITY VULNERABILITY.—The
4 term ‘grid security vulnerability’ means a weakness
5 in the bulk power system that, in the event of—

6 “(A) a malicious act using electronic com-
7 munication or an electromagnetic pulse, would
8 pose a substantial risk of disruption to the op-
9 eration of those electronic devices or commu-
10 nications networks, including hardware, soft-
11 ware, and data, that are essential to the reli-
12 ability of the bulk-power system; or

13 “(B) a direct physical attack on the bulk-
14 power system, would pose a substantial risk of
15 significant adverse effects on the reliability of
16 the bulk-power system.

17 “(8) LARGE TRANSFORMER.—The term ‘large
18 transformer’ means an electric transformer that is
19 part of the bulk-power system.

20 “(9) PROTECTED INFORMATION.—The term
21 ‘protected information’ means information, other
22 than classified national security information, des-
23 ignated as protected information by the Commission
24 under subsection (e)(2)—

1 “(A) that was developed or submitted in
2 connection with the implementation of this sec-
3 tion;

4 “(B) that specifically discusses grid secu-
5 rity threats, grid security vulnerabilities, de-
6 fense critical electric infrastructure vulnerabili-
7 ties, or plans, procedures, or measures to ad-
8 dress the threats or vulnerabilities; and

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

13 “(10) SECRETARY.—The term ‘Secretary’
14 means the Secretary of Energy.

15 “(11) SECURITY.—The term ‘security’ does not
16 have the definition of the term provided in section
17 3.

18 “(b) EMERGENCY RESPONSE MEASURES.—

19 “(1) AUTHORITY TO ADDRESS GRID SECURITY
20 THREATS.—

21 “(A) IN GENERAL.—If the President issues
22 and provides to the Commission (either directly
23 or through the Secretary) a written directive or
24 determination identifying an imminent grid se-
25 curity threat, the Commission may, with or

1 without notice, hearing, or report, issue such
2 orders for emergency measures as are necessary
3 in the judgment of the Commission to protect
4 the reliability of the bulk-power system or of
5 defense critical electric infrastructure against
6 the threat.

7 “(B) RULES OF PROCEDURE.—As soon as
8 practicable but not later than 180 days after
9 the date of enactment of this section, the Com-
10 mission shall, after notice and opportunity for
11 comment, establish rules of procedure that en-
12 sure that the authority described in subpara-
13 graph (A) can be exercised expeditiously.

14 “(2) NOTIFICATION OF CONGRESS.—If the
15 President issues and provides to the Commission (ei-
16 ther directly or through the Secretary) a written di-
17 rective or determination under paragraph (1), the
18 President (or the Secretary, as the case may be)
19 shall promptly notify congressional committees of
20 relevant jurisdiction, including the Committee on
21 Energy and Commerce of the House of Representa-
22 tives and the Committee on Energy and Natural Re-
23 sources of the Senate, of the contents of, and jus-
24 tification for, the directive or determination.

1 “(3) CONSULTATION.—Before issuing an order
2 for emergency measures under paragraph (1), the
3 Commission shall, to the extent practicable in light
4 of the nature of the grid security threat and the ur-
5 gency of the need for the emergency measures, con-
6 sult with appropriate governmental authorities in
7 Canada and Mexico, entities described in paragraph
8 (4), the Secretary, and other appropriate Federal
9 agencies regarding implementation of the emergency
10 measures.

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

13 “(A) the Electric Reliability Organization;

14 “(B) a regional entity; or

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

18 “(5) DISCONTINUANCE.—The Commission shall
19 issue an order discontinuing any emergency meas-
20 ures ordered under this subsection, effective not
21 later than 30 days after the earliest of the following:

22 “(A) The date on which the President
23 issues and provides to the Commission (either
24 directly or through the Secretary) a written di-
25 rective or determination that the grid security

1 threat identified under paragraph (1) no longer
2 exists.

3 “(B) The date on which the Commission
4 issues a written determination that the emer-
5 gency measures are no longer needed to address
6 the grid security threat identified under para-
7 graph (1), including by means of Commission
8 approval of a reliability standard under section
9 215 that the Commission determines adequately
10 addresses the threat.

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

13 “(6) COST RECOVERY.—If the Commission de-
14 termines that owners, operators, or users of the
15 bulk-power system or of defense critical electric in-
16 frastructure have incurred substantial costs to com-
17 ply with an order under this subsection and that the
18 costs were prudently incurred and cannot reasonably
19 be recovered through regulated rates or market
20 prices for the electric energy or services sold by the
21 owners, operators, or users, the Commission shall,
22 after notice and an opportunity for comment, estab-
23 lish a mechanism that permits the owners, opera-
24 tors, or users to recover the costs.

1 “(c) MEASURES TO ADDRESS GRID SECURITY
2 VULNERABILITIES.—

3 “(1) COMMISSION AUTHORITY.—

4 “(A) IN GENERAL.—If the Commission, in
5 consultation with appropriate Federal agencies,
6 identifies a grid security vulnerability that the
7 Commission determines has not adequately been
8 addressed through a reliability standard devel-
9 oped and approved under section 215, the Com-
10 mission shall, after notice and opportunity for
11 comment and after consultation with the Sec-
12 retary, other appropriate Federal agencies, and
13 appropriate governmental authorities in Canada
14 and Mexico, promulgate a rule or issue an order
15 requiring implementation, by any owner, oper-
16 ator, or user of the bulk-power system in the
17 United States, of measures to protect the bulk-
18 power system against such vulnerability.

19 “(B) RECOMMENDATIONS.—

20 “(i) IN GENERAL.—Before promul-
21 gating a rule or issuing an order under
22 this paragraph, the Commission shall, to
23 the extent practicable in light of the ur-
24 gency of the need for action to address the
25 grid security vulnerability, request and

1 consider recommendations from the Elec-
2 tric Reliability Organization regarding the
3 rule or order.

4 “(ii) DEADLINE.—The Commission
5 may establish an appropriate deadline for
6 the submission of the recommendations.

7 “(2) CERTAIN EXISTING CYBERSECURITY
8 VULNERABILITIES.—Not later than 180 days after
9 the date of enactment of this section, the Commis-
10 sion shall, after notice and opportunity for comment
11 and after consultation with the Secretary, other ap-
12 propriate Federal agencies, and appropriate govern-
13 mental authorities in Canada and Mexico, promul-
14 gate a rule or issue an order requiring the imple-
15 mentation, by any owner, user, or operator of the
16 bulk-power system in the United States, of such
17 measures as are necessary to protect the bulk-power
18 system against the vulnerabilities identified in the
19 communication entitled ‘Electricity Sector Owners
20 and Operators’, dated June 21, 2007, of the North
21 American Electric Reliability Corporation, acting in
22 the capacity of the Corporation as the Electricity
23 Sector Information and Analysis Center.

24 “(3) RESCISSION.—

1 “(A) IN GENERAL.—The Commission shall
2 approve a reliability standard developed under
3 section 215 that addresses a grid security vul-
4 nerability that is the subject of a rule or order
5 under paragraph (1) or (2), unless the Commis-
6 sion determines that the reliability standard
7 does not adequately protect against the vulner-
8 ability or otherwise does not satisfy the require-
9 ments of section 215.

10 “(B) RESCISSION.—On such approval, the
11 Commission shall rescind the rule promulgated
12 or order issued under paragraph (1) or (2) ad-
13 dressing the vulnerability, effective on the effec-
14 tive date of the newly approved reliability
15 standard.

16 “(4) LARGE TRANSFORMER AVAILABILITY.—

17 “(A) IN GENERAL.—Not later than 1 year
18 after the date of enactment of this section, the
19 Commission shall, after notice and an oppor-
20 tunity for comment and after consultation with
21 the Secretary and other appropriate Federal
22 agencies, issue an order directing the Electric
23 Reliability Organization to submit to the Com-
24 mission for approval under section 215, not
25 later than 1 year after the issuance of the

1 order, reliability standards addressing avail-
2 ability of large transformers.

3 “(B) RESTORATION OF BULK-POWER SYS-
4 TEM.—The standards shall require entities that
5 own or operate large transformers to ensure, in-
6 dividually or jointly, adequate availability of
7 large transformers to promptly restore the reli-
8 able operation of the bulk-power system in the
9 event that any such transformer is destroyed or
10 disabled as a result of a reasonably foreseeable
11 physical or other attack or geomagnetic storm
12 event.

13 “(C) BASIS FOR STANDARDS.—The order
14 of the Commission shall specify the nature and
15 magnitude of the reasonably foreseeable attacks
16 or events that shall provide the basis for the
17 standards.

18 “(D) STANDARDS.—The standards shall—

19 “(i) provide entities subject to the
20 standards with the option of meeting the
21 standards individually or jointly; and

22 “(ii) appropriately balance the risks
23 associated with a reasonably foreseeable
24 attack or event, including—

1 “(I) any regional variation in the
2 risks; and

3 “(II) the costs of ensuring ade-
4 quate availability of spare trans-
5 formers.

6 “(d) CRITICAL DEFENSE FACILITIES.—

7 “(1) DESIGNATION.—

8 “(A) IN GENERAL.—Not later than 180
9 days after the date of enactment of this section,
10 the President shall designate, in a written direc-
11 tive or determination provided to the Commis-
12 sion, facilities located in the United States (in-
13 cluding the territories) that are—

14 “(i) critical to the defense of the
15 United States; and

16 “(ii) vulnerable to a disruption of the
17 supply of electric energy provided to such
18 facility by an external provider.

19 “(B) MAXIMUM NUMBER.—The number of
20 facilities designated by the directive or deter-
21 mination shall not exceed 100.

22 “(C) REVISION.—The President may peri-
23 odically revise the list of designated facilities
24 through a subsequent written directive or deter-
25 mination provided to the Commission, except

1 that the total number of designated facilities at
2 any time shall not exceed 100.

3 “(2) COMMISSION AUTHORITY.—

4 “(A) IN GENERAL.—If the Commission
5 identifies a defense critical electric infrastruc-
6 ture vulnerability that the Commission, in con-
7 sultation with owners and operators of any 1 or
8 more facilities designated by the President pur-
9 suant to paragraph (1), determines has not
10 adequately been addressed through measures
11 undertaken by owners or operators of defense
12 critical electric infrastructure, the Commission
13 shall, after notice and an opportunity for com-
14 ment and after consultation with the Secretary
15 and other appropriate Federal agencies, pro-
16 mulgate a rule or issue an order requiring im-
17 plementation, by any owner or operator of de-
18 fense critical electric infrastructure, of meas-
19 ures to protect the defense critical electric in-
20 frastructure against the vulnerability.

21 “(B) EXEMPTIONS.—

22 “(i) IN GENERAL.—The Commission
23 shall exempt from any rule or order pro-
24 mulgated under subparagraph (A) any spe-
25 cific defense critical electric infrastructure

1 that the Commission determines already
2 has been adequately protected against the
3 identified vulnerability.

4 “(ii) CONSULTATION.—The Commis-
5 sion shall make any determination under
6 clause (i) in consultation with the owner or
7 operator of the facility designated by the
8 President pursuant to paragraph (1) that
9 relies on the defense critical electric infra-
10 structure.

11 “(3) COST RECOVERY.—An owner or operator
12 of defense critical electric infrastructure shall be re-
13 quired to take measures under paragraph (2) only to
14 the extent that the owners or operators of 1 or more
15 facilities designated by the President pursuant to
16 paragraph (1) that rely on the infrastructure agree
17 to bear the full incremental costs of compliance with
18 a rule promulgated or order issued under paragraph
19 (2).

20 “(e) PROTECTION OF INFORMATION.—

21 “(1) PROHIBITION OF PUBLIC DISCLOSURE OF
22 PROTECTED INFORMATION.—Protected informa-
23 tion—

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

4 “(B) shall not be made available pursuant
5 to any State, local, or tribal law requiring dis-
6 closure of information or records.

7 “(2) INFORMATION SHARING.—

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

15 “(B) SHARING OF PROTECTED INFORMA-
16 TION.—

17 “(i) IN GENERAL.—The regulations
18 promulgated and orders issued pursuant to
19 subparagraph (A) shall provide standards
20 for and facilitate the appropriate sharing
21 of protected information with, between,
22 and by Federal, State, local, and tribal au-
23 thorities, the Electric Reliability Organiza-
24 tion, regional entities, and owners, opera-
25 tors, and users of the bulk-power system in

1 the United States and of defense critical
2 electric infrastructure.

3 “(ii) STATE COMMISSIONS.—In pro-
4 mulgating the regulations and issuing the
5 orders, the Commission shall take account
6 of the role of State commissions in review-
7 ing the prudence and cost of investments
8 within the respective jurisdictions of the
9 State commissions.

10 “(iii) CANADA AND MEXICO.—The
11 Commission shall consult with appropriate
12 Canadian and Mexican authorities to de-
13 velop protocols for the sharing of protected
14 information with, between, and by appro-
15 priate Canadian and Mexican authorities
16 and owners, operators, and users of the
17 bulk-power system outside the United
18 States.

19 “(3) SUBMISSION OF INFORMATION TO CON-
20 GRESS.—Nothing in this section permits or author-
21 izes the withholding of information from Congress,
22 any committee or subcommittee of Congress, or the
23 Comptroller General of the United States.

24 “(4) DISCLOSURE OF NONPROTECTED INFOR-
25 MATION.—

1 “(A) IN GENERAL.—In implementing this
2 section, the Commission shall protect from dis-
3 closure only the minimum quantity of informa-
4 tion necessary to protect the reliability of the
5 bulk-power system and of defense critical elec-
6 tric infrastructure.

7 “(B) SEGREGATION OF PROTECTED INFOR-
8 MATION.—The Commission shall segregate pro-
9 tected information within documents and elec-
10 tronic communications, whenever feasible, to fa-
11 cilitate disclosure of information that is not des-
12 ignated as protected information.

13 “(5) DURATION OF DESIGNATION.—Informa-
14 tion may not be designated as protected information
15 for longer than 5 years, unless specifically redesign-
16 ated by the Commission.

17 “(6) REMOVAL OF DESIGNATION.—The Com-
18 mission may remove the designation of protected in-
19 formation, in whole or in part, from a document or
20 electronic communication if the unauthorized disclo-
21 sure of the information could no longer be used to
22 impair the reliability of the bulk-power system or of
23 defense critical electric infrastructure.

24 “(7) JUDICIAL REVIEW OF DESIGNATIONS.—

1 “(A) IN GENERAL.—Notwithstanding sub-
2 section (f) or section 313, a person or entity
3 may seek judicial review of a determination by
4 the Commission concerning the designation of
5 protected information under this subsection ex-
6 clusively in the district court of the United
7 States in the district in which the complainant
8 resides, or has a principal place of business, or
9 in the District of Columbia.

10 “(B) PROCEDURE.—In a case described in
11 subparagraph (A), the court—

12 “(i) shall determine the matter de
13 novo; and

14 “(ii) may examine the contents of doc-
15 uments or electronic communications des-
16 igned as protected information in camera
17 to determine whether the documents or
18 any part of the documents were improperly
19 designated as protected information.

20 “(C) BURDEN OF PROOF.—The burden
21 shall be on the Commission to sustain the des-
22 ignation of the Commission.

23 “(f) JUDICIAL REVIEW.—

24 “(1) IN GENERAL.—The Commission shall act
25 expeditiously to resolve all applications for rehearing

1 of orders issued pursuant to this section that are
2 filed under section 313(a).

3 “(2) JURISDICTION.—Any party seeking judi-
4 cial review pursuant to section 313 of an order
5 issued under this section may obtain the review only
6 in the United States Court of Appeals for the Dis-
7 trict of Columbia Circuit.

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

10 “(1) EXPERTISE AND RESOURCES.—

11 “(A) IN GENERAL.—The Secretary shall
12 establish a program, in consultation with other
13 appropriate Federal agencies, to develop tech-
14 nical expertise in the protection of systems for
15 the generation, transmission, and distribution
16 of electric energy against geomagnetic storms
17 or malicious acts using electronic communica-
18 tions or electromagnetic pulse that would pose
19 a substantial risk of disruption to the operation
20 of those electronic devices or communications
21 networks, including hardware, software, and
22 data, that are essential to the reliability of the
23 systems.

24 “(B) RESOURCES.—The program shall in-
25 clude the identification and development of ap-

1 appropriate technical and electronic resources, in-
2 cluding hardware, software, and system equip-
3 ment.

4 “(2) SHARING EXPERTISE.—

5 “(A) IN GENERAL.—As appropriate, the
6 Secretary shall offer to share technical expertise
7 developed under the program under paragraph
8 (1), through consultation and assistance, with
9 owners, operators, or users of systems for the
10 generation, transmission, or distribution of elec-
11 tric energy located in the United States and
12 with State commissions.

13 “(B) PRIORITY.—In offering the support,
14 the Secretary shall assign higher priority to sys-
15 tems serving facilities designated by the Presi-
16 dent pursuant to subsection (d)(1) and other
17 critical-infrastructure facilities, which the Sec-
18 retary shall identify in consultation with the
19 Commission and other appropriate Federal
20 agencies.

21 “(3) SECURITY CLEARANCES AND COMMUNICA-
22 TION.—

23 “(A) IN GENERAL.—The Secretary shall
24 facilitate and, to the extent practicable, expedite
25 the acquisition of adequate security clearances

1 by key personnel of any entity subject to the re-
2 quirements of this section to enable optimum
3 communication with Federal agencies regarding
4 grid security threats, grid security vulnerabili-
5 ties, and defense critical electric infrastructure
6 vulnerabilities.

7 “(B) ACTIONABLE INFORMATION.—The
8 Secretary, the Commission, and other appro-
9 priate Federal agencies shall, to the extent
10 practicable and consistent with their obligations
11 to protect classified and protected information,
12 share timely actionable information regarding
13 grid security threats, grid security vulnerabili-
14 ties, and defense critical electric infrastructure
15 vulnerabilities with appropriate key personnel of
16 owners, operators, and users of the bulk-power
17 system and of defense critical electric infra-
18 structure.

19 “(h) CERTAIN FEDERAL ENTITIES.—During the 11-
20 year period beginning on the date of enactment of this
21 section, the Tennessee Valley Authority and the Bonneville
22 Power Administration shall be exempt from any require-
23 ment under subsection (b) or (c) (except for any require-
24 ment addressing a malicious act using electronic commu-
25 nication).”.

1 (b) CONFORMING AMENDMENTS.—

2 (1) JURISDICTION.—Section 201(b)(2) of the
3 Federal Power Act (16 U.S.C. 824(b)(2)) is amend-
4 ed by inserting “215A,” after “215,” each place it
5 appears.

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

○