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”.


SEC. 2. CRITICAL ELECTRIC INFRASTRUCTURE SECURITY.

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

“SEC. 215A. CRITICAL ELECTRIC INFRASTRUCTURE SECURITY.

“(a) DEFINITIONS.—In this section:

“(1) BULK-POWER SYSTEM; ELECTRIC RELIABILITY ORGANIZATION; REGIONAL ENTITY.—The terms ‘bulk-power system’, ‘Electric Reliability Organization’, and ‘regional entity’ have the meanings given those terms in section 215(a).

“(2) DEFENSE CRITICAL ELECTRIC INFRASTRUCTURE.—The term ‘defense critical electric infrastructure’ means any infrastructure located in the United States (including the territories) used for the generation, transmission, or distribution of electric energy that—

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

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

“(3) DEFENSE CRITICAL ELECTRIC INFRASTRUCTURE VULNERABILITY.—The term ‘defense
critical electric infrastructure vulnerability’ means a weakness in defense critical electric infrastructure that, in the event of—

“(A) a malicious act using electronic communication or an electromagnetic pulse, would pose a substantial risk of disruption of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of defense critical electric infrastructure; or

“(B) a direct physical attack on the defense critical electric infrastructure, would pose a substantial risk of significant adverse effects on the reliability of defense critical electric infrastructure.

“(4) ELECTROMAGNETIC PULSE.—The term ‘electromagnetic pulse’ means 1 or more pulses of electromagnetic energy emitted by any device or weapon capable of generating a pulse that would pose a substantial risk of disruption to the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of systems necessary for the generation, transmission, and distribution of electric energy.
“(5) GEOMAGNETIC STORM.—The term ‘geomagnetic storm’ means a temporary disturbance of the magnetic field of the Earth resulting from solar activity.

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

“(A)(i) a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of the bulk-power system or of defense critical electric infrastructure; and

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

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

“(ii) significant adverse effects on the reliability of the bulk-power system or of defense
critical electric infrastructure as a result of the physical attack.

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

“(A) a malicious act using electronic communication or an electromagnetic pulse, would pose a substantial risk of disruption to the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of the bulk-power system; or

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

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

“(9) PROTECTED INFORMATION.—The term ‘protected information’ means information, other than classified national security information, designated as protected information by the Commission under subsection (e)(2)—
“(A) that was developed or submitted in connection with the implementation of this section;

“(B) that specifically discusses grid security threats, grid security vulnerabilities, defense critical electric infrastructure vulnerabilities, or plans, procedures, or measures to address the threats or vulnerabilities; and

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

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

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

“(b) EMERGENCY RESPONSE MEASURES.—

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

“(A) IN GENERAL.—If the President issues and provides to the Commission (either directly or through the Secretary) a written directive or determination identifying an imminent grid security threat, the Commission may, with or
without notice, hearing, or report, issue such
orders for emergency measures as are necessary
in the judgment of the Commission to protect
the reliability of the bulk-power system or of
defense critical electric infrastructure against
the threat.

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

“(2) Notification of Congress.—If the
President issues and provides to the Commission (ei-
ther directly or through the Secretary) a written di-
rective or determination under paragraph (1), the
President (or the Secretary, as the case may be)
shall promptly notify congressional committees of
relevant jurisdiction, including the Committee on
Energy and Commerce of the House of Representa-
tives and the Committee on Energy and Natural Re-
sources of the Senate, of the contents of, and jus-
tification for, the directive or determination.
“(3) CONSULTATION.—Before issuing an order for emergency measures under paragraph (1), the Commission shall, to the extent practicable in light of the nature of the grid security threat and the urgency of the need for the emergency measures, consult with appropriate governmental authorities in Canada and Mexico, entities described in paragraph (4), the Secretary, and other appropriate Federal agencies regarding implementation of the emergency measures.

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

“(A) the Electric Reliability Organization;

“(B) a regional entity; or

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

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

“(A) The date on which the President issues and provides to the Commission (either directly or through the Secretary) a written directive or determination that the grid security
threat identified under paragraph (1) no longer exists.

“(B) The date on which the Commission issues a written determination that the emergency measures are no longer needed to address the grid security threat identified under paragraph (1), including by means of Commission approval of a reliability standard under section 215 that the Commission determines adequately addresses the threat.

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

“(6) COST RECOVERY.—If the Commission determines that owners, operators, or users of the bulk-power system or of defense critical electric infrastructure have incurred substantial costs to comply with an order under this subsection and that the costs were prudently incurred and cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by the owners, operators, or users, the Commission shall, after notice and an opportunity for comment, establish a mechanism that permits the owners, operators, or users to recover the costs.
“(c) MEASURES TO ADDRESS GRID SECURITY VULNERABILITIES.—

“(1) COMMISSION AUTHORITY.—

“(A) IN GENERAL.—If the Commission, in consultation with appropriate Federal agencies, identifies a grid security vulnerability that the Commission determines has not adequately been addressed through a reliability standard developed and approved under section 215, the Commission shall, after notice and opportunity for comment and after consultation with the Secretary, other appropriate Federal agencies, and appropriate governmental authorities in Canada and Mexico, promulgate a rule or issue an order requiring implementation, by any owner, operator, or user of the bulk-power system in the United States, of measures to protect the bulk-power system against such vulnerability.

“(B) RECOMMENDATIONS.—

“(i) IN GENERAL.—Before promulgating a rule or issuing an order under this paragraph, the Commission shall, to the extent practicable in light of the urgency of the need for action to address the grid security vulnerability, request and
consider recommendations from the Electric Reliability Organization regarding the rule or order.

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

“(2) CERTAIN EXISTING CYBERSECURITY VULNERABILITIES.—Not later than 180 days after the date of enactment of this section, the Commission shall, after notice and opportunity for comment and after consultation with the Secretary, other appropriate Federal agencies, and appropriate governmental authorities in Canada and Mexico, promulgate a rule or issue an order requiring the implementation, by any owner, user, or operator of the bulk-power system in the United States, of such measures as are necessary to protect the bulk-power system against the vulnerabilities identified in the communication entitled ‘Electricity Sector Owners and Operators’, dated June 21, 2007, of the North American Electric Reliability Corporation, acting in the capacity of the Corporation as the Electricity Sector Information and Analysis Center.

“(3) RESCISSION.—
“(A) IN GENERAL.—The Commission shall approve a reliability standard developed under section 215 that addresses a grid security vulnerability that is the subject of a rule or order under paragraph (1) or (2), unless the Commission determines that the reliability standard does not adequately protect against the vulnerability or otherwise does not satisfy the requirements of section 215.

“(B) RESCISSION.—On such approval, the Commission shall rescind the rule promulgated or order issued under paragraph (1) or (2) addressing the vulnerability, effective on the effective date of the newly approved reliability standard.

“(4) LARGE TRANSFORMER AVAILABILITY.—

“(A) IN GENERAL.—Not later than 1 year after the date of enactment of this section, the Commission shall, after notice and an opportunity for comment and after consultation with the Secretary and other appropriate Federal agencies, issue an order directing the Electric Reliability Organization to submit to the Commission for approval under section 215, not later than 1 year after the issuance of the
order, reliability standards addressing availability of large transformers.

“(B) Restoration of bulk-power system.—The standards shall require entities that own or operate large transformers to ensure, individually or jointly, adequate availability of large transformers to promptly restore the reliable operation of the bulk-power system in the event that any such transformer is destroyed or disabled as a result of a reasonably foreseeable physical or other attack or geomagnetic storm event.

“(C) Basis for standards.—The order of the Commission shall specify the nature and magnitude of the reasonably foreseeable attacks or events that shall provide the basis for the standards.

“(D) Standards.—The standards shall—

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

“(ii) appropriately balance the risks associated with a reasonably foreseeable attack or event, including—
“(I) any regional variation in the risks; and

“(II) the costs of ensuring adequate availability of spare transformers.

“(d) CRITICAL DEFENSE FACILITIES.—

“(1) Designation.—

“(A) In general.—Not later than 180 days after the date of enactment of this section, the President shall designate, in a written directive or determination provided to the Commission, facilities located in the United States (including the territories) that are—

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

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

“(B) Maximum number.—The number of facilities designated by the directive or determination shall not exceed 100.

“(C) Revision.—The President may periodically revise the list of designated facilities through a subsequent written directive or determination provided to the Commission, except
that the total number of designated facilities at
any time shall not exceed 100.

“(2) COMMISSION AUTHORITY.—

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

“(B) EXEMPTIONS.—

“(i) IN GENERAL.—The Commission
shall exempt from any rule or order pro-
mulgated under subparagraph (A) any spe-
cific defense critical electric infrastructure
that the Commission determines already
has been adequately protected against the
identified vulnerability.

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

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

“(e) PROTECTION OF INFORMATION.—

“(1) PROHIBITION OF PUBLIC DISCLOSURE OF
protected information.—Protected informa-
—
“(A) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and

“(B) shall not be made available pursuant to any State, local, or tribal law requiring disclosure of information or records.

“(2) INFORMATION SHARING.—

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

“(B) SHARING OF PROTECTED INFORMATION.—

“(i) IN GENERAL.—The regulations promulgated and orders issued pursuant to subparagraph (A) shall provide standards for and facilitate the appropriate sharing of protected information with, between, and by Federal, State, local, and tribal authorities, the Electric Reliability Organization, regional entities, and owners, operators, and users of the bulk-power system in
the United States and of defense critical
electric infrastructure.

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

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

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

“(4) DISCLOSURE OF NONPROTECTED INFOR-
MATION.—
“(A) IN GENERAL.—In implementing this section, the Commission shall protect from disclosure only the minimum quantity of information necessary to protect the reliability of the bulk-power system and of defense critical electric infrastructure.

“(B) SEGREGATION OF PROTECTED INFORMATION.—The Commission shall segregate protected information within documents and electronic communications, whenever feasible, to facilitate disclosure of information that is not designated as protected information.

“(5) DURATION OF DESIGNATION.—Information may not be designated as protected information for longer than 5 years, unless specifically redesignated by the Commission.

“(6) REMOVAL OF DESIGNATION.—The Commission may remove the designation of protected information, in whole or in part, from a document or electronic communication if the unauthorized disclosure of the information could no longer be used to impair the reliability of the bulk-power system or of defense critical electric infrastructure.

“(7) JUDICIAL REVIEW OF DESIGNATIONS.—
“(A) IN GENERAL.—Notwithstanding subsection (f) or section 313, a person or entity may seek judicial review of a determination by the Commission concerning the designation of protected information under this subsection exclusively in the district court of the United States in the district in which the complainant resides, or has a principal place of business, or in the District of Columbia.

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

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

“(ii) may examine the contents of documents or electronic communications designated as protected information in camera to determine whether the documents or any part of the documents were improperly designated as protected information.

“(C) BURDEN OF PROOF.—The burden shall be on the Commission to sustain the designation of the Commission.

“(f) JUDICIAL REVIEW.—

“(1) IN GENERAL.—The Commission shall act expeditiously to resolve all applications for rehearing
of orders issued pursuant to this section that are
filed under section 313(a).

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

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

“(1) EXPERTISE AND RESOURCES.—

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

“(B) RESOURCES.—The program shall in-
clude the identification and development of ap-
propriate technical and electronic resources, including hardware, software, and system equipment.

“(2) SHARING EXPERTISE.—

“(A) IN GENERAL.—As appropriate, the Secretary shall offer to share technical expertise developed under the program under paragraph (1), through consultation and assistance, with owners, operators, or users of systems for the generation, transmission, or distribution of electric energy located in the United States and with State commissions.

“(B) PRIORITY.—In offering the support, the Secretary shall assign higher priority to systems serving facilities designated by the President pursuant to subsection (d)(1) and other critical-infrastructure facilities, which the Secretary shall identify in consultation with the Commission and other appropriate Federal agencies.

“(3) SECURITY CLEARANCES AND COMMUNICATION.—

“(A) IN GENERAL.—The Secretary shall facilitate and, to the extent practicable, expedite the acquisition of adequate security clearances
by key personnel of any entity subject to the requirements of this section to enable optimum communication with Federal agencies regarding grid security threats, grid security vulnerabilities, and defense critical electric infrastructure vulnerabilities.

“(B) ACTIONABLE INFORMATION.—The Secretary, the Commission, and other appropriate Federal agencies shall, to the extent practicable and consistent with their obligations to protect classified and protected information, share timely actionable information regarding grid security threats, grid security vulnerabilities, and defense critical electric infrastructure vulnerabilities with appropriate key personnel of owners, operators, and users of the bulk-power system and of defense critical electric infrastructure.

“(h) CERTAIN FEDERAL ENTITIES.—During the 11-year period beginning on the date of enactment of this section, the Tennessee Valley Authority and the Bonneville Power Administration shall be exempt from any requirement under subsection (b) or (e) (except for any requirement addressing a malicious act using electronic communication).”
(b) CONFORMING AMENDMENTS.—

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

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