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, physical, and other threats and vulnerabilities.

IN THE HOUSE OF REPRESENTATIVES

MARCH 26, 2014

Mr. WAXMAN introduced the following bill; which was referred to the Committee on Energy and Commerce

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

4 SEC. 2. AMENDMENT TO THE FEDERAL POWER ACT.

5 (a) CRITICAL ELECTRIC INFRASTRUCTURE SECURITY.—Part II of the Federal Power Act (16 U.S.C. 824
et seq.) is amended by adding after section 215 the follow-  
ina new section:
  
“SEC. 215A. CRITICAL ELECTRIC INFRASTRUCTURE SECU-  
RITY.
  
“(a) DEFINITIONS.—For purposes of this section:
  
“(1) BULK-POWER SYSTEM; ELECTRIC RELIABILITY ORGANIZATION; REGIONAL ENTITY.—The terms ‘bulk-power system’, ‘Electric Reliability Organiza- 

tion’, and ‘regional entity’ have the meanings given such terms in paragraphs (1), (2), and (7) of section 215(a), respectively.
  
“(2) DEFENSE CRITICAL ELECTRIC INFRA- 

STRUCTURE.—The term ‘defense critical electric infra- 

structure’ 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 such facility.
  
“(3) DEFENSE CRITICAL ELECTRIC INFRA- 

STRUCTURE 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 com-
munication 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 defense
critical electric infrastructure, would pose a
substantial risk of significant adverse effects on
the reliability of defense critical electric infra-
structure.

“(4) ELECTROMAGNETIC PULSE.—The term
‘electromagnetic pulse’ means 1 or more pulses of
electromagnetic energy, emitted by any device or
weapon capable of generating such a pulse, that
would pose a substantial risk of disruption to the op-
eration of those electronic devices or communications
networks, including hardware, software, and data,
that are essential to the reliability of systems nec-
essary for the generation, transmission, and dis-
tribution of electric energy.
“(5) GEOMAGNETIC STORM.—The term ‘geomagnetic storm’ means a temporary disturbance of the Earth’s magnetic field 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 such 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 such 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 such 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 such 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 definition of ‘security’ in section 3(16) shall not apply to the provisions in this section.

“(b) EMERGENCY RESPONSE MEASURES.—

“(1) AUTHORITY TO ADDRESS GRID SECURITY THREATS.—Whenever 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 its judgment to protect the reli-
ability of the bulk-power system or of defense critical
electric infrastructure against such threat. As soon
as practicable but not later than 180 days after the
date of enactment of this section, the Commission
shall, after notice and opportunity for comment, es-
establish rules of procedure that ensure that such au-
thority can be exercised expeditiously.

“(2) Notification of Congress.—Whenever
the President issues and provides to the Commission
(either directly or through the Secretary) a written
directive 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, such 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 ur-
gency of the need for such emergency measures, con-
result with appropriate governmental authorities in Canada and Mexico, entities described in paragraph (4), the Secretary, and other appropriate Federal agencies regarding implementation of such 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 upon 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 upon which the Commission issues a written determination that the emergency measures are no longer needed to address
the grid security threat identified under para-
graph (1), including by means of Commission
approval of a reliability standard under section
215 that the Commission determines adequately
addresses such threat.

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

“(6) COST RECOVERY.—If the Commission de-
determines that owners, operators, or users of the
bulk-power system or of defense critical electric in-
frastructure have incurred substantial costs to com-
ply with an order under this subsection and that
such costs were prudently incurred and cannot rea-
sonably be recovered through regulated rates or
market prices for the electric energy or services sold
by such owners, operators, or users, the Commission
shall, after notice and an opportunity for comment,
establish a mechanism that permits such owners, op-
erators, or users to recover such costs.

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

“(1) COMMISSION AUTHORITY.—If the Commiss-
ion, in consultation with appropriate Federal agen-
cies, identifies a grid security vulnerability that the
Commission determines has not adequately been ad-
dressed 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 au-
thorities 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. Before pro-
mulgating a rule or issuing an order under this
paragraph, the Commission shall, to the extent prac-
ticable in light of the urgency of the need for action
to address the grid security vulnerability, request
and consider recommendations from the Electric Re-
liability Organization regarding such rule or order.
The Commission may establish an appropriate dead-
line for the submission of such recommendations.

“(2) CERTAIN EXISTING CYBERSECURITY
VULNERABILITIES.—Not later than 180 days after
the date of enactment of this section, the Commiss-
ion shall, after notice and opportunity for comment
and after consultation with the Secretary, other ap-
propriate Federal agencies, and appropriate govern-
mental authorities in Canada and Mexico, promul-
gate a rule or issue an order requiring the implement-
ment, 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 June 21, 2007, communication to certain ‘Electricity Sector Owners and Operators’ from the North American Electric Reliability Corporation, acting in its capacity as the Electricity Sector Information and Analysis Center.

“(3) RESCISSION.—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 such reliability standard does not adequately protect against such vulnerability or otherwise does not satisfy the requirements of section 215. Upon such approval, the Commission shall rescind the rule promulgated or order issued under paragraph (1) or (2) addressing such vulnerability, effective upon the effective date of the newly approved reliability standard.

“(4) LARGE TRANSFORMER AVAILABILITY.—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 consulta-
tion with the Secretary and other appropriate Fed-
eral agencies, issue an order directing the Electric
Reliability Organization to submit to the Commiss-
ion for approval under section 215, not later than
1 year after the issuance of such order, reliability
standards addressing availability of large trans-
formers. Such standards shall require entities that
own or operate large transformers to ensure, individ-
ually or jointly, adequate availability of large trans-
formers 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. The Commission’s order
shall specify the nature and magnitude of the rea-
sonably foreseeable attacks or events that shall pro-
vide the basis for such standards. Such standards
shall—

“(A) provide entities subject to the stand-
ards with the option of meeting such standards
individually or jointly; and

“(B) appropriately balance the risks asso-
ciated with a reasonably foreseeable attack or
event, including any regional variation in such
risks, and the costs of ensuring adequate avail-
ability of spare transformers.

“(d) CRITICAL DEFENSE FACILITIES.—

“(1) DESIGNATION.—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 terri-
tories) that are—

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

“(B) vulnerable to a disruption of the sup-
ply of electric energy provided to such facility
by an external provider.

The number of facilities designated by such directive
or determination shall not exceed 100. The Presi-
dent may periodically revise the list of designated fa-
cilities through a subsequent written directive or de-
termination provided to the Commission, provided
that the total number of designated facilities at any
time shall not exceed 100.

“(2) COMMISSION AUTHORITY.—If the Commiss-
ion identifies a defense critical electric infrastruk-
ture vulnerability that the Commission, in consultati-
tion with owners and operators of any facility or fa-
cilities designated by the President pursuant to
paragraph (1), determines has not adequately been
addressed through measures undertaken by owners
or operators of defense critical electric infrastruc-
ture, the Commission shall, after notice and an op-
portunity for comment and after consultation with
the Secretary and other appropriate Federal agen-
cies, promulgate a rule or issue an order requiring
implementation, by any owner or operator of defense
critical electric infrastructure, of measures to protect
the defense critical electric infrastructure against
such vulnerability. The Commission shall exempt
from any such rule or order any specific defense
critical electric infrastructure that the Commission
determines already has been adequately protected
against the identified vulnerability. The Commission
shall make any such determination in consultation
with the owner or operator of the facility designated
by the President pursuant to paragraph (1) that re-
lies upon such defense critical electric infrastructure.

“(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 a facility
or facilities designated by the President pursuant to paragraph (1) that rely upon such 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 information—

“(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 such protected information.

“(B) Sharing of protected information.—The regulations promulgate and orders
issued pursuant to subparagraph (A) shall pro-
vide standards for and facilitate the appropriate
sharing of protected information with, between,
and by Federal, State, local, and tribal authori-
ties, the Electric Reliability Organization, re-
gional entities, and owners, operators, and
users of the bulk-power system in the United
States and of defense critical electric infrastruc-
ture. In promulgating such regulations and
issuing such orders, the Commission shall take
account of the role of State commissions in re-
viewing the prudence and cost of investments
within their respective jurisdictions. The Com-
mission shall consult with appropriate Canadian
and Mexican authorities to develop protocols for
the sharing of protected information with, be-
tween, and by appropriate Canadian and Mexi-
can 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 shall permit or au-
thorize the withholding of information from Con-
gress, any committee or subcommittee thereof, or
the Comptroller General.
“(4) Disclosure of non-protected information.—In implementing this section, the Commission shall protect from disclosure only the minimum amount of information necessary to protect the reliability of the bulk-power system and of defense critical electric infrastructure. The Commission shall segregate protected information within documents and electronic communications, wherever 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 such 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.—Notwithstanding subsection (f) of this section 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 his principal place of business, or in the District of Columbia. In such a case the court shall determine the matter de novo, and may examine the contents of documents or electronic communications designated as protected information in camera to determine whether such documents or any part thereof were improperly designated as protected information. The burden is on the Commission to sustain its designation.

“(f) Judicial Review.—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). Any party seeking judicial review pursuant to section 313 of an order issued under this section may obtain such review only in the United States Court of Appeals for the District of Columbia Circuit.

“(g) Provision of Assistance to Industry in Meeting Grid Security Protection Needs.—

“(1) Expertise and Resources.—The Secretary shall establish a program, in consultation with other appropriate Federal agencies, to develop technical expertise in the protection of systems for the
generation, transmission, and distribution of electric energy against geomagnetic storms or malicious acts using electronic communications 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 such systems. Such program shall include the identification and development of appropriate technical and electronic resources, including hardware, software, and system equipment.

“(2) SHARING EXPERTISE.—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. In offering such 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.—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. 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.—For the 11-year period commencing 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 (c) (except for any require-
ment 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,”.