

111TH CONGRESS
1ST SESSION

H. R. 2195

To amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 30, 2009

Mr. THOMPSON of Mississippi (for himself, Mr. KING of New York, Ms. CLARKE, Mr. DANIEL E. LUNGREN of California, Ms. JACKSON-LEE of Texas, Ms. LORETTA SANCHEZ of California, Ms. HARMAN, Mr. CUELLAR, Mr. CARNEY, Ms. ZOE LOFGREN of California, Mr. PASCRELL, Mr. LUJÁN, and Mr. LANGEVIN) introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committee on Homeland Security, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack, and for other purposes.

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. CRITICAL ELECTRIC INFRASTRUCTURE.**

4 (a) FINDINGS.—

5 (1) The critical electric infrastructure of the
6 United States and Canada has more than \$1 trillion

1 in asset value, more than 200,000 miles of trans-
2 mission lines, and more than 800,000 megawatts of
3 generating capability, serving over 300 million peo-
4 ple.

5 (2) The effective functioning of this infrastruc-
6 ture is highly dependent on computer-based control
7 systems that are used to monitor and manage sen-
8 sitive processes and physical functions.

9 (3) These control systems are becoming increas-
10 ingly connected to open networks, such as corporate
11 intranets and the Internet. According to the Depart-
12 ment of Homeland Security's United States Com-
13 puter Emergency Readiness Team ("US-CERT"),
14 this transition towards widely used technologies and
15 open connectivity exposes control systems to the
16 ever-present cyber risks that exist in the information
17 technology world in addition to control system spe-
18 cific risks.

19 (4) Malicious actors pose a significant risk to
20 this infrastructure. The Federal Bureau of Inves-
21 tigation ("FBI") has identified multiple sources of
22 threats, including foreign nation states, domestic
23 criminals and hackers, and disgruntled employees.

24 (5) Intentional or naturally occurring Electro-
25 magnetic Pulse ("EMP") events also threaten crit-

1 ical electric infrastructure. The Commission to As-
2 sess the Threat to the United States from EMP At-
3 tack reported in 2008 that an EMP attack could
4 cause significant damage or disruption to critical
5 electric infrastructure and other critical infrastruc-
6 ture due to the widespread use of Supervisory Con-
7 trol and Data Acquisition (“SCADA”) systems. The
8 National Academy of Sciences also reported in 2008
9 that Severe Space Weather Events could produce
10 similar results.

11 (6) The Department of Homeland Security’s
12 Control Systems Security Program is designed to in-
13 crease the reliability, security, and resilience of con-
14 trol systems to guard against and enhance domestic
15 preparedness for and collective response to a cyber
16 attack by a terrorist or other person. This is done
17 by developing voluntary cyber risk reduction prod-
18 ucts, supporting the Department of Homeland Secu-
19 rity’s Industrial Control Systems Computer Emer-
20 gency Response Team (“ICS-CERT”) in developing
21 vulnerability mitigation recommendations and strate-
22 gies, and coordinating and leveraging activities for
23 improving the Nation’s critical infrastructure secu-
24 rity posture.

1 (7) According to recent news reports, the elec-
2 tronic control systems of the electrical system in the
3 United States have been routinely penetrated and
4 compromised. According to current and former na-
5 tional security officials, cyber spies from China, Rus-
6 sia, and other countries have penetrated the United
7 States electrical system in order to map the system,
8 and have left behind software programs that could
9 be used to disrupt and disable the system.

10 (8) In the interest of national security, and to
11 enhance domestic preparedness for and collective re-
12 sponse to a cyber attack by a terrorist or other per-
13 son, a statutory mechanism is necessary to protect
14 the critical electric infrastructure against cyber
15 threats.

16 (9) In spite of existing mandatory cybersecurity
17 standards, a report from the North American Elec-
18 tric Reliability Corporation (“NERC”) suggests that
19 many utilities are underreporting their assets, poten-
20 tially to avoid compliance requirements. In April
21 2009, NERC reported that only 23 percent of re-
22 sponding utilities identified a “Critical Cyber Asset”
23 as required by NERC Reliability Standard 002–1.
24 According to NERC, the results of this survey sug-
25 gest that utilities may not have identified certain

1 qualifying assets as “Critical”. NERC requested
2 that entities take a fresh, comprehensive look at
3 their methodology in order to identify and secure
4 more Critical Cyber Assets.

5 (10) On May 21, 2008, in testimony before the
6 House Committee on Homeland Security, Joseph
7 Kelliher, then-Chairman of the Federal Energy Reg-
8 ulatory Commission (“the Commission”), stated that
9 his agency is in need of additional legal authorities
10 to adequately protect the electric power system
11 against cyber attack.

12 (b) RESEARCH ON CYBER COMPROMISE OF CRITICAL
13 ELECTRIC INFRASTRUCTURE.—(1) Pursuant to section
14 201 of the Homeland Security Act of 2002 (6 U.S.C. 121)
15 and in furtherance of domestic preparedness for and col-
16 lective response to a cyber attack by a terrorist or other
17 person, the Secretary of Homeland Security, working with
18 other national security and intelligence agencies, shall con-
19 duct research and determine if the security of federally
20 owned programmable electronic devices and communica-
21 tion networks (including hardware, software, and data) es-
22 sential to the reliable operation of critical electric infra-
23 structure have been compromised.

24 (2) The scope of the research referred to in para-
25 graph (1) shall include: the extent of compromise, identi-

1 fication of attackers, the method of penetration, ramifica-
2 tions of the compromise on future operations of critical
3 electric infrastructure, secondary ramifications of the com-
4 promise on other critical infrastructure sectors and the
5 functioning of civil society, ramifications of compromise
6 on national security, including war fighting capability, and
7 recommended mitigation activities.

8 (3) The Secretary of Homeland Security shall report
9 the findings to the appropriate committees of Congress,
10 including the Committee on Homeland Security of the
11 House of Representatives and the Homeland Security and
12 Governmental Affairs Committee of the Senate. The re-
13 port may contain a classified annex.

14 (c) FEDERAL POWER ACT AMENDMENT.—Part II of
15 the Federal Power Act (16 U.S.C. 791a and following)
16 is amended by adding the following new sections at the
17 end thereof:

18 **“SEC. 224 CRITICAL INFRASTRUCTURE.**

19 “(a) DEFINITIONS.—For purposes of this section:

20 “(1) CRITICAL ELECTRIC INFRASTRUCTURE.—

21 The term ‘critical electric infrastructure’ means sys-
22 tems and assets, whether physical or cyber used for
23 the generation, transmission, distribution, or meter-
24 ing of electric energy that, in the determination of
25 the Commission, in consultation with the Secretary

1 of Homeland Security and other national security
2 agencies, are so vital to the United States that the
3 incapacity or destruction of such systems and assets,
4 either alone or in combination with the failure of
5 other assets, would cause significant harm to the se-
6 curity, national or regional economic security, or na-
7 tional or regional public health or safety.

8 “(2) CRITICAL ELECTRIC INFRASTRUCTURE IN-
9 FORMATION.—The term ‘critical electric infrastruc-
10 ture information’ means critical infrastructure infor-
11 mation related to critical electric infrastructure.

12 “(3) CRITICAL INFRASTRUCTURE INFORMA-
13 TION.—The term ‘critical infrastructure information’
14 has the same meaning as is given that term in sec-
15 tion 212(3) of the Critical Infrastructure Informa-
16 tion Act of 2002 (6 U.S.C. 131(3)).

17 “(4) CYBER THREAT.—The term ‘cyber threat’
18 means any act by a terrorist or other person that
19 disrupts, attempts to disrupt, or poses a significant
20 risk of disruption to the operation of programmable
21 electronic devices and communication networks (in-
22 cluding hardware, software, and data) essential to
23 the reliable operation of critical electric infrastruc-
24 ture.

1 “(5) CYBER VULNERABILITY.—The term ‘cyber
2 vulnerability’ means any weakness that, if exploited
3 by a terrorist or other person, poses a significant
4 risk of disruption to the operation of programmable
5 electronic devices and communication networks (in-
6 cluding hardware, software, and data) essential to
7 the reliable operation of critical electric infrastruc-
8 ture.

9 “(b) ASSESSMENT, REPORT, AND DETERMINA-
10 TION.—

11 “(1) IN GENERAL.—Pursuant to section 201 of
12 the Homeland Security Act of 2002 (6 U.S.C. 121),
13 the Secretary of Homeland Security shall assess
14 cyber vulnerabilities or threats to critical infrastruc-
15 ture, including critical electric infrastructure and ad-
16 vanced metering infrastructure, on an ongoing basis
17 and produce reports, including recommendations, on
18 a periodic basis for the purposes of homeland secu-
19 rity, including the enhancement of domestic pre-
20 paredness for and collective response to a cyber at-
21 tack by a terrorist, nation-state, or other person,
22 and for other purposes.

23 “(2) ELEMENTS OF THE REPORT.—The Sec-
24 retary shall—

1 “(A) include in the reports under this sec-
2 tion findings regarding a cyber vulnerability or
3 terrorist threat or potential terrorist threat, and
4 a nation-state threat or potential threat to crit-
5 ical electric infrastructure; and

6 “(B) provide recommendations regarding
7 actions that may be performed to enhance indi-
8 vidualized and collective domestic preparedness
9 and response to the cyber vulnerability or ter-
10 rorist or nation-state.

11 “(3) TRANSMITTAL OF REPORT.—The Sec-
12 retary of Homeland Security shall transmit reports
13 prepared in response to the cyber vulnerability or
14 threat to the Commission and the appropriate com-
15 mittees of Congress, including the Committee on
16 Homeland Security of the House of Representatives
17 and the Homeland Security and Governmental Af-
18 fairs Committee of the Senate, of the Secretary’s de-
19 terminations under this section. Each such report
20 may contain a classified annex.

21 “(4) TIMELY DETERMINATION.—If, in carrying
22 out the assessment required under paragraph (1),
23 the Secretary of Homeland Security determines that
24 a significant cyber vulnerability or threat to critical
25 electric infrastructure has been identified, the Sec-

1 retary of Homeland Security shall communicate such
2 a determination to the Commission in a timely man-
3 ner. The Secretary of Homeland Security may incor-
4 porate intelligence or information received from
5 other national security or intelligence agencies in
6 making such determination.

7 “(c) COMMISSION AUTHORITY.—

8 “(1) ISSUANCE OF RULES OR ORDERS.—Fol-
9 lowing receipt of a finding under subsection (b), the
10 Commission shall issue (and from time to time
11 thereafter amend) such rules or orders as are nec-
12 essary to protect critical electric infrastructure
13 against vulnerabilities or threats.

14 “(2) EMERGENCY PROCEDURES.—The Commis-
15 sion may issue, in consultation with the Secretary of
16 Homeland Security, a rule or order under this sec-
17 tion without prior notice or hearing if it determines
18 the rule or order must be issued immediately to pro-
19 tect critical electric infrastructure from an imminent
20 threat or vulnerability.

21 “(d) DURATION OF EMERGENCY RULES OR OR-
22 DERS.—Any rule or order issued by the Commission with-
23 out prior notice or hearing under subsection (c)(2) shall
24 remain effective for not more than 90 days unless, during
25 such 90 days, the Commission gives interested persons an

1 opportunity to submit written data, views, or arguments
2 (with or without opportunity for oral presentation) and af-
3 firms, amends, or repeals the rule or order.

4 “(e) JURISDICTION.—Notwithstanding section 201,
5 the provisions of this section shall apply to any entity that
6 owns, controls, or operates critical electric infrastructure,
7 and such entities shall be subject to the jurisdiction of the
8 Commission for purposes of carrying out this section and
9 for purposes of applying the enforcement authorities of
10 this Act with respect to such provisions, but shall not
11 make an electric utility or any other entity subject to the
12 jurisdiction of the Commission for any other purposes.

13 “(f) PROTECTION OF CRITICAL ELECTRIC INFRA-
14 STRUCTURE INFORMATION.—The provisions of section
15 214 of the Homeland Security Act of 2002 (6 U.S.C. 133)
16 shall apply to critical electric infrastructure information
17 submitted to the Commission under this section to the
18 same extent that they apply to critical infrastructure in-
19 formation voluntarily submitted to the Department of
20 Homeland Security under that Act (6 U.S.C. 101 and fol-
21 lowing).

1 **“SEC. 224B. PROTECTION AGAINST KNOWN CYBER**
2 **VULNERABILITIES OR THREATS TO THE**
3 **CRITICAL ELECTRIC INFRASTRUCTURE.**

4 “(a) INTERIM MEASURES.—After notice and oppor-
5 tunity for comment, the Commission shall establish, in
6 consultation with the Secretary of Homeland Security, by
7 rule or order, within 120 days of enactment of this section,
8 such mandatory interim measures as are necessary to pro-
9 tect against known cyber vulnerabilities or threats to the
10 reliable operation of the critical electric infrastructure in
11 the United States. Such interim reliability measures:

12 “(1) shall serve to supplement, replace, or mod-
13 ify cybersecurity reliability standards that, as of the
14 date of enactment of this section, were in effect pur-
15 suant to section 215, but that are determined by the
16 Commission, in consultation with the Secretary of
17 Homeland Security and other national security agen-
18 cies, to be inadequate to address known cyber
19 vulnerabilities or threats; and

20 “(2) may be replaced by new cybersecurity reli-
21 ability standards that are developed and approved
22 pursuant to section 215 following the date of enact-
23 ment of this section.

24 “(b) PLANS.—The rule or order issued under this
25 subsection may require any owner, user or operator of crit-
26 ical electric infrastructure in the United States to develop

1 a plan to address cyber vulnerabilities or threats identified
2 by the Commission and to submit such plan to the Com-
3 mission for approval.”.

4 **SEC. 2. EVALUATION OF EXISTING AUTHORITIES.**

5 Section 214 of title II, subtitle B of the Homeland
6 Security Act of 2002 (6 U.S.C. 133(i)) is amended by add-
7 ing at the end the following:

8 “(i) **REVIEW OF AUTHORITIES TO PROTECT CRIT-**
9 **ICAL INFRASTRUCTURE.**—The Secretary of Homeland Se-
10 curity shall evaluate the capacity and authority of the De-
11 partment of Homeland Security and other Federal agen-
12 cies to ensure the security and resilience of electronic de-
13 vices and communication networks essential to each of the
14 critical infrastructure sectors identified pursuant to
15 Homeland Security Presidential Directive 7 against a
16 cyber attack by a terrorist, nation-state, or other person,
17 for the purpose of enhancing domestic preparedness for,
18 and collective response to, a cyber attack by a terrorist,
19 nation-state, or other person and to enhance the Nation’s
20 homeland security posture.”.

○