

111TH CONGRESS
1ST SESSION

S. 946

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

IN THE SENATE OF THE UNITED STATES

APRIL 30, 2009

Mr. LIEBERMAN introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To amend the Federal Power Act to provide additional legal 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. SHORT TITLE.**

4 This Act may be cited as the “Critical Electric Infra-
5 structure Protection Act of 2009”.

6 **SEC. 2. FINDINGS.**

7 Congress finds that—

8 (1) the critical electric infrastructure of the
9 United States and Canada has more than

1 \$1,000,000,000,000 in asset value, more than
2 200,000 miles of transmission lines, and more than
3 800,000 megawatts of generating capability, serving
4 over 300,000,000 people;

5 (2) the effective functioning of electric infra-
6 structure is highly dependent on computer-based
7 control systems that are used to monitor and man-
8 age sensitive processes and physical functions;

9 (3)(A) control systems are becoming increas-
10 ingly connected to open networks, such as corporate
11 intranets and the Internet; and

12 (B) according to the United States Computer
13 Emergency Readiness Team of the Department of
14 Homeland Security, the transition towards widely
15 used technologies and open connectivity exposes con-
16 trol systems to the ever-present cyber risks that
17 exist in the information technology world in addition
18 to control system specific risks;

19 (4) malicious actors pose a significant risk to
20 the electric infrastructure;

21 (5) the Federal Bureau of Investigation has
22 identified multiple sources of threats to the critical
23 electric infrastructure, including foreign nation
24 states, domestic criminals and hackers, and disgrun-
25 tled employees;

1 (6) foreign electric infrastructure has been re-
2 peatedly subject to cyber attack;

3 (7) the Commission to Assess the Threat to the
4 United States from Electromagnetic Pulse Attack
5 reported in 2008 that an electromagnetic pulse at-
6 tack could cause significant damage or disruption to
7 critical electric infrastructure and other critical in-
8 frastructure, due to the widespread use of super-
9 visory control and data acquisition systems;

10 (8) the Control Systems Security Program of
11 the Department of Homeland Security is designed to
12 increase the reliability, security, and resilience of
13 control systems by—

14 (A) developing voluntary cyber risk reduc-
15 tion products;

16 (B) supporting the Industrial Control Sys-
17 tems Computer Emergency Response Team of
18 the Department of Homeland Security in devel-
19 oping vulnerability mitigation recommendations
20 and strategies; and

21 (C) coordinating and leveraging activities
22 for improving the critical infrastructure security
23 posture of the United States;

24 (9) in the interest of national and homeland se-
25 curity, a statutory mechanism is necessary to protect

1 the critical electric infrastructure against cyber secu-
 2 rity threats; and

3 (10) on May 21, 2008, in testimony before the
 4 Committee on Homeland Security of the House of
 5 Representatives, Joseph Kelliher, then-Chairman of
 6 the Federal Energy Regulatory Commission, stated
 7 that the Commission is in need of additional legal
 8 authorities to adequately protect the electric power
 9 system against cyber attack.

10 **SEC. 3. INVESTIGATION OF CYBER COMPROMISE OF CRIT-**
 11 **ICAL ELECTRIC INFRASTRUCTURE.**

12 (a) IN GENERAL.—Pursuant to section 201 of the
 13 Homeland Security Act of 2002 (6 U.S.C. 121), the Sec-
 14 retary of Homeland Security, working with other national
 15 security and intelligence agencies, shall conduct an inves-
 16 tigation to determine if the security of Federally owned
 17 programmable electronic devices and communication net-
 18 works (including hardware, software, and data) essential
 19 to the reliable operation of critical electric infrastructure
 20 have been compromised.

21 (b) FOCUS.—The investigation under this section
 22 shall focus on—

- 23 (1) the extent of compromise;
- 24 (2) the identification of attackers;
- 25 (3) the method of penetration;

1 (4) the ramifications of the compromise on fu-
2 ture operations of critical electric infrastructure;

3 (5) the secondary ramifications of the com-
4 promise on other critical infrastructure sectors and
5 the functioning of civil society;

6 (6) the ramifications of the compromise on na-
7 tional security, including war fighting capability; and

8 (7) recommended mitigation activities.

9 (c) REPORT.—The Secretary of Homeland Security
10 shall submit to the appropriate committees of Congress
11 (including the Committee on Homeland Security of the
12 House of Representatives and the Homeland Security and
13 Governmental Affairs Committee of the Senate) a report
14 on findings of the investigation, including (at the option
15 of the Secretary) a classified annex.

16 **SEC. 4. CRITICAL INFRASTRUCTURE.**

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

19 **“SEC. 224. CRITICAL INFRASTRUCTURE.**

20 “(a) DEFINITIONS.—In this section:

21 “(1) CRITICAL ELECTRIC INFRASTRUCTURE.—

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

1 are so vital to the United States that the incapacity
2 or destruction of the systems and assets, either
3 alone or in combination with the failure of other as-
4 sets, would have a debilitating impact on the secu-
5 rity of the United States, national or regional eco-
6 nomic security, or national or regional public health
7 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 given the term in section 212
15 of the Critical Infrastructure Information Act of
16 2002 (6 U.S.C. 131).

17 “(4) CYBER THREAT.—The term ‘cyber threat’
18 means any act that disrupts, attempts to disrupt, or
19 poses a significant risk of disruption to the oper-
20 ation of programmable electronic devices and com-
21 munication networks (including hardware, software,
22 and data) essential to the reliable operation of crit-
23 ical electric infrastructure.

24 “(5) CYBER VULNERABILITY.—The term ‘cyber
25 vulnerability’ means any weakness that, if exploited,

1 poses a significant risk of disruption to the oper-
 2 ation of programmable electronic devices and com-
 3 munication networks (including hardware, software,
 4 and data) essential to the reliable operation of crit-
 5 ical electric infrastructure.

6 “(b) ASSESSMENT, REPORT, AND DETERMINATION
 7 OF VULNERABILITY OR THREAT TO CRITICAL ELECTRIC
 8 INFRASTRUCTURE.—

9 “(1) IN GENERAL.—Pursuant to section 201 of
 10 the Homeland Security Act of 2002 (6 U.S.C. 121),
 11 the Secretary of Homeland Security shall—

12 “(A) assess cyber vulnerabilities and cyber
 13 threats to critical infrastructure, including crit-
 14 ical electric infrastructure and advanced meter-
 15 ing infrastructure, on an ongoing basis; and

16 “(B) produce reports, including rec-
 17 ommendations, on a periodic basis.

18 “(2) ELEMENTS OF REPORTS.—The Secretary
 19 shall—

20 “(A) include in the reports under this sec-
 21 tion findings regarding cyber vulnerabilities and
 22 cyber threats to critical electric infrastructure;
 23 and

24 “(B) provide recommendations regarding
 25 actions that may be performed by the Federal

1 Government or the private sector to enhance in-
2 dividualized and collective domestic prepared-
3 ness and response to the cyber vulnerability or
4 cyber threat.

5 “(3) SUBMISSION OF REPORT.—The Secretary
6 of Homeland Security shall submit to the Commis-
7 sion and the appropriate committees of Congress
8 (including the Committee on Homeland Security of
9 the House of Representatives and the Committee on
10 Homeland Security and Governmental Affairs of the
11 Senate) reports prepared in response to the cyber
12 vulnerability or cyber threat that describe the deter-
13 minations of the Secretary, including (at the option
14 of the Secretary) a classified annex.

15 “(4) TIMELY DETERMINATION.—

16 “(A) IN GENERAL.—In carrying out the
17 assessment required under paragraph (1), if the
18 Secretary of Homeland Security determines
19 that a significant cyber vulnerability or cyber
20 threat to critical electric infrastructure has been
21 identified, the Secretary shall communicate the
22 determination to the Commission in a timely
23 manner.

24 “(B) INFORMATION.—The Secretary of
25 Homeland Security may incorporate intelligence

1 or information received from other national se-
2 curity or intelligence agencies in making the de-
3 termination.

4 “(c) COMMISSION AUTHORITY.—

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

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

18 “(d) DURATION OF EMERGENCY RULES OR OR-
19 DERS.—Any rule or order promulgated or issued by the
20 Commission without prior notice or hearing under sub-
21 section (c)(2) shall remain effective for a period of not
22 more than 90 days unless, during the 90-day period, the
23 Commission—

1 “(1) gives interested persons an opportunity to
2 submit written data, views, or arguments (with or
3 without opportunity for oral presentation); and

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

6 “(e) JURISDICTION.—

7 “(1) IN GENERAL.—Notwithstanding section
8 201, this section shall apply to any entity that owns,
9 controls, or operates critical electric infrastructure.

10 “(2) COVERED ENTITIES.—

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

14 “(i) carrying out this section; and

15 “(ii) applying the enforcement au-
16 thorities of this Act with respect to this
17 section.

18 “(B) JURISDICTION.—This subsection
19 shall not make an electric utility or any other
20 entity subject to the jurisdiction of the Commis-
21 sion for any other purposes.

22 “(f) PROTECTION OF CRITICAL ELECTRIC INFRA-
23 STRUCTURE INFORMATION.—Section 214 of the Home-
24 land Security Act of 2002 (6 U.S.C. 133) shall apply to
25 critical electric infrastructure information submitted to

1 the Commission under this section to the same extent as
2 that section applies to critical infrastructure information
3 voluntarily submitted to the Department of Homeland Se-
4 curity under that Act (6 U.S.C. 101 et seq.).

5 “(g) PROTECTION AGAINST KNOWN CYBER
6 VULNERABILITIES OR CYBER THREATS TO CRITICAL
7 ELECTRIC INFRASTRUCTURE.—

8 “(1) INTERIM MEASURES.—

9 “(A) IN GENERAL.—After notice and op-
10 portunity for comment, the Commission shall
11 establish, in consultation with the Secretary of
12 Homeland Security, by rule or order, not later
13 than 120 days after the date of enactment of
14 this Act, such mandatory interim measures as
15 are necessary to protect against known cyber
16 vulnerabilities or cyber threats to the reliable
17 operation of the critical electric infrastructure
18 of the United States.

19 “(B) ADMINISTRATION.—The interim reli-
20 ability measures—

21 “(i) shall serve to supplement, replace,
22 or modify cybersecurity reliability stand-
23 ards that, as of the date of enactment of
24 this section, were in effect pursuant to this
25 Act, but that are determined by the Com-

1 mission, in consultation with the Secretary
2 of Homeland Security and other national
3 security agencies, to be inadequate to ad-
4 dress known cyber vulnerabilities or cyber
5 threats; and

6 “(ii) may be replaced by new cyberse-
7 curity reliability standards that are devel-
8 oped and approved pursuant to this Act
9 following the date of enactment of this sec-
10 tion.

11 “(2) PLANS.—The rule or order issued under
12 this subsection may require any owner, user, or op-
13 erator of critical electric infrastructure in the United
14 States—

15 “(A) to develop a plan to address cyber
16 vulnerabilities or cyber threats identified by the
17 Commission; and

18 “(B) to submit the plan to the Commission
19 for approval.”.

○