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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Critical Electric Infrastructure Protection Act of 2009''.

SEC. 2. FINDINGS.

Congress finds that—

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

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

(2) the effective functioning of electric infrastructure is highly dependent on computer-based control systems that are used to monitor and manage sensitive processes and physical functions;

(3)(A) control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet; and

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

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

(5) the Federal Bureau of Investigation has identified multiple sources of threats to the critical electric infrastructure, including foreign nation states, domestic criminals and hackers, and disgruntled employees;

(6) foreign electric infrastructure has been repeatedly subject to cyber attack;

(7) the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack reported in 2008 that an electromagnetic pulse attack could cause significant damage or disruption to critical electric infrastructure and other critical infrastructure, due to the widespread use of supervisory control and data acquisition systems;

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

(A) developing voluntary cyber risk reduction products;

(B) supporting the Industrial Control Systems Computer Emergency Response Team of the Department of Homeland Security in developing vulnerability mitigation recommendations and strategies; and

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

(9) in the interest of national and homeland security, a statutory mechanism is necessary to protect

the critical electric infrastructure against cyber security threats; and

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

SEC. 3. INVESTIGATION OF CYBER COMPROMISE OF CRITICAL ELECTRIC INFRASTRUCTURE.

(a) IN GENERAL.—Pursuant to section 201 of the Homeland Security Act of 2002 (6 U.S.C. 121), the Secretary of Homeland Security, working with other national security and intelligence agencies, shall conduct an investigation to determine if the security of Federally owned programmable electronic devices and communication networks (including hardware, software, and data) essential to the reliable operation of critical electric infrastructure have been compromised.

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

(1) the extent of compromise;

(2) the identification of attackers;

(3) the method of penetration;

(4) the ramifications of the compromise on future operations of critical electric infrastructure;

(5) the secondary ramifications of the compromise on other critical infrastructure sectors and the functioning of civil society;

(6) the ramifications of the compromise on national security, including war fighting capability; and

(7) recommended mitigation activities.

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

SEC. 4. CRITICAL INFRASTRUCTURE.

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

"SEC. 224. CRITICAL INFRASTRUCTURE.

''(a) DEFINITIONS.—In this section:

''(1) CRITICAL ELECTRIC INFRASTRUCTURE.—The term 'critical electric infrastructure' means systems and assets, whether physical or cyber, used for the generation, transmission, distribution, or metering of electric energy in interstate commerce that

are so vital to the United States that the incapacity or destruction of the systems and assets, either alone or in combination with the failure of other assets, would have a debilitating impact on the security of the United States, national or regional economic security, or national or regional public health or safety.

''(2) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—The term 'critical electric infrastructure information' means critical infrastructure information related to critical electric infrastructure.

''(3) CRITICAL INFRASTRUCTURE INFORMATION.—The term 'critical infrastructure information' has the same meaning given the term in section 212 of the Critical Infrastructure Information Act of 2002 (6 U.S.C. 131).

''(4) CYBER THREAT.—The term 'cyber threat' means any act that disrupts, attempts to disrupt, or poses a significant risk of disruption to the operation of programmable electronic devices and communication networks (including hardware, software, and data) essential to the reliable operation of critical electric infrastructure.

''(5) CYBER VULNERABILITY.—The term 'cyber vulnerability' means any weakness that, if exploited,

poses a significant risk of disruption to the operation of programmable electronic devices and communication networks (including hardware, software, and data) essential to the reliable operation of critical electric infrastructure.

''(b) ASSESSMENT, REPORT, AND DETERMINATION OF VULNERABILITY OR THREAT TO CRITICAL ELECTRIC INFRASTRUCTURE.—

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

''(A) assess cyber vulnerabilities and cyber threats to critical infrastructure, including critical electric infrastructure and advanced metering infrastructure, on an ongoing basis; and

''(B) produce reports, including recommendations, on a periodic basis.

''(2) ELEMENTS OF REPORTS.—The Secretary shall—

''(A) include in the reports under this section findings regarding cyber vulnerabilities and cyber threats to critical electric infrastructure; and

''(B) provide recommendations regarding actions that may be performed by the Federal

Government or the private sector to enhance individualized and collective domestic preparedness and response to the cyber vulnerability or cyber threat.

''(3) SUBMISSION OF REPORT.—The Secretary of Homeland Security shall submit to the Commission and the appropriate committees of Congress (including the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate) reports prepared in response to the cyber vulnerability or cyber threat that describe the determinations of the Secretary, including (at the option of the Secretary) a classified annex.

''(4) TIMELY DETERMINATION.—

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

''(B) INFORMATION.—The Secretary of Homeland Security may incorporate intelligence

or information received from other national security or intelligence agencies in making the determination.

''(c) COMMISSION AUTHORITY.—

''(1) ISSUANCE OF RULES OR ORDERS.—Following receipt of a finding under subsection (b), the Commission shall promulgate or issue (and from time to time amend) such rules or orders as are necessary to protect critical electric infrastructure against cyber vulnerabilities or cyber threats.

''(2) EMERGENCY PROCEDURES.—The Commission may issue, in consultation with the Secretary of Homeland Security, a rule or order under this section without prior notice or hearing if the Commission determines the rule or order must be issued immediately to protect critical electric infrastructure from an imminent threat or vulnerability.

''(d) DURATION OF EMERGENCY RULES OR ORDERS.—Any rule or order promulgated or issued by the Commission without prior notice or hearing under subsection (c)(2) shall remain effective for a period of not more than 90 days unless, during the 90-day period, the Commission—

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

''(2) affirms, amends, or repeals the rule or order.

''(e) JURISDICTION.—

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

''(2) COVERED ENTITIES.—

''(A) IN GENERAL.—An entity described in paragraph (1) shall be subject to the jurisdiction of the Commission for purposes of—

''(i) carrying out this section; and

''(ii) applying the enforcement authorities of this Act with respect to this section.

''(B) JURISDICTION.—This subsection shall not make an electric utility or any other entity subject to the jurisdiction of the Commission for any other purposes.

''(f) PROTECTION OF CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—Section 214 of the Homeland Security Act of 2002 (6 U.S.C. 133) shall apply to critical electric infrastructure information submitted to

the Commission under this section to the same extent as that section applies to critical infrastructure information voluntarily submitted to the Department of Homeland Security under that Act (6 U.S.C. 101 et seq.).

''(g) PROTECTION AGAINST KNOWN CYBER VULNERABILITIES OR CYBER THREATS TO CRITICAL ELECTRIC INFRASTRUCTURE.—

''(1) INTERIM MEASURES.—

''(A) IN GENERAL.—After notice and opportunity for comment, the Commission shall establish, in consultation with the Secretary of Homeland Security, by rule or order, not later than 120 days after the date of enactment of this Act, such mandatory interim measures as are necessary to protect against known cyber vulnerabilities or cyber threats to the reliable operation of the critical electric infrastructure of the United States.

''(B) ADMINISTRATION.—The interim reliability measures—

''(i) shall serve to supplement, replace, or modify cybersecurity reliability standards that, as of the date of enactment of this section, were in effect pursuant to this Act, but that are determined by the Com-

mission, in consultation with the Secretary of Homeland Security and other national security agencies, to be inadequate to address known cyber vulnerabilities or cyber threats; and

''(ii) may be replaced by new cybersecurity reliability standards that are developed and approved pursuant to this Act following the date of enactment of this section.

''(2) PLANS.—The rule or order issued under this subsection may require any owner, user, or operator of critical electric infrastructure in the United States—

''(A) to develop a plan to address cyber vulnerabilities or cyber threats identified by the Commission; and

''(B) to submit the plan to the Commission for approval.''.

○