I

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.

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

SECTION 1. CRITICAL ELECTRIC INFRASTRUCTURE.

(a) FINDINGS.—

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

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

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

(3) These control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet. According to the Department of Homeland Security's United States Computer Emergency Readiness Team (''US–CERT''), this 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 this infrastructure. The Federal Bureau of Investigation (''FBI'') has identified multiple sources of threats, including foreign nation states, domestic criminals and hackers, and disgruntled employees.

(5) Intentional or naturally occurring Electromagnetic Pulse (''EMP'') events also threaten crit-

ical electric infrastructure. The Commission to Assess the Threat to the United States from EMP Attack reported in 2008 that an EMP 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 (''SCADA'') systems. The National Academy of Sciences also reported in 2008 that Severe Space Weather Events could produce similar results.

(6) The Department of Homeland Security's Control Systems Security Program is designed to increase the reliability, security, and resilience of control systems to guard against and enhance domestic preparedness for and collective response to a cyber attack by a terrorist or other person. This is done by developing voluntary cyber risk reduction products, supporting the Department of Homeland Security's Industrial Control Systems Computer Emergency Response Team (''ICS–CERT'') in developing vulnerability mitigation recommendations and strategies, and coordinating and leveraging activities for improving the Nation's critical infrastructure security posture.

(7) According to recent news reports, the electronic control systems of the electrical system in the United States have been routinely penetrated and compromised. According to current and former national security officials, cyber spies from China, Russia, and other countries have penetrated the United States electrical system in order to map the system, and have left behind software programs that could be used to disrupt and disable the system.

(8) In the interest of national security, and to enhance domestic preparedness for and collective response to a cyber attack by a terrorist or other person, a statutory mechanism is necessary to protect the critical electric infrastructure against cyber threats.

(9) In spite of existing mandatory cybersecurity standards, a report from the North American Electric Reliability Corporation (''NERC'') suggests that many utilities are underreporting their assets, potentially to avoid compliance requirements. In April 2009, NERC reported that only 23 percent of responding utilities identified a ''Critical Cyber Asset'' as required by NERC Reliability Standard 002–1. According to NERC, the results of this survey suggest that utilities may not have identified certain

qualifying assets as ''Critical''. NERC requested that entities take a fresh, comprehensive look at their methodology in order to identify and secure more Critical Cyber Assets.

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

(b) RESEARCH ON CYBER COMPROMISE OF CRITICAL ELECTRIC INFRASTRUCTURE.—(1) Pursuant to section 201 of the Homeland Security Act of 2002 (6 U.S.C. 121) and in furtherance of domestic preparedness for and collective response to a cyber attack by a terrorist or other person, the Secretary of Homeland Security, working with other national security and intelligence agencies, shall conduct research and 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.

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

fication of attackers, the method of penetration, ramifications of the compromise on future operations of critical electric infrastructure, secondary ramifications of the compromise on other critical infrastructure sectors and the functioning of civil society, ramifications of compromise on national security, including war fighting capability, and recommended mitigation activities.

(3) The Secretary of Homeland Security shall report the findings 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. The report may contain a classified annex.

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

"SEC. 224 CRITICAL INFRASTRUCTURE.

''(a) DEFINITIONS.—For purposes of 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 that, in the determination of the Commission, in consultation with the Secretary

of Homeland Security and other national security agencies, are so vital to the United States that the incapacity or destruction of such systems and assets, either alone or in combination with the failure of other assets, would cause significant harm to the security, 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 as is given that term in section 212(3) of the Critical Infrastructure Information Act of 2002 (6 U.S.C. 131(3)).

''(4) CYBER THREAT.—The term 'cyber threat' means any act by a terrorist or other person 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 by a terrorist or other person, 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.—

''(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 assess cyber vulnerabilities or threats to critical infrastructure, including critical electric infrastructure and advanced metering infrastructure, on an ongoing basis and produce reports, including recommendations, on a periodic basis for the purposes of homeland security, including the enhancement of domestic preparedness for and collective response to a cyber attack by a terrorist, nation-state, or other person, and for other purposes.

''(2) ELEMENTS OF THE REPORT.—The Secretary shall—

"(A) include in the reports under this section findings regarding a cyber vulnerability or terrorist threat or potential terrorist threat, and a nation-state threat or potential threat to critical electric infrastructure; and

"(B) provide recommendations regarding actions that may be performed to enhance individualized and collective domestic preparedness and response to the cyber vulnerability or terrorist or nation-state.

"(3) TRANSMITTAL OF REPORT.—The Secretary of Homeland Security shall transmit reports prepared in response to the cyber vulnerability or threat to the Commission and 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, of the Secretary's determinations under this section. Each such report may contain a classified annex.

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

retary of Homeland Security shall communicate such a determination to the Commission in a timely manner. The Secretary of Homeland Security may incorporate intelligence or information received from other national security or intelligence agencies in making such determination.

''(c) COMMISSION AUTHORITY.—

''(1) ISSUANCE OF RULES OR ORDERS.—Following receipt of a finding under subsection (b), the Commission shall issue (and from time to time thereafter amend) such rules or orders as are necessary to protect critical electric infrastructure against vulnerabilities or 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 it 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 issued by the Commission without prior notice or hearing under subsection (c)(2) shall remain effective for not more than 90 days unless, during such 90 days, the Commission gives interested persons an

opportunity to submit written data, views, or arguments (with or without opportunity for oral presentation) and affirms, amends, or repeals the rule or order.

''(e) JURISDICTION.—Notwithstanding section 201, the provisions of this section shall apply to any entity that owns, controls, or operates critical electric infrastructure, and such entities shall be subject to the jurisdiction of the Commission for purposes of carrying out this section and for purposes of applying the enforcement authorities of this Act with respect to such provisions, but 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.—The provisions of 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 that they apply to critical infrastructure information voluntarily submitted to the Department of Homeland Security under that Act (6 U.S.C. 101 and following).

"SEC. 224B. PROTECTION AGAINST KNOWN CYBER VULNERABILITIES OR THREATS TO THE CRITICAL ELECTRIC INFRASTRUCTURE.

''(a) INTERIM MEASURES.—After notice and opportunity for comment, the Commission shall establish, in consultation with the Secretary of Homeland Security, by rule or order, within 120 days of enactment of this section, such mandatory interim measures as are necessary to protect against known cyber vulnerabilities or threats to the reliable operation of the critical electric infrastructure in the United States. Such interim reliability measures:

''(1) 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 section 215, but that are determined by the Commission, in consultation with the Secretary of Homeland Security and other national security agencies, to be inadequate to address known cyber vulnerabilities or threats; and

''(2) may be replaced by new cybersecurity reliability standards that are developed and approved pursuant to section 215 following the date of enactment of this section.

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

a plan to address cyber vulnerabilities or threats identified by the Commission and to submit such plan to the Commission for approval.''.

SEC. 2. EVALUATION OF EXISTING AUTHORITIES.

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

''(i) REVIEW OF AUTHORITIES TO PROTECT CRITICAL INFRASTRUCTURE.—The Secretary of Homeland Security shall evaluate the capacity and authority of the Department of Homeland Security and other Federal agencies to ensure the security and resilience of electronic devices and communication networks essential to each of the critical infrastructure sectors identified pursuant to Homeland Security Presidential Directive 7 against a cyber attack by a terrorist, nation-state, or other person, for the purpose of enhancing domestic preparedness for, and collective response to, a cyber attack by a terrorist, nation-state, or other person and to enhance the Nation's homeland security posture.''.

○