112TH CONGRESS
1ST SESSION

S. 813

To promote public awareness of cyber security.

IN THE SENATE OF THE UNITED STATES

APRIL 13, 2011

Mr. WHITEHOUSE (for himself and Mr. KYL) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To promote public awareness of cyber security.

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 ''Cyber Security Public Awareness Act of 2011''.

SEC. 2. FINDINGS.

(a) Congress finds the following:

(1) Information technology is central to the effectiveness, efficiency, and reliability of the industry and commercial services, Armed Forces and national

security systems, and the critical infrastructure of the United States.

(2) Cyber criminals, terrorists, and agents of foreign powers have taken advantage of the connectivity of the United States to inflict substantial damage to the economic and national security interests of the Nation.

(3) The cyber security threat is sophisticated, relentless, and massive, exposing all consumers in the United States to the risk of substantial harm.

(4) Businesses in the United States are bearing enormous losses as a result of criminal cyber attacks, depriving businesses of hard-earned profits that could be reinvested in further job-producing innovation.

(5) Hackers continuously probe the networks of Federal and State agencies, the Armed Forces, and the commercial industrial base of the Armed Forces, and already have caused substantial damage and compromised sensitive and classified information.

(6) Severe cyber security threats will continue, and will likely grow, as the economy of the United States grows more connected, criminals become increasingly sophisticated in efforts to steal from consumers, industries, and businesses in the United

States, and terrorists and foreign nations continue to use cyberspace as a means of attack against the national and economic security of the United States.

(7) Public awareness of cyber security threats is essential to cyber security defense. Only a well-informed public and Congress can make the decisions necessary to protect consumers, industries, and the national and economic security of the United States.

(8) As of 2011, the level of public awareness of cyber security threats is unacceptably low. Only a tiny portion of relevant cyber security information is released to the public. Information about attacks on Federal Government systems is usually classified. Information about attacks on private systems is ordinarily kept confidential. Sufficient mechanisms do not exist to provide meaningful threat reports to the public in unclassified and anonymized form.

SEC. 3. CYBER INCIDENTS AGAINST GOVERNMENT NETWORKS.

(a) DEPARTMENT OF HOMELAND SECURITY.—Not later than 180 days after the date of enactment of this Act, and annually thereafter, the Secretary of Homeland Security shall submit to Congress a report that—

(1) summarizes major cyber incidents involving networks of executive agencies (as defined in section

105 of title 5, United States Code), except for the Department of Defense;

(2) provides aggregate statistics on the number of breaches of networks of executive agencies, the volume of data exfiltrated, and the estimated cost of remedying the breaches; and

(3) discusses the risk of cyber sabotage.

(b) DEPARTMENT OF DEFENSE.—Not later than 180 days after the date of enactment of this Act, and annually thereafter, the Secretary of Defense shall submit to Congress a report that—

(1) summarizes major cyber incidents against networks of the Department of Defense and the military departments;

(2) provides aggregate statistics on the number of breaches against networks of the Department of Defense and the military departments, the volume of data exfiltrated, and the estimated cost of remedying the breaches; and

(3) discusses the risk of cyber sabatoge.

(c) FORM OF REPORTS.—Each report submitted under this section shall be in unclassified form, but may include a classified annex as necessary to protect sources, methods, and national security.

SEC. 4. PROSECUTION FOR CYBERCRIME.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Attorney General and the Director of the Federal Bureau of Investigation shall submit to Congress reports—

(1) describing investigations and prosecutions by the Department of Justice relating to cyber intrusions or other cybercrimes the preceding year, including—

(A) the number of investigations initiated relating to such crimes;

(B) the number of arrests relating to such crimes;

(C) the number and description of instances in which investigations or prosecutions relating to such crimes have been delayed or prevented because of an inability to extradite a criminal defendant in a timely manner; and

(D) the number of prosecutions for such crimes, including—

(i) the number of defendants prosecuted;

(ii) whether the prosecutions resulted in a conviction;

(iii) the sentence imposed and the statutory maximum for each such crime for which a defendant was convicted; and

(iv) the average sentence imposed for a conviction of such crimes;

(2) identifying the number of employees, financial resources, and other resources (such as technology and training) devoted to the enforcement, investigation, and prosecution of cyber intrusions or other cybercrimes, including the number of investigators, prosecutors, and forensic specialists dedicated to investigating and prosecuting cyber intrusions or other cybercrimes; and

(3) discussing any impediments under the laws of the United States or international law to prosecutions for cyber intrusions or other cybercrimes.

(b) UPDATES.—The Attorney General and the Director of the Federal Bureau of Investigation shall annually submit to Congress reports updating the reports submitted under section (a) at the same time the Attorney General and Director submit annual reports under section 404 of the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (42 U.S.C. 3713d).

SEC. 5. ASSISTANCE PLAN FOR SIGNIFICANT PRIVATE CYBER INCIDENTS.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, and annually thereafter, the Secretary of Homeland Security shall submit to Congress a report that describes policies and procedures for Federal agencies to assist a private sector entity in the defending of the information networks of the private sector entity against cyber threats that could result in loss of life or significant harm to the national economy or national security.

(b) FORM OF REPORTS.—Each report submitted under this section shall be in unclassified form, but may include a classified annex as necessary to protect sources, methods, proprietary or sensitive business information, and national security.

SEC. 6. CYBERCRIME REPORTING TO SHAREHOLDERS.

Not later than 180 days after the date of enactment of this Act, the Securities and Exchange Commission, in consultation with the Secretary of Homeland Security, shall submit to Congress a report on—

(1) the extent of financial risk to issuers of securities caused by cyber intrusions or other cybercrimes, and any resulting legal liability; and

(2) whether current financial statements of issuers transparently reflect the risk described in paragraph (1) to shareholders.

SEC. 7. PRIMARY REGULATORS OF CRITICAL INFRASTRUCTURE.

(a) DEFINITIONS.—In this section the term ''primary regulators responsible for the physical and economic security of each critical industry'' means—

(1) for the energy industry, the Federal Energy Regulatory Commission, the Nuclear Regulatory Commission, and the Secretary of Energy;

(2) for the financial services industry, the Federal Deposit Insurance Commission, the Secretary of the Treasury, and the Chairman of the Securities and Exchange Commission;

(3) for the air, rail, and ground transportation industry, the Secretary of Transportation;

(4) for the communications industry, the Federal Communications Commission;

(5) for the food supply industry, the Commissioner of Food and Drugs;

(6) for the water supply industry, the Administrator of the Environmental Protection Agency; and

(7) for any other element of the economy determined to be critical by the Secretary of Homeland Security, the Federal Trade Commission.

(b) REPORTS.—Not later than 180 days after the date of enactment of this Act, and annually thereafter for 3 years, the primary regulator for each critical industry, in consultation with the Secretary of Homeland Security, shall submit to Congress a report that describes the—

(1) nature and state of the vulnerabilities to cyber attacks of each industry described in subsection (a);

(2) prevalence and seriousness of cyber attacks in each industry described in subsection (a);

(3) recommended steps to thwart or diminish cyber attacks; and

(4) whether the concept of cyber security and information assurance cooperative activities with private sector partners developed by the Defense Industrial Base of the Department of Defense may be applied to the critical industries described in subsection (a).

(c) FORM OF REPORTS.—Each report submitted under this section—

(1) shall be—

(A) in unclassified form; and

(B) anonymized as the Secretary determines necessary to protect confidential business information; and

(2) may include a classified annex as necessary to protect sources, methods, proprietary or sensitive business information, and national security.

SEC. 8. RESEARCH REPORT ON IMPROVING SECURITY OF INFORMATION NETWORKS OF CRITICAL INFRASTRUCTURE ENTITIES.

(a) DEFINITION.—In this section, the term ''critical infrastructure'' has the meaning given that term in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)).

(b) REPORTS.—

(1) IN GENERAL.—The Secretary of Homeland Security shall enter into a contract with the National Research Council, or another federally funded research and development corporation, under which the Council or corporation shall submit to Congress reports on available technical options, consistent with Constitutional and statutory privacy rights, for enhancing the security of the information networks of entities that own or manage critical infrastructure through—

(A) technical improvements, including developing a secure domain; or

(B) increased notice of and consent to the use of technologies to scan for, detect, and defeat cyber security threats, such as technologies used in a secure domain.

(2) TIMING.—The contract entered into under paragraph (1) shall require that the report described in paragraph (1) be submitted—

(A) not later than 180 days after the date of enactment of this Act;

(B) annually, after the first report submitted under paragraph (1), for 3 years; and

(C) more frequently, as determined appropriate by the Secretary of Homeland Security in response to new risks or technologies that emerge.

SEC. 9. PREPAREDNESS OF FEDERAL COURTS TO PROMOTE CYBER SECURITY.

Not later than 180 days after the date of enactment of this Act, the Attorney General, in coordination with the Administrative Office of the United States Courts, shall submit to Congress a report—

(1) on whether Federal courts have granted timely relief in matters relating to botnets and other cybercrime and cyber security threats; and

(2) that includes, as appropriate, recommendations on changes or improvements to—

(A) the Federal Rules of Civil Procedure or the Federal Rules of Criminal Procedure;

(B) the training and other resources available to support the Federal judiciary;

(C) the capabilities and specialization of courts to which such cases may be assigned; and

(D) Federal civil and criminal laws.

SEC. 10. IMPEDIMENTS TO PUBLIC AWARENESS.

Not later than 180 days after the date of enactment of this Act, and annually thereafter for 3 years (or more frequently if determined appropriate by the Secretary of Homeland Security) the Secretary of Homeland Security shall submit to Congress a report on—

(1) legal or other impediments to appropriate public awareness of—

(A) the nature of, methods of propagation of, and damage caused by common cyber security threats such as computer viruses, phishing techniques, and malware;

(B) the minimal standards of computer security necessary for responsible Internet use; and

(C) the availability of commercial off the shelf technology that allows consumers to meet such levels of computer security;

(2) a summary of the plans of the Secretary of Homeland Security to enhance public awareness of common cyber security threats, including a description of the metrics used by the Department of Homeland Security for evaluating the efficacy of public awareness campaigns; and

(3) recommendations for congressional actions to address these impediments to appropriate public awareness of common cyber security threats.

SEC. 11. PROTECTING THE INFORMATION TECHNOLOGY SUPPLY CHAIN OF THE UNITED STATES.

(a) DEFINITIONS.—In this section—

(1) the term ''information technology supply chain of the United States'' means the public and private telecommunications networks of the United States; and

(2) the term ''telecommunications networks of the United States'' includes—

(A) telephone systems;

(B) Internet systems;

(C) fiber optic lines, including cable landings;

(D) computer networks; and

(E) smart grid technology under development by the Department of Energy.

(b) REPORT.—Not later than 90 days after the date of enactment of this Act, and annually thereafter, the Secretary of Homeland Security shall submit to Congress a report that—

(1) identifies foreign suppliers of information technology (including equipment, software, and services) that are linked directly or indirectly to a foreign government, including—

(A) by ties to the military forces of a foreign government; or

(B) by being the beneficiaries of significant low interest or no interest loans, loan forgiveness, or other support by a foreign government;

(2) discusses the extent to which goods produced by suppliers identified under paragraph (2) have been integrated into the information technology supply chain of the United States;

(3) identifies specific telecommunications networks of the United States that include information technology identified under paragraph (1); and

(4) assesses the vulnerability to malicious activity, including cyber crime or espionage, of the tele-

communications networks of the United States identified under paragraph (3) due to the presence of technology produced by suppliers identified under paragraph (1).

SEC. 12. PROTECTING THE ELECTRICAL GRID OF THE UNITED STATES.

Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security, in consultation with the Secretary of Defense and the Director of National Intelligence, shall submit to Congress a report on—

(1) the threat of a cyber attack disrupting the electrical grid of the United States;

(2) the implications for the national security of the United States if the electrical grid is disrupted;

(3) the options available to the United States and private sector entities to quickly reconstitute electrical service to provide for the national security of the United States, and, within a reasonable time frame, the reconstitution of all electrical service within the United States; and

(4) a plan to prevent disruption of the electric grid of the United States caused by a cyber attack.

○