113TH CONGRESS
1ST SESSION

S. 1638

To promote public awareness of cybersecurity.

IN THE SENATE OF THE UNITED STATES

OCTOBER 31, 2013

Mr. WHITEHOUSE (for himself, Mr. BLUNT, Mr. GRAHAM, and Mr. BLUMENTHAL) 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 cybersecurity.

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 ''Cybersecurity Public Awareness Act of 2013''.

SEC. 2. FINDINGS.

(a) Congress finds the following:

(1) Information technology is central to the effectiveness, efficiency, and reliability of industrial 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 threat is sophisticated, relentless, and massive, exposing consumers in the United States to the risk of substantial harm.

(4) Businesses in the United States are bearing substantial 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 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 threats is essential to cybersecurity. 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 2013, the level of public awareness of cyber threats is unacceptably low. Only a tiny portion of relevant cybersecurity 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 sabotage.

(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, computer or network compromise, or other forms of illegal hacking 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, computer or network compromised, or other forms of illegal hacking, including the number of investigators, prosecutors, and forensic specialists dedicated to investigating and prosecuting cyber intrusions, computer or network compromise, or other forms of illegal hacking; and

(3) discussing any impediments under the laws of the United States or international law to prosecutions for cyber intrusions, computer or network compromise, or other forms of illegal hacking.

(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. RESPONSE TO REQUESTS FOR ASSISTANCE IN PRIVATE SECTOR 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 through which Federal agencies, upon request from a private sector entity, assist in the defense of the information networks of the requesting 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. REPORTING TO SHAREHOLDERS OF CYBER RISKS AND CYBER INCIDENTS.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, and annually thereafter for 3 years, the Securities and Exchange Commission, in consultation with the Secretary of Commerce and the Sec-

retary of Homeland Security, shall submit to Congress a report—

(1) assessing the reporting of cyber risk or cyber incidents in financial statements by issuers of securities; and

(2) evaluating relevant Commission actions, including the staff guidance issued by the Commission on October 13, 2011.

(b) PROHIBITION.—A report submitted under this section shall not include proprietary or sensitive business information or identify any individual issuer.

SEC. 7. REGULATORS OF CRITICAL INFRASTRUCTURE.

(a) DEFINITIONS.—In this section—

(1) the term ''critical infrastructure sector'' means any sector identified in Presidential Policy Directive–21, issued February 12, 2013 (or any successor thereto); and

(2) the term ''relevant agencies'' means—

(A) the sector-specific agencies identified in Presidential Policy Directive–21, issued February 12, 2013 (or any successor thereto); and

(B) each agency (as defined in section 3502(1) of title 44, United States Code) that has substantial regulatory authority in a critical infrastructure sector.

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

(1) nature and state of the vulnerabilities to cyber threats of each critical infrastructure sector;

(2) prevalence and seriousness of cyber threats in each critical infrastructure sector;

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

(4) the degree to which cybersecurity and information assurance cooperative activities with private sector partners developed by the Department of Defense and its defense industrial base have been employed in each critical infrastructure sector.

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

(1) shall be in unclassified form;

(2) shall not—

(A) identify any individual private sector entity; and

(B) include proprietary or sensitive business information; and

(3) may include a classified annex as necessary to protect sources, methods, and national security.

SEC. 8. RESEARCH REPORT ON DEVELOPING TECHNOLOGIES THAT WOULD ENHANCE CYBERSECURITY 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 a report on opportunities to develop new technologies or technological approaches, including developing a secure domain, that would enhance the cybersecurity of critical infrastructure entities.

(2) LIMITATIONS.—The report required under paragraph (1) shall—

(A) consider only technologies or technological options that can be deployed consistent with constitutional and statutory privacy rights; and

(B) identify any technologies or technological options described in subparagraph (A) that merit Federal research support.

(3) TIMING.—The contract entered into under paragraph (1) shall require that the report described in paragraph (1) be submitted not later than 1 year after the date of enactment of this Act. The Secretary of Homeland Security may enter into additional subsequent contracts as appropriate.

SEC. 9. PREPAREDNESS OF FEDERAL COURTS TO PROMOTE CYBERSECURITY.

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 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, social engineering 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 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 threats.

○