

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.

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 “Cybersecurity Public
5 Awareness Act of 2013”.

6 **SEC. 2. FINDINGS.**

7 (a) Congress finds the following:

8 (1) Information technology is central to the ef-
9 fectiveness, efficiency, and reliability of industrial
10 and commercial services, Armed Forces and national

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

3 (2) Cyber criminals, terrorists, and agents of
4 foreign powers have taken advantage of the
5 connectivity of the United States to inflict substan-
6 tial damage to the economic and national security
7 interests of the Nation.

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

11 (4) Businesses in the United States are bearing
12 substantial losses as a result of criminal cyber at-
13 tacks, depriving businesses of hard-earned profits
14 that could be reinvested in further job-producing in-
15 novation.

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

21 (6) Severe cyber threats will continue, and will
22 likely grow, as the economy of the United States
23 grows more connected, criminals become increasingly
24 sophisticated in efforts to steal from consumers, in-
25 dustries, and businesses in the United States, and

1 terrorists and foreign nations continue to use cyber-
2 space as a means of attack against the national and
3 economic security of the United States.

4 (7) Public awareness of cyber threats is essen-
5 tial to cybersecurity. Only a well-informed public and
6 Congress can make the decisions necessary to pro-
7 tect consumers, industries, and the national and eco-
8 nomic security of the United States.

9 (8) As of 2013, the level of public awareness of
10 cyber threats is unacceptably low. Only a tiny por-
11 tion of relevant cybersecurity information is released
12 to the public. Information about attacks on Federal
13 Government systems is usually classified. Informa-
14 tion about attacks on private systems is ordinarily
15 kept confidential. Sufficient mechanisms do not exist
16 to provide meaningful threat reports to the public in
17 unclassified and anonymized form.

18 **SEC. 3. CYBER INCIDENTS AGAINST GOVERNMENT NET-**
19 **WORKS.**

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

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

1 105 of title 5, United States Code), except for the
2 Department of Defense;

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

7 (3) discusses the risk of cyber sabotage.

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

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

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

20 (3) discusses the risk of cyber sabotage.

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

1 **SEC. 4. PROSECUTION FOR CYBERCRIME.**

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

6 (1) describing investigations and prosecutions
7 by the Department of Justice relating to cyber in-
8 trusions, computer or network compromise, or other
9 forms of illegal hacking the preceding year, includ-
10 ing—

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

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

15 (C) the number and description of in-
16 stances in which investigations or prosecutions
17 relating to such crimes have been delayed or
18 prevented because of an inability to extradite a
19 criminal defendant in a timely manner; and

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

22 (i) the number of defendants pros-
23 ecuted;

24 (ii) whether the prosecutions resulted
25 in a conviction;

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

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

6 (2) identifying the number of employees, finan-
7 cial resources, and other resources (such as tech-
8 nology and training) devoted to the enforcement, in-
9 vestigation, and prosecution of cyber intrusions,
10 computer or network compromised, or other forms of
11 illegal hacking, including the number of investiga-
12 tors, prosecutors, and forensic specialists dedicated
13 to investigating and prosecuting cyber intrusions,
14 computer or network compromise, or other forms of
15 illegal hacking; and

16 (3) discussing any impediments under the laws
17 of the United States or international law to prosecu-
18 tions for cyber intrusions, computer or network com-
19 promise, or other forms of illegal hacking.

20 (b) UPDATES.—The Attorney General and the Direc-
21 tor of the Federal Bureau of Investigation shall annually
22 submit to Congress reports updating the reports sub-
23 mitted under section (a) at the same time the Attorney
24 General and Director submit annual reports under section

1 404 of the Prioritizing Resources and Organization for In-
2 tellectual Property Act of 2008 (42 U.S.C. 3713d).

3 **SEC. 5. RESPONSE TO REQUESTS FOR ASSISTANCE IN PRI-**
4 **VATE SECTOR CYBER INCIDENTS.**

5 (a) IN GENERAL.—Not later than 180 days after the
6 date of enactment of this Act, and annually thereafter,
7 the Secretary of Homeland Security shall submit to Con-
8 gress a report that describes policies and procedures
9 through which Federal agencies, upon request from a pri-
10 vate sector entity, assist in the defense of the information
11 networks of the requesting private sector entity against
12 cyber threats that could result in loss of life or significant
13 harm to the national economy or national security.

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

19 **SEC. 6. REPORTING TO SHAREHOLDERS OF CYBER RISKS**
20 **AND CYBER INCIDENTS.**

21 (a) IN GENERAL.—Not later than 180 days after the
22 date of enactment of this Act, and annually thereafter for
23 3 years, the Securities and Exchange Commission, in con-
24 sultation with the Secretary of Commerce and the Sec-

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

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

6 (2) evaluating relevant Commission actions, in-
7 cluding the staff guidance issued by the Commission
8 on October 13, 2011.

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

12 **SEC. 7. REGULATORS OF CRITICAL INFRASTRUCTURE.**

13 (a) DEFINITIONS.—In this section—

14 (1) the term “critical infrastructure sector”
15 means any sector identified in Presidential Policy
16 Directive–21, issued February 12, 2013 (or any suc-
17 cessor thereto); and

18 (2) the term “relevant agencies” means—

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

22 (B) each agency (as defined in section
23 3502(1) of title 44, United States Code) that
24 has substantial regulatory authority in a critical
25 infrastructure sector.

1 (b) REPORTS.—Not later than 180 days after the
2 date of enactment of this Act, and annually thereafter for
3 3 years, the Secretary of Homeland Security, in consulta-
4 tion with relevant agencies, shall submit to Congress a re-
5 port that describes the—

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

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

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

12 (4) the degree to which cybersecurity and infor-
13 mation assurance cooperative activities with private
14 sector partners developed by the Department of De-
15 fense and its defense industrial base have been em-
16 ployed in each critical infrastructure sector.

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

19 (1) shall be in unclassified form;

20 (2) shall not—

21 (A) identify any individual private sector
22 entity; and

23 (B) include proprietary or sensitive busi-
24 ness information; and

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

3 **SEC. 8. RESEARCH REPORT ON DEVELOPING TECH-**
4 **NOLOGIES THAT WOULD ENHANCE CYBERSE-**
5 **CURITY OF CRITICAL INFRASTRUCTURE EN-**
6 **TITIES.**

7 (a) DEFINITION.—In this section, the term “critical
8 infrastructure” has the meaning given that term in section
9 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)).

10 (b) REPORTS.—

11 (1) IN GENERAL.—The Secretary of Homeland
12 Security shall enter into a contract with the Na-
13 tional Research Council, or another federally funded
14 research and development corporation, under which
15 the Council or corporation shall submit to Congress
16 a report on opportunities to develop new tech-
17 nologies or technological approaches, including devel-
18 oping a secure domain, that would enhance the cy-
19 bersecurity of critical infrastructure entities.

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

22 (A) consider only technologies or techno-
23 logical options that can be deployed consistent
24 with constitutional and statutory privacy rights;
25 and

1 (B) identify any technologies or techno-
2 logical options described in subparagraph (A)
3 that merit Federal research support.

4 (3) TIMING.—The contract entered into under
5 paragraph (1) shall require that the report described
6 in paragraph (1) be submitted not later than 1 year
7 after the date of enactment of this Act. The Sec-
8 retary of Homeland Security may enter into addi-
9 tional subsequent contracts as appropriate.

10 **SEC. 9. PREPAREDNESS OF FEDERAL COURTS TO PRO-**
11 **MOTE CYBERSECURITY.**

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

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

19 (2) that includes, as appropriate, recommenda-
20 tions on changes or improvements to—

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

23 (B) the training and other resources avail-
24 able to support the Federal judiciary;

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

4 (D) Federal civil and criminal laws.

5 **SEC. 10. IMPEDIMENTS TO PUBLIC AWARENESS.**

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

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

13 (A) the nature of, methods of propagation
14 of, and damage caused by common cyber secu-
15 rity threats such as computer viruses, social en-
16 gineering techniques, and malware;

17 (B) the minimal standards of computer se-
18 curity necessary for responsible internet use;
19 and

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

23 (2) a summary of the plans of the Secretary of
24 Homeland Security to enhance public awareness of
25 common cyber threats, including a description of the

1 metrics used by the Department of Homeland Secu-
2 rity for evaluating the efficacy of public awareness
3 campaigns; and

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

○