

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.

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 “Cyber Security Public  
5 Awareness Act of 2011”.

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 the industry  
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 security threat is sophisticated,  
9 relentless, and massive, exposing all consumers in  
10 the United States to the risk of substantial harm.

11 (4) Businesses in the United States are bearing  
12 enormous 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 security threats will continue,  
22 and will likely grow, as the economy of the United  
23 States grows more connected, criminals become in-  
24 creasingly sophisticated in efforts to steal from con-  
25 sumers, industries, and businesses in the United

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

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

9 (8) As of 2011, the level of public awareness of  
10 cyber security threats is unacceptably low. Only a  
11 tiny portion of relevant cyber security information is  
12 released to the public. Information about attacks on  
13 Federal Government systems is usually classified.  
14 Information about attacks on private systems is or-  
15 dinary kept confidential. Sufficient mechanisms do  
16 not exist to provide meaningful threat reports to the  
17 public in 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 or other cybercrimes the preceding year, in-  
9 cluding—

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

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

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

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

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

23 (ii) whether the prosecutions resulted  
24 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 or  
10 other cybercrimes, including the number of inves-  
11 tigators, prosecutors, and forensic specialists dedi-  
12 cated to investigating and prosecuting cyber intru-  
13 sions or other cybercrimes; and

14 (3) discussing any impediments under the laws  
15 of the United States or international law to prosecu-  
16 tions for cyber intrusions or other cybercrimes.

17 (b) UPDATES.—The Attorney General and the Direc-  
18 tor of the Federal Bureau of Investigation shall annually  
19 submit to Congress reports updating the reports sub-  
20 mitted under section (a) at the same time the Attorney  
21 General and Director submit annual reports under section  
22 404 of the Prioritizing Resources and Organization for In-  
23 tellectual Property Act of 2008 (42 U.S.C. 3713d).

1 **SEC. 5. ASSISTANCE PLAN FOR SIGNIFICANT PRIVATE**  
2 **CYBER INCIDENTS.**

3 (a) **IN GENERAL.**—Not later than 180 days after the  
4 date of enactment of this Act, and annually thereafter,  
5 the Secretary of Homeland Security shall submit to Con-  
6 gress a report that describes policies and procedures for  
7 Federal agencies to assist a private sector entity in the  
8 defending of the information networks of the private sec-  
9 tor entity against cyber threats that could result in loss  
10 of life or significant harm to the national economy or na-  
11 tional security.

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

17 **SEC. 6. CYBERCRIME REPORTING TO SHAREHOLDERS.**

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

22 (1) the extent of financial risk to issuers of se-  
23 curities caused by cyber intrusions or other  
24 cybercrimes, and any resulting legal liability; and

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

4 **SEC. 7. PRIMARY REGULATORS OF CRITICAL INFRASTRUC-**  
5 **TURE.**

6           (a) DEFINITIONS.—In this section the term “primary  
7 regulators responsible for the physical and economic secu-  
8 rity of each critical industry” means—

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

12          (2) for the financial services industry, the Fed-  
13          eral Deposit Insurance Commission, the Secretary of  
14          the Treasury, and the Chairman of the Securities  
15          and Exchange Commission;

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

18          (4) for the communications industry, the Fed-  
19          eral Communications Commission;

20          (5) for the food supply industry, the Commis-  
21          sioner of Food and Drugs;

22          (6) for the water supply industry, the Adminis-  
23          trator of the Environmental Protection Agency; and



1           (7) for any other element of the economy deter-  
2           mined to be critical by the Secretary of Homeland  
3           Security, the Federal Trade Commission.

4           (b) REPORTS.—Not later than 180 days after the  
5           date of enactment of this Act, and annually thereafter for  
6           3 years, the primary regulator for each critical industry,  
7           in consultation with the Secretary of Homeland Security,  
8           shall submit to Congress a report that describes the—

9           (1) nature and state of the vulnerabilities to  
10          cyber attacks of each industry described in sub-  
11          section (a);

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

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

16          (4) whether the concept of cyber security and  
17          information assurance cooperative activities with pri-  
18          vate sector partners developed by the Defense Indus-  
19          trial Base of the Department of Defense may be ap-  
20          plied to the critical industries described in subsection  
21          (a).

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

24                  (1) shall be—

25                          (A) in unclassified form; and

1 (B) anonymized as the Secretary deter-  
2 mines necessary to protect confidential business  
3 information; and

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

7 **SEC. 8. RESEARCH REPORT ON IMPROVING SECURITY OF**  
8 **INFORMATION NETWORKS OF CRITICAL IN-**  
9 **FRAStructure ENTITIES.**

10 (a) DEFINITION.—In this section, the term “critical  
11 infrastructure” has the meaning given that term in section  
12 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)).

13 (b) REPORTS.—

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

24 (A) technical improvements, including de-  
25 veloping a secure domain; or

1 (B) increased notice of and consent to the  
2 use of technologies to scan for, detect, and de-  
3 feat cyber security threats, such as technologies  
4 used in a secure domain.

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

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

10 (B) annually, after the first report sub-  
11 mitted under paragraph (1), for 3 years; and

12 (C) more frequently, as determined appro-  
13 priate by the Secretary of Homeland Security  
14 in response to new risks or technologies that  
15 emerge.

16 **SEC. 9. PREPAREDNESS OF FEDERAL COURTS TO PRO-**  
17 **MOTE CYBER SECURITY.**

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

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

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

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

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

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

10                   (D) Federal civil and criminal laws.

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

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

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

19                           (A) the nature of, methods of propagation  
20                           of, and damage caused by common cyber secu-  
21                           rity threats such as computer viruses, phishing  
22                           techniques, and malware;

23                           (B) the minimal standards of computer se-  
24                           curity necessary for responsible Internet use;  
25                           and

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

4 (2) a summary of the plans of the Secretary of  
5 Homeland Security to enhance public awareness of  
6 common cyber security threats, including a descrip-  
7 tion of the metrics used by the Department of  
8 Homeland Security for evaluating the efficacy of  
9 public awareness campaigns; and

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

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

15 (a) DEFINITIONS.—In this section—

16 (1) the term “information technology supply  
17 chain of the United States” means the public and  
18 private telecommunications networks of the United  
19 States; and

20 (2) the term “telecommunications networks of  
21 the United States” includes—

22 (A) telephone systems;

23 (B) Internet systems;

24 (C) fiber optic lines, including cable land-  
25 ings;

1 (D) computer networks; and

2 (E) smart grid technology under develop-  
3 ment by the Department of Energy.

4 (b) REPORT.—Not later than 90 days after the date  
5 of enactment of this Act, and annually thereafter, the Sec-  
6 retary of Homeland Security shall submit to Congress a  
7 report that—

8 (1) identifies foreign suppliers of information  
9 technology (including equipment, software, and serv-  
10 ices) that are linked directly or indirectly to a for-  
11 eign government, including—

12 (A) by ties to the military forces of a for-  
13 eign government; or

14 (B) by being the beneficiaries of significant  
15 low interest or no interest loans, loan forgive-  
16 ness, or other support by a foreign government;

17 (2) discusses the extent to which goods pro-  
18 duced by suppliers identified under paragraph (2)  
19 have been integrated into the information technology  
20 supply chain of the United States;

21 (3) identifies specific telecommunications net-  
22 works of the United States that include information  
23 technology identified under paragraph (1); and

24 (4) assesses the vulnerability to malicious activ-  
25 ity, including cyber crime or espionage, of the tele-

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

5 **SEC. 12. PROTECTING THE ELECTRICAL GRID OF THE**  
6 **UNITED STATES.**

7 Not later than 180 days after the date of enactment  
8 of this Act, the Secretary of Homeland Security, in con-  
9 sultation with the Secretary of Defense and the Director  
10 of National Intelligence, shall submit to Congress a report  
11 on—

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

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

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

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

○