

113TH CONGRESS
1ST SESSION

S. 21

To secure the United States against cyber attack, to improve communication and collaboration between the private sector and the Federal Government, to enhance American competitiveness and create jobs in the information technology industry, and to protect the identities and sensitive information of American citizens and businesses.

IN THE SENATE OF THE UNITED STATES

JANUARY 22 (legislative day, JANUARY 3), 2013

Mr. ROCKEFELLER (for himself, Mr. CARPER, Mrs. FEINSTEIN, Mr. LEVIN, Ms. MIKULSKI, Mr. WHITEHOUSE, and Mr. COONS) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To secure the United States against cyber attack, to improve communication and collaboration between the private sector and the Federal Government, to enhance American competitiveness and create jobs in the information technology industry, and to protect the identities and sensitive information of American citizens and businesses.

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 and
5 American Cyber Competitiveness Act of 2013”.

1 **SEC. 2. FINDINGS.**

2 Congress makes the following findings:

3 (1) The country's leading officials in business,
4 intelligence, and defense affairs agree that malicious
5 state, terrorist, and criminal actors exploiting
6 vulnerabilities in information and communications
7 networks and gaps in cybersecurity pose one of the
8 most serious and rapidly growing threats to both the
9 national security and the economy of the United
10 States.

11 (2) With information technology now the back-
12 bone of the United States economy, a critical ele-
13 ment of United States national security infrastruc-
14 ture and defense systems, the primary foundation of
15 global communications, and a key enabler of most
16 critical infrastructure, nearly every single United
17 States citizen is touched by cyberspace and is threat-
18 ened by cyber attacks.

19 (3) Malicious actors in cyberspace have already
20 caused significant damage to the United States Gov-
21 ernment, the United States economy, and United
22 States citizens, and the threat continues to grow.

23 (4) In its 2009 Cyberspace Policy Review, the
24 White House concluded, "Ensuring that cyberspace
25 is sufficiently resilient and trustworthy to support
26 U.S. goals of economic growth, civil liberties and pri-

1 vacy protections, national security, and the contin-
2 ued advancement of democratic institutions requires
3 making cybersecurity a national priority.”.

4 (5) Leading experts in the private sector and
5 the government agree that the United States should
6 establish a new model of public-private collaboration,
7 which fits the realities of the 21st century, to secure
8 the country against cyber attack.

9 **SEC. 3. SENSE OF CONGRESS.**

10 It is the sense of Congress that Congress should
11 enact, and the President should sign, bipartisan legislation
12 to improve communication and collaboration between the
13 private sector and the Federal Government to secure the
14 United States against cyber attack, to enhance the com-
15 petitiveness of the United States and create jobs in the
16 information technology industry, and to protect the identi-
17 ties and sensitive information of United States citizens
18 and businesses by—

19 (1) enhancing the security and resiliency of
20 public and private communications and information
21 networks against cyber attack by nation-states, ter-
22 rorists, and cyber criminals;

23 (2) establishing mechanisms for sharing cyber
24 threat and vulnerability information between the
25 government and the private sector;

1 (3) developing a coherent public-private system
2 to improve the capability of the United States to as-
3 sess cyber risk and prevent, detect, and robustly re-
4 spond to cyber attacks against United States critical
5 infrastructure, such as the electric grid, the financial
6 sector, and telecommunications networks;

7 (4) promoting research and development invest-
8 ments in the United States information technology
9 sector that create and maintain good, well-paying
10 jobs in the United States and help to enhance the
11 economic competitiveness and cybersecurity of the
12 United States;

13 (5) promoting cybersecurity and information
14 technology training to develop the country's next
15 generation of cyber professionals;

16 (6) preventing and mitigating identity theft and
17 guarding against abuses or breaches of personally
18 identifiable information;

19 (7) enhancing United States diplomatic capaci-
20 ty and public-private international cooperation to
21 respond to emerging cyber threats, including pro-
22 moting security and freedom of access for commu-
23 nications and information networks around the
24 world and battling global cyber crime through fo-
25 cused diplomacy;

1 (8) expanding tools and resources for inves-
2 tigating and prosecuting cyber crimes in a manner
3 that respects privacy rights and civil liberties and
4 promotes United States innovation; and

5 (9) maintaining robust protections of the pri-
6 vacy of United States citizens and their online activi-
7 ties and communications.

○