

111<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION

# S. 4021

To reduce the ability of terrorists, spies, criminals, and other malicious actors to compromise, disrupt, damage, and destroy computer networks, critical infrastructure, and key resources, and for other purposes.

---

## IN THE SENATE OF THE UNITED STATES

DECEMBER 9, 2010

Mr. CARDIN (for himself and Mr. WHITEHOUSE) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

## A BILL

To reduce the ability of terrorists, spies, criminals, and other malicious actors to compromise, disrupt, damage, and destroy computer networks, critical infrastructure, and key resources, and for other purposes.

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 “Internet and Cyberse-  
5       curity Safety Standards Act”.

6       **SEC. 2. DEFINITIONS.**

7       In this Act:

1           (1) COMPUTERS.—Except as otherwise specifi-  
2 cally provided, the term “computers” means com-  
3 puters and other devices that connect to the Inter-  
4 net.

5           (2) PROVIDERS.—The term “providers” means  
6 Internet service providers, communications service  
7 providers, electronic messaging providers, electronic  
8 mail providers, and other persons who provide a  
9 service or capability to enable computers to connect  
10 to the Internet.

11           (3) SECRETARY.—Except as otherwise specifi-  
12 cally provided, the term “Secretary” means the Sec-  
13 retary of Homeland Security.

14 **SEC. 3. FINDINGS.**

15 Congress finds the following:

16           (1) While the Internet has had a profound im-  
17 pact on the daily lives of the people of the United  
18 States by enhancing communications, commerce,  
19 education, and socialization between and among per-  
20 sons regardless of their location, computers may be  
21 used, exploited, and compromised by terrorists,  
22 criminals, spies, and other malicious actors, and,  
23 therefore, computers pose a risk to computer net-  
24 works, critical infrastructure, and key resources in  
25 the United States. Indeed, users of computers are

1 generally unaware that their computers may be  
2 used, exploited, and compromised by others with  
3 spam, viruses, and other malicious software and  
4 agents.

5 (2) Since computer networks, critical infra-  
6 structure, and key resources of the United States  
7 are at risk of being compromised, disrupted, dam-  
8 aged, or destroyed by terrorists, criminals, spies, and  
9 other malicious actors who use computers, Internet  
10 and cybersecurity safety is an urgent homeland secu-  
11 rity issue that needs to be addressed by providers,  
12 technology companies, and persons who use com-  
13 puters.

14 (3) The Government and the private sector  
15 need to work together to develop and enforce min-  
16 imum Internet and cybersecurity safety standards  
17 for users of computers to prevent terrorists, crimi-  
18 nals, spies, and other malicious actors from compro-  
19 mising, disrupting, damaging, or destroying the com-  
20 puter networks, critical infrastructure, and key re-  
21 sources of the United States.

22 **SEC. 4. COST-BENEFIT ANALYSIS.**

23 (a) **REQUIREMENT FOR ANALYSIS.**—The Secretary,  
24 in consultation with the Attorney General and the Sec-  
25 retary of Commerce, shall conduct an analysis to deter-

1 mine the costs and benefits of requiring providers to de-  
2 velop and enforce minimum Internet and cybersecurity  
3 safety standards for users of computers to prevent terror-  
4 ists, criminals, spies, and other malicious actors from com-  
5 promising, disrupting, damaging, or destroying computer  
6 networks, critical infrastructure, and key resources.

7 (b) **FACTORS.**—In conducting the analysis required  
8 by subsection (a), the Secretary shall consider all relevant  
9 factors, including the effect that the development and en-  
10 forcement of minimum Internet and cybersecurity safety  
11 standards may have on homeland security, the global econ-  
12 omy, innovation, individual liberty, and privacy.

13 **SEC. 5. CONSULTATION.**

14 In conducting the analysis required by section 4, the  
15 Secretary, in consultation with the Attorney General and  
16 the Secretary of Commerce, shall consult with relevant  
17 stakeholders in the Government and the private sector, in-  
18 cluding the academic community, groups, or other institu-  
19 tions, that have scientific and technical expertise related  
20 to standards for computer networks, critical infrastruc-  
21 ture, or key resources.

22 **SEC. 6. REPORT.**

23 (a) **IN GENERAL.**—Not later than 1 year after the  
24 date of the enactment of this Act, the Secretary shall sub-  
25 mit to the appropriate committees of Congress a final re-

1 port on the results of the analysis required by section 4.  
2 Such report shall include the consensus recommendations,  
3 if any, for minimum voluntary or mandatory Internet and  
4 cybersecurity safety standards that should be developed  
5 and enforced for users of computers to prevent terrorists,  
6 criminals, spies, and other malicious actors from compro-  
7 mising, disrupting, damaging, or destroying computer net-  
8 works, critical infrastructure, and key resources

9 (b) APPROPRIATE COMMITTEES OF CONGRESS.—In  
10 this section, the term “appropriate committees of Con-  
11 gress” means—

12 (1) the Committee on Commerce, Science, and  
13 Transportation, the Committee on Homeland Secu-  
14 rity and Governmental Affairs, and the Committee  
15 on the Judiciary of the Senate; and

16 (2) the Committee on Energy and Commerce,  
17 the Committee on Homeland Security, the Com-  
18 mittee on the Judiciary, and the Committee on  
19 Oversight and Government Reform of the House of  
20 Representatives.

○