AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

112TH CONGRESS
1ST SESSION

S. 372

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

FEBRUARY 16, 2011

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.

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 and Internet Safety Standards Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) COMPUTERS.—Except as otherwise specifically provided, the term ''computers'' means computers and other devices that connect to the Internet.

(2) PROVIDERS.—The term ''providers'' means Internet service providers, communications service providers, electronic messaging providers, electronic mail providers, and other persons who provide a service or capability to enable computers to connect to the Internet.

(3) SECRETARY.—Except as otherwise specifically provided, the term ''Secretary'' means the Secretary of Homeland Security.

SEC. 3. FINDINGS.

Congress finds the following:

(1) While the Internet has had a profound impact on the daily lives of the people of the United States by enhancing communications, commerce, education, and socialization between and among persons regardless of their location, computers may be used, exploited, and compromised by terrorists, criminals, spies, and other malicious actors, and, therefore, computers pose a risk to computer networks, critical infrastructure, and key resources in the United States. Indeed, users of computers are

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

(2) Since computer networks, critical infrastructure, and key resources of the United States are at risk of being compromised, disrupted, damaged, or destroyed by terrorists, criminals, spies, and other malicious actors who use computers, cybersecurity and Internet safety is an urgent homeland security issue that needs to be addressed by providers, technology companies, and persons who use computers.

(3) The Government and the private sector need to work together to develop and enforce minimum voluntary or mandatory cybersecurity and Internet safety standards for users of computers to prevent terrorists, criminals, spies, and other malicious actors from compromising, disrupting, damaging, or destroying the computer networks, critical infrastructure, and key resources of the United States.

SEC. 4. COST-BENEFIT ANALYSIS.

(a) REQUIREMENT FOR ANALYSIS.—The Secretary, in consultation with the Attorney General, the Secretary

of Commerce, and the Director of National Intelligence, shall conduct an analysis to determine the costs and benefits of requiring providers to develop and enforce voluntary or mandatory minimum cybersecurity and Internet safety standards for users of computers to prevent terrorists, criminals, spies, and other malicious actors from compromising, disrupting, damaging, or destroying computer networks, critical infrastructure, and key resources.

(b) FACTORS.—In conducting the analysis required by subsection (a), the Secretary shall consider—

(1) all relevant factors, including the effect that the development and enforcement of minimum voluntary or mandatory cybersecurity and Internet safety standards may have on homeland security, the global economy, innovation, individual liberty, and privacy; and

(2) any legal impediments that may exist to the implementation of such standards.

SEC. 5. CONSULTATION.

In conducting the analysis required by section 4, the Secretary shall consult with the Attorney General, the Secretary of Commerce, the Director of National Intelligence, the Federal Communications Commission, and relevant stakeholders in the Government and the private sector, including the academic community, groups, or other institu-

tions, that have scientific and technical expertise related to standards for computer networks, critical infrastructure, or key resources.

SEC. 6. REPORT.

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Secretary shall submit to the appropriate committees of Congress a final report on the results of the analysis required by section 4. Such report shall include the consensus recommendations, if any, for minimum voluntary or mandatory cybersecurity and Internet safety standards that should be developed and enforced for users of computers to prevent terrorists, criminals, spies, and other malicious actors from compromising, disrupting, damaging, or destroying computer networks, critical infrastructure, and key resources.

(b) APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the Committee on Commerce, Science, and Transportation, the Committee on Homeland Security and Governmental Affairs, and the Committee on the Judiciary of the Senate; and

(2) the Committee on Energy and Commerce, the Committee on Homeland Security, the Committee on the Judiciary, and the Committee on

Oversight and Government Reform of the House of Representatives.

○