The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3913 | APRIL 16, 2013

House Cybersecurity Legislation: A Small Step, But Flaws Need Correction

By David S. Addington

Congress has begun to consider cybersecurity legislation in earnest for the 113th Congress. The House of Representatives is scheduled to consider shortly H.R. 624, the Cyber Intelligence Sharing and Protection Act (CISPA). The bill addresses the growing problem of foreign powers infiltrating U.S. public and private computer systems to steal valuable information. The bill represents only a small step toward addressing the cybersecurity threats the country faces. The bill as ordered reported has significant flaws, but the House has the opportunity to correct them.

The bill establishes an information-sharing regime under which private sector entities may, but are not required to, share information with the government about efforts to gain unauthorized access to their computer systems. Conversely, the government may, but is not required to, share cybersecurity information under appropriate security rules with private sector entities. The bill encourages the private sector entities to share cyber threat information with the government by limiting the government's use of the information to cybersecurity-related purposes and protecting them from liability.

Protect the Privacy of Americans. The bill falls short of protecting the privacy of Americans in one major respect. Although proposed section 1104(c)(4) of the National Security Act of 1947 as contained in the bill may have been intended to protect firearms sales records, tax return records, medical records, and similar records, the provision has exactly the opposite effect. Regarding cybersecurity information that is identified with a person and is shared with the federal government under the legislation, section 1104(c)(4) says:

> The Federal Government may not use the following information . . . shared with the Federal Government . . . unless such information is used in accordance with the policies and procedures established under paragraph (7) : . . . (E) Firearms sales records. (F) Tax return records. . . . (H) Medical records.

In turn, the referenced paragraph (7) says:

> The Director of National Intelligence, in consultation with the Secretary of Homeland Security and the Attorney General, shall establish and periodically review policies and procedures governing the receipt, retention, use, and disclosure of non-publicly available cyber threat information shared with the Federal Government . . . .

The result of the interaction of sections 1104(c)(4) and 1104(c)(7) is that section 1104(c)(4) actually *affirmatively authorizes* the government to make use of firearms sales records, tax return records, and medical records shared under the legislation, as long as the government does so under rules set by the Director of National Intelligence (DNI), in consultation with the Attorney General and the Secretary of

This paper, in its entirety, can be found at
http://report.heritage.org/ib3913

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Homeland Security, pursuant to section 1104(d)(7).

Congress has long recognized the need for protection of privacy with respect to firearms sales records, tax return records, and medical records and has passed laws to protect them. Thus, for example, section 103(i) of Public Law 103-159 prohibits having a federal firearms registry, section 6103 of title 26 of the U.S. Code provides for the confidentiality of tax return records and specifies detailed requirements before intelligence agencies can have access to them, and the Health Insurance Portability and Accountability Act privacy regulations protect the confidentiality of medical records. The CISPA should not displace privacy protections under current federal law and, in particular, should not make the privacy of Americans' firearms sales records, tax records, and medical records shared under the legislation subject to whatever rules the DNI, after consulting the Attorney General and the Secretary of Homeland Security, comes up with.

The House should revise section 1104(c)(4) to make clear that nothing in section 1104 impairs or otherwise affects the protections in the Privacy Act nor provides any authority to collect under the legislation the types of information listed in section 1104(c)(4), such as firearms sales records, tax records, or medical records.

Enact Permanent Legislation or at Least Fix the Five-year Sunset Provision. Another major concern with the bill is the sunset clause in section 3 of the bill. It automatically repeals the entire bill after five years. It would be best for the Congress to enact useful cybersecurity legislation on a permanent basis.

If the legislation is to be temporary, the sunset clause must take into account that, when the five-year self-repeal occurs, the government still will be in possession of cybersecurity information shared by private entities under the legislation. Additionally, private entities still will be in possession of cybersecurity information they received from the government under the legislation. Further, claims may have arisen under the legislation and lawsuits may be underway.

It would be preferable for the House to make the legislation permanent, but if the House limits the effect of the legislation for five years, the House should revise the sunset clause to preserve in effect after five years the provisions in the bill that protect the confidentiality of and limit the use of information shared or received under the legislation and the provisions that govern legal liability and judicial process.

Allow Additional Government Uses of Cybersecurity Information Received. Section 1104(b)(3)(D) of National Security Act of 1947, as contained in the bill, provides strict limits on the uses the government can make of cybersecurity information received from the private sector under the bill. The House should consider whether to permit the government to use cybersecurity information it receives under the legislation for purposes in addition to those specifically listed in bill, such as for U.S. Secret Service protective functions under section 3056 of title 18 of the U.S. Code and for continuity of government purposes in emergencies. The government's freedom under the legislation to use the cybersecurity information it receives should not be too broad, but it should not be too narrow, either.

Conclusion: Fix the Flaws and Stick with a Model of Government–Private Sector Cooperation. With the correction of the flaws outlined above, House passage of the CISPA legislation would mark a small step forward on the long path toward achieving the cybersecurity of the United States. But that small step will go for naught if the Senate persists in its effort of the last Congress to enact legislation to regulate rather than cooperate with the private sector on cybersecurity. The command approach of government regulation will never keep pace with the ever-changing world of cybersecurity; cooperation between government and the private sector holds out the best hope for prompt progress on cybersecurity. If the House and Senate meet in conference on cybersecurity legislation later in the current Congress, the House approach of cooperation between the government and the private sector should prevail.

*—**David S. Addington** is the Group Vice President for Research at The Heritage Foundation.*