WebMemo
Published by The Heritage Foundation
No. 3300
June 27, 2011

# Obama Cybersecurity Proposal Flawed, But Fixable

*Paul Rosenzweig*

In May, the Administration unveiled a legislative proposal for cybersecurity that is now working its way through Congress. It is one of several major legislative packages offered that seek to enhance the security and resilience of the nation's cyber infrastructure. Getting the federal government's role right in cybersecurity is crucial. One of the key principles in addressing any proposed law is that Congress should take its time and get the solution right. What Washington does online should enhance the security, freedom, and prosperity of Americans in equal measure. The Administration's proposal does not adequately address all these priorities.

**Positives in the Proposal**. For too long, national companies have been faced with a proliferation of state laws that require service providers to notify their customers whenever they suffer a data breach and the disclosure of personal information. Today, there is a patchwork of laws in 47 of the 50 states, each a little different. In this truly national—indeed, international—market, the Administration is wise to propose a uniform federal standard.

Sometimes private-sector actors voluntarily seek the government's assistance in dealing with cyber intrusions. However, the law is often unclear as to whether the government (for example, the Department of Homeland Security) has the authority to give the private sector the assistance it wants. That does not make sense, and the Administration proposal wisely clarifies it.

**Room for Improvement: Catching Cyber Criminals.** The Administration has proposed to increase penalties for computer criminals. In general, those who use the Internet to deliberately target American infrastructure or command and control systems should be punished harshly. But caution is necessary: The Computer Fraud and Abuse Act (CFAA), which penalizes criminal computer conduct, is remarkably broad and ill-defined. Some examples of its use are good examples of what we have previously called the phenomenon of "over-criminalization"—making a crime out of anything. Before Congress enhances the penalties for violating the CFAA, it needs to fix the underlying criminal law so that it applies only to true criminals.

**Encourage Information Sharing.** Often private-sector actors have information that they want to share with the government about a threat they have discovered. But existing law—principally the Electronic Communications Privacy Act (ECPA)—is sometimes said to prevent the private sector from sharing information with the government if that information can identify individuals. That reading of the ECPA is probably wrong, but the ambiguity in the law has made Internet Service Providers cautious. The Administration is wise to move to eliminate that ambiguity.

This paper, in its entirety, can be found at:
*http://report.heritage.org/wm3300*

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

There is a problem, however, with the proposal: The Administration's legislation focuses only on private-to-government sharing of information, as if the government were the only solution to cybersecurity. It is not. The private sector can and should self-organize, sharing information among service providers, as a way of enhancing cybersecurity. But the draft proposal is silent on information sharing between private-sector actors. By affirming private-to-government information sharing to protect an information system, the law is likely to be taken as prohibiting or limiting such sharing amongst private-sector actors. If it is read in that way, the draft proposal will have done actual harm. It needs to be modified before it is enacted.

**Avoid Unnecessary Bureaucracy.** The Administration's proposal would speed the deployment of intrusion prevention systems that can actually block cyber intrusions and attacks against government computers. The proposal would confirm that the Department of Homeland Security (DHS) is responsible for overseeing the intrusion prevention systems for all federal executive branch civilian computers. It would also streamline the process by which Internet Service Providers (ISPs) that implement these systems on behalf of DHS are immunized from liability for their assistance to the government.

Where the proposal goes wrong, however, is in the imposition of burdensome congressional reporting, an annual certification requirement, and unnecessary privacy and civil liberties protections. The proposal applies only to intrusion prevention systems that protect government computers, yet it is laden with privacy protections. The Department of Justice concluded rightly that no person sending information to government has an expectation of privacy in his communications—after all, he *wanted* the government to read the mail he was sending. The additional protections are merely extra bureaucracy that will only slow the development and deployment of effective intrusion detection systems.

**Public-Private Cooperation, Not Government Dictates**. Under the Administration's proposal, DHS would take a much stronger regulatory role in managing cybersecurity in the private sector. Working with industry, DHS would identify certain core critical infrastructure operators (presumably things like the electric grid and the financial markets) and then develop a priority list of the most important cyber threats and vulnerabilities for those operators.

Using those priority lists, the infrastructure operators would be required to develop their own plans to address cyber threats and have them assessed by a third-party commercial auditor. Some operators would also be required to report to the Security and Exchange Commission and certify that their plans are sufficient. Third-party auditors would be responsible for assessing service provider compliance. If DHS decides that a security framework adopted by a critical infrastructure sector is not adequate, DHS would be authorized to work with the National Institute of Standards and Technology (NIST) to mandate a modified framework. Finally, DHS would be authorized to publicly name critical infrastructure providers whose plans it deemed inadequate.

This proposal creates a regulatory maelstrom. It was apparently adopted with little or no private-sector consultation. It would enshrine a structure of prioritization and regulatory development that would, inevitably, be far behind the technological curve. And, in the end, it holds out the specter of a federal government dictating security standards to a private industry that is far more nimble and innovative than the government can ever be.

The security of the private sector can be improved, and private-sector cybersecurity is of vital interest to the federal government. However, cybersecurity cannot come as a dictate from DHS and NIST. It can be provided only through public-private cooperation. This aspect of the Administration's proposal misses the mark by a wide margin.

**Revisions Needed.** The Administration's proposal is a good starting point for discussion. Congress needs to evaluate the proposal on its merits and revise it consistent with sound conservative principles.[1] Congress should:

1. Paul Rosenzweig, "10 Conservative Principles for Cybersecurity Policy," Heritage Foundation *Backgrounder* No. 2513, January 31, 2011, at *http://www.heritage.org/research/reports/2011/01/10-conservative-principles-for-cybersecurity-policy.*

- Hold detailed hearings on all aspects of the proposal, closely examining, in particular: the criminal provisions, the private-sector information-sharing proposals, and the regulatory proposal for critical infrastructure;
- Insist on modifications to the proposal that enhance capacity for true public-private partnership in the development of cybersecurity without putting private industry in a federal straitjacket; and
- Pass solid cybersecurity legislation only if it enhances America's defenses without compromising innovation. It would be better to have no legislation at all than to pass harmful legislation that compromises U.S. competitiveness.

*—**Paul Rosenzweig** is Visiting Fellow in the Center for Legal & Judicial Studies and the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.*