The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3675 | JULY 24, 2012

Cybersecurity Act of 2012: Revised Cyber Bill Still Has Problems

Paul Rosenzweig

Senators Joseph Lieberman (I–CT) and Susan Collins (R–ME) recently released a revised version of their Cybersecurity Act of 2012. The expectation is that Senate leadership will attempt to bring the bill to the floor before the August recess. Though an able effort, the revised bill still has grave problems that are likely to chill innovation without improving cybersecurity.

The Regulatory Morass. The original bill would have assigned the Department of Homeland Security (DHS) the role of creating mandatory cybersecurity standards for critical infrastructure industries.[1] To its authors' credit, the bill moves away from that mandatory system, but it still has far too great an intrusive federal role in defining cybersecurity standards.

The revised bill still requires the creation of industry best practice standards for protecting critical infrastructure. Instead of making those standards mandatory, it pushes the owners of critical infrastructure to adopt new "voluntary" standards. Those incentives include liability protection, priority assistance for cyber threats, and access to classified information about threats.

There are several problems with this new approach. First, the government should not be in the position of denying its threat information to critical infrastructure owners who choose not to adopt the voluntary standards, likely for justifiable business reasons. If the infrastructure in question is truly "critical," it is in America's collective interest to protect it as much as possible.

Second, the liability protections provided as an incentive are far too weak. If a company adopts the voluntary standards, it could still be sued for consequential damages. All it gains is protection against punitive damages, which it would almost certainly obtain anyway for any reasonable effort at providing cybersecurity. Additionally, these government standards would likely form the basis for lawsuits against those who do not adopt them, giving business to trial lawyers at the expense of real security.

Third, voluntary standards would stifle innovation and likely be obsolete by the time they are written. Over the multi-year process when standards are being written and adopted, innovation and investment in cybersecurity products will cease. No thoughtful investor will invest in a product that might *not* be one of the standard-approved methods of providing cybersecurity, even if it might be a better one. Given the government's own track record of combating cyber threats and the glacial pace at which it develops rules and regulations, there is good reason to be deeply skeptical that the government can set the right standards in a dynamic environment such as cybersecurity.[2]

Finally, a voluntary standard system is a short step from a mandatory one. Senator Lieberman has already said that if industries do not adopt the voluntary standards, Congress will make them do so. Indeed, it appears that the "voluntary standards" may not even be voluntary after all. Under section 103(g) of the bill, federal regulatory agencies are free to make the voluntary regulations mandatory in the sectors they regulate, and they are required to report to Congress if they choose not

This paper, in its entirety, can be found at **http://report.heritage.org/ib3675**

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

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

to do so—which is a strong incentive to adopt the "voluntary" rules.

Information Sharing Weakened. The other critical portion of the bill is the set of information-sharing provisions. This bill continues the earlier focus of the prior version on the creation of cybersecurity exchanges in the federal government for sharing threat and vulnerability information. As drafted, the bill is likely to fail to achieve these modest objectives.

The bill requires the creation of a federal civilian cybersecurity information exchange, presumably led by DHS. The idea of strengthening DHS's role in this program is laudable, but the bill deliberately excludes the possibility that the Department of Defense and/or the National Security Agency might also operate an exchange. While there is a legitimate reason for concern over the militarization of cyberspace defense, it seems highly inefficient and ineffective to require all defense efforts go through DHS to get information in all cases. Surely there must be a subset of cases where direct military engagement is both appropriate and even necessary.

Additionally, the bill would limit the sharing of cyber threat information with other federal agencies, recreating the stovepipes that contributed to the 9/11 attacks. This is a step backward. The cyber exchanges may disclose information to law enforcement only to prevent a cyber threat, to combat an imminent threat of death or serious bodily injury, or to protect minors—e.g., from child pornography. While these are clearly important goals, the bill prohibits sharing with law enforcement for other equally or more important reasons, such as to protect the nation from a biological threat or to combat serious crime, such as that of Mexican drug cartels.

The bill also authorizes lawsuits against the U.S. government for violations of the limitations and authorizes the award of attorney's fees. This inclusion is clearly an attempt to create an incentive for lawsuits, which would chill information sharing.

A final and serious weakness is that the bill provides insufficient liability protection for the private-sector actors who share information. The bill protects only those who act in good faith and without gross negligence. Any clever lawyer can find a way to sue, and the private-sector actors are at risk of years of long litigation with all of the attendant costs. This provision alone is likely to ensure that nobody shares cyber threat information at all for fear of being sued.

The Way Forward. Congress should reject any effort to create a new regulatory system for cybersecurity. Furthermore, it should strengthen protections for private-sector actors in order to authorize and incentivize the sharing of cyber threat and vulnerability information. As drafted, the new offering from Senators Lieberman and Collins does neither of these things.

*—**Paul Rosenzweig** is a 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.*

1. See Paul Rosenzweig, "Senate Cybersecurity Bill: Not Ready for Prime Time," Heritage Foundation *Backgrounder* No. 2661, March 7, 2012, http://www.heritage.org/research/reports/2012/03/senate-cybersecurity-bill-not-ready-for-prime-time.
2. See Paul Rosenzweig, "The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government," Heritage Foundation *Backgrounder* No. 2695, May 24, 2012, http://www.heritage.org/research/reports/2012/05/the-alarming-trend-of-cybersecurity-breaches-and-failures-in-the-us-government.