The Heritage Foundation
LEADERSHIP FOR AMERICA

BACKGROUNDER

No. 2661 | MARCH 7, 2012

Senate Cybersecurity Bill: Not Ready for Prime Time

Paul Rosenzweig

Abstract
The Senate has introduced the Cybersecurity Act of 2012. A floor vote is expected in March or April. The Cybersecurity Act contains laudable elements—enhancement of and protection for private-sector information sharing are crucial. The act's new regulatory provisions, however, would create a new system of—potentially harmful and expensive—government controls. Furthermore, too many components remain undefined, leaving the door open to uncertainty. Improvements for information sharing should not be contingent on regulation. Congress should pursue a step-by-step approach to cybersecurity, with alleviating burdens on sharing information in the private sector constituting the first step. A regulatory structure—if needed—can be built as a next step.

This paper, in its entirety, can be found at **http://report.heritage.org/bg2661**

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

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

Cybersecurity legislation is one of the big issues in Washington that might actually see progress this year. Weighing in at 205 pages, the Cybersecurity Act of 2012 (S. 2105), is currently one of the primary cybersecurity bills before Congress.[1] Hearings have been held and Senate Majority Leader Harry Reid (D–NV) promises to bring the bill to the floor during the next work period in March or April.

Provisions of the bill that enhance information sharing, which allow members of the private sector to share threat and warning information with other private-sector actors without fear of being sued, are a solid improvement over current law. The new regulatory provisions, however, will create a new system of government control and are not well justified. The better course is to take one step at a time and allow information sharing now, and then create the regulatory structure if it is needed down the road.

Improving the Sharing of Threat Information

The Cybersecurity Act of 2012 recognizes that privacy rules, antitrust laws, and fears of liability preclude private-sector actors from effectively monitoring their cyber

Talking Points

- The Cybersecurity Act of 2012 is currently one of the primary cybersecurity bills before Congress.
- Provisions of the Cybersecurity Act that enhance information sharing, which allow members of the private sector to share threat and warning information with other private-sector actors without fear of being sued, are a solid improvement over current law.
- The new regulatory provisions, however, would create a new system of government control. The better course is to take one step at a time and allow information sharing now—and create the regulatory structure if it is needed down the road.
- The authors of the Cybersecurity Act are to be commended for wisely promoting information sharing and even attempting to avoid the usual pitfalls of regulation through a novel, outcome-oriented process. This attempt, however, falls short, and the regulatory program will be the main field of conflict in the next few weeks.

systems and systems for which they provide cybersecurity. Furthermore, when they do locate threats, they currently are legally barred from sharing threat information with other private-sector actors.

Section 701 of the act removes those onerous legal barriers and permits private entities to monitor and defend their own systems and the systems of third parties who authorize them to act on their behalf. Section 702 further promotes sharing by allowing private-sector entities to voluntarily share cyber threat information among themselves. To guard, presumably, against collusion on other matters, shared information can only be used to protect information systems, and personally identifiable information (PII) must be reasonably safeguarded. Together, these two sections are likely to achieve a great deal of voluntary private-to-private sharing, much like two pending House bills.[2]

Section 703 creates at least one "lead Federal cybersecurity exchange" to facilitate and encourage information sharing with both federal and private-sector entities. In addition, the Department of Homeland Security (DHS) may designate additional exchanges, which could be run by federal or non-federal entities. Since DHS already runs the "lead" exchange, it is unclear if this addition will meaningfully increase information sharing.[3] Section 704 authorizes private entities to disclose cyber threat information to these new exchanges. In return, the information provided is exempt from the Freedom of Information Act (FOIA), does not waive any legal privilege, and is exempt from rules against ex-parte communications.

Disclosure of cyber threat information to law enforcement is limited. The bill allows threat disclosure only when a crime "has been, is being, or is about to be committed," and then only in conformance with a set of privacy and civil liberties protection procedures that the Homeland Security Secretary is charged with developing. To ensure that the impact on privacy and civil liberties is minimized, the Attorney General, the DHS and Justice Department privacy officers, and the Privacy and Civil Liberties Oversight Board will oversee compliance with these procedures. The authors of the bill seem genuinely concerned with privacy protections, but some groups worry these protections might not be enough.[4]

Other important sections regarding information sharing are 706 and 707. Section 706 creates a limitation on liability: No lawsuit may be filed against actors who, in accordance with this bill, voluntarily disclose cyber threat information as long as the actors proceeded in good faith. A liability waiver is also provided for the reasonable failure of a private entity to act on information received.[5] The only unfortunate exception to this rule is the retention of a private right of action against private-sector entities for failing to maintain the security of personally identifiable information or the misuse of shared information. In an ideal bill, those sorts of suits would also be prohibited.[6]

Section 707 supports information-sharing provisions by providing a federal preemption rule that expressly preempts all contrary state or local laws.[7] In a nod to anti-trust concerns, price-fixing and market-allocation allegations are not included in the preemption and remain legitimate grounds for litigation.

1. "Lieberman, Collins, Rockefeller, Feinstein Offer Bipartisan, Comprehensive Bill to Secure Fed and Critical Private Sector Cyber Systems," U.S. Senate Committee on Homeland Security and Governmental Affairs, February 14, 2012, at *http://www.hsgac.senate.gov/media/majority-media/lieberman-collins-rockefeller-feinstein_offer-bipartisan-comprehensive-bill-to-secure-fed-and-critical-private-sector-cyber-systems* (March 5, 2012).
2. Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness (PRECISE) Act of 2011 (H.R. 3674) and the Cyber Intelligence Sharing and Protection Act of 2011 (H.R. 3523).
3. Paul Rosenzweig, "Information Sharing and the Cybersecurity Act of 2012," *Lawfare*, February 14, 2012, at *http://www.lawfareblog.com/2012/02/information-sharing-and-the-cybersecurity-act-of-2012/* (March 5, 2012).
4. Elinor Mills, "Civil Liberties Groups: Proposed Cybersecurity Bill Is Too Broad," CNet News, February 23, 2012, at *http://news.cnet.com/8301-27080_3-57384137-245/civil-liberties-groups-proposed-cybersecurity-bill-is-too-broad/* (March 5, 2011).
5. The Cyber Security Act of 2012, S. 2105, 112th Congress, 2nd Sess., pp. 173–175.
6. Gus P. Coldebella, "Cybersecurity Act of 2012 Requires a Liability Protection Bug Fix," *The Hill*, February 22, 2012, at *http://thehill.com/blogs/congress-blog/technology/212049-cyber-security-act-of-2012-requires-a-liability-protection-bug-fix* (March 5, 2012).
7. Howard W. Waltzman, "Worldwide: The Proposed 'Cybersecurity Act of 2012' Would Impact Owners and Operators of Critical Infrastructure," Mondaq, February, 17, 2011, at *http://www.mondaq.com/unitedstates/x/165592/International+Trade/The+Proposed+Cybersecurity+Act+of+2012+Would+Impact+Owners+and+Operators+of+Critical+Infrastructure* (March 5, 2012).

The Cybersecurity Act reflects a general convergence of opinion in Congress that information can best be shared by authorizing private-to-private-sector sharing, a rejection of the Obama Administration's proposal to centralize information sharing through the government. The act also reflects a broad consensus that in order for private-sector information sharing to be effective, it must be protected from liability under federal and state laws—a consensus that is sure to generate some pushback from civil libertarians.[8] Their resistance should not derail this initiative. The need for greater sharing of information is vital, and the strong oversight provisions offer a good answer to privacy concerns.

A Regulatory Leviathan

The basic philosophy of the regulatory provisions is relatively novel—they set performance standards rather than specific technological mandates for cybersecurity. Though there is reason to be skeptical even of this prospect, one should acknowledge that a more intrusive measure might have been considered and that the chosen method is, in some ways, a unique effort and a decided change from traditional programs.[9]

There are three questions that should be asked of this new regulatory regime: (1) Which systems will have to meet the new performance standards? (2) How will the standards be set? (3) How will the standards be enforced?

Defining Covered Systems. The new regulatory system defines "covered systems" as those whose failure would cause catastrophic interruption of life-sustaining services, catastrophic economic damage, or severe degradation of national security capabilities. The bill creates a two-stage process for determining which systems and services fall into this category. First, the Homeland Security Secretary is directed to conduct a sector-by-sector analysis to determine which sectors are at greatest risk of cybercrime. Presumably, this analysis will both determine which systems are critical (e.g., the electric grid) and which systems have already taken significant steps to counter a cyber attack (e.g., the financial sector).

The Homeland Security Secretary will then develop a process for designating critical systems within a sector. The actual designation will begin with the most at-risk systems and assets in the most critical and at-risk sectors. For example, larger electrical grids will likely precede smaller ones based on the size of the population they serve. Owners of such systems may challenge their designation as critical through a civil action in federal court.[10]

The bill starts from a reasonable premise by limiting the authority to regulate cybersecurity systems to "covered critical infrastructure" and then defines that infrastructure as a system or asset where "damage or unauthorized access to that system or asset could result in" the following:

- "the interruption of life-sustaining services, including energy, water, transportation, emergency services, or food, sufficient to cause"
  1. "a mass casualty event comparable to the consequences of a weapon of mass destruction," or
  2. "mass evacuations of a major population center or a large geographic area in the United States,"
- "catastrophic economic damage to the United States including":
  1. "failure or substantial disruption of a United States financial market,"
  2. "incapacitation or sustained disruption of a financial system," or
  3. "other systemic, long-term damage to the United States economy," or
- "severe degradation of national security or national security capabilities, including intelligence and defense functions."[11]

8. Rosenzweig, "Information Sharing and the Cybersecurity Act of 2012."
9. Paul Rosenzweig, "The Regulatory Provisions of the Cybersecurity Act of 2012," *Lawfare*, February 19, 2012, at *http://www.lawfareblog.com/2012/02/the-regulatory-provisions-of-the-cybersecurity-act-of-2012/* (March 5, 2012).
10. *Ibid.*
11. The Cyber Security Act of 2012, p. 16.

The first problem with this structure is that it depends on the ability of the new regulatory system to establish sound regulations. As written, this definition will require greater elaboration, since it is unclear if systems such as agriculture will be covered.

Stewart Baker, former General Counsel of the National Security Agency, and former Assistant Secretary for Policy at DHS, noted in his 2012 testimony before the Senate that limiting coverage to systems whose failure will cause an "extraordinary number" of fatalities is strange.[12] What constitutes an "extraordinary" number? Understandably, the drafters of this bill want to avoid the charge that they are expanding cybersecurity regulation to cover every last cyber system in America, but it remains a disconcerting point.

A greater concern is the great "carve-out" that gives a direct waiver from coverage to a particular subset of the economy. The bill text reads:

> The following commercial items shall not be designated as covered critical infrastructure: (a) a commercial information technology product, including hardware and software; and (b) any service provided in support of a product specified in subparagraph (a), including installation services, maintenance services, repair services, training services, and any other services provided in support of the product.

In other words, the entire architecture of the Internet is excluded from regulation. Companies and products such as Oracle, Cisco, Intel, Hewlett-Packard, and Facebook are, or at least seem to be, "commercial information technology" products that are exempt from regulation. The bill seems to put the entire regulatory burden on the end users—people in the financial industry, the electric utility industry, and such—rather than on any of the Internet service providers (ISPs).[13]

Supporters of the bill claim that this exclusion for commercial information technology is not really an "exclusion," but a point of emphasis that reflects the philosophy of the bill—that government should not be in the business of regulating software and hardware performance. Instead of mandating that Microsoft fix a bug in Internet Explorer (IE), for instance, the bill's supporters want to set performance security standards for industry and then let industry and the marketplace figure out the best way to meet those standards.[14]

Thus, if the most cost-effective measure is for industry to demand a debugged IE program, industry will do so, and Microsoft, presumably, will provide a debugged IE or lose the business. But if the best way is simply to start disconnecting critical systems from the Internet, known as "air gapping," then that is what the private sector will do. So, the point of the exclusion is to make clear that particular solutions are not mandated, but particular results are mandated. While this is a reasonable explanation, it still leaves two points of uncertainty.

First, the argument for not managing software or hardware development ignores the reality of cyber vulnerability. A large amount of the malicious activity that takes place in cyberspace occurs because of gaps in underlying coding. Indeed, one cyber expert recently stated that the single most effective "bang for the buck" measure that the U.S. could do to improve cybersecurity is simply exile all of the old, security-gap laden programs, such as Widows ME and early versions of Internet Explorer.[15] Ignoring an effective answer does not appear to be a good approach.

On the other hand, it would also be unwise to empower government bureaucrats to tell Microsoft and Apple how to upgrade their operating systems. This aspect of the exclusion seems debatable, but certainly plausible.

Second, it is unclear whether the carve-out would also exempt the major ISPs, which operate the large backbone services of the Internet, from the definition of covered infrastructure. It would be wrong to say that Verizon, Comcast, Sprint, and the other major backbone operators

12. Lolita C. Baldor, "Experts Urge Stronger Online Regulation Bill," Boston.com, February 16, 2012, at *http://articles.boston.com/2012-02-16/business/31068147_1_computer-security-power-plants-cybersecurity* (March 5, 2012).
13. Paul Rosenzweig, "The Cybersecurity Carve Out?" *Lawfare*, February 13, 2012, at *http://www.lawfareblog.com/2012/02/the-great-cybersecurity-carve-out/* (March 5, 2012).
14. *Ibid.*
15. Communication with author on February 15, 2012.

were not critical to the American economy. Indeed, the bill's supporters are confident that the definition includes the backbone operators, and that using the procedures outlined in the bill they would be eligible for designation.[16] The carve-out for "commercial information technology products" seems to include Internet backbone services, which are sold wholesale and commercially to a host of purchasers.

The definitions in the bill do not provide additional clarity. Under section 2(1) of the bill, a commercial information technology product is defined as "a commercial item that organizes or communicates information electronically." ISPs do that.

Then, a commercial item is defined by cross-reference to 41 USC 103 as "an item, that—(1)(A) is of a type customarily used by the general public or by nongovernmental entities for purposes other than governmental purposes." That is where the ambiguity creeps in—the ISP backbone is "used" by the general public (people use it to read articles online, for instance). But "used" in this context might mean "marketed to"—a requirement that might not include the ISP backbone.

To add to the confusion subsection 103(6) states that "commercial items" include "services offered and sold competitively, in substantial quantities, in the commercial marketplace based on established catalog or market prices for specific tasks performed or specific outcomes to be achieved and under standard commercial terms and conditions." This strongly appears to include the transmission services that ISP backbone companies provide.

The bill's supporters are quite confident that the ISP backbone can be a critical piece of infrastructure. This is a good idea, but an idea that does not match the bill text. If the intent of the bill is to include Internet transmission service providers as covered critical infrastructure, the language likely requires some tweaking. Either way, the uncertainty of the language makes it clear why a comprehensive approach is so fraught with peril—the unintended consequences are never fully known.

Finally, the bill attempts to further limit the scope of its regulations by specifying that the new performance standards will not apply if the critical infrastructure system or asset is already adequately regulated by another federal agency. If the Homeland Security Secretary believes that the cybersecurity regulations for the electric grid put in place by the Federal Energy Regulatory Commission (FERC) are adequate, the Secretary will not override them. Likewise, performance standards will not apply if the owner of the critical infrastructure has already taken the necessary steps to protect his critical system or asset from a cyber attack.

These two exclusions, for adequate regulation by another body and for taking voluntary steps to protect one's system, are not clear exclusions. For one thing, it is evident that critical systems will have to meet some standard of protection, and whether or not they have done so adequately will, ultimately, be judged by the Homeland Security Secretary. Thus, the "adequacy" of alternatives will, inevitably, converge to whatever standards DHS sets, and DHS will have the final word in defining them.[17]

James Lewis of the Center for Strategic and International Studies testified that, by definition, the entire process of creating a protected list creates an unprotected list and is a "bit like writing a targeting list of our opponents."[18] There is no way to avoid that problem unless, again, one expands this regulatory structure to be the structure for everything. The reality is that it is not possible to protect all systems all the time.

No Strategy for Setting Standards

The bill tasks the Homeland Security Secretary with developing cybersecurity performance requirements. In doing so, the Secretary will consider existing regulations, performance requirements developed by the private sector, and any other industry standards and guidelines identified through a review of existing practices. Once that review of the practices, regulations, and performance requirements is completed, the Secretary will next consider whether they are "adequate." If they are not, the Secretary, in consultation with the private sector, will develop, on a sector-by-sector basis, risk-based cybersecurity performance requirements for owners of "covered" critical infrastructure.

Finally, section 104(g) of the act provides that the Secretary, "in

16. Rosenzweig, "The Cybersecurity Carve Out?"
17. Rosenzweig, "The Regulatory Provisions of the Cybersecurity Act of 2012."
18. Baldor, "Experts Urge Stronger Online Regulation Bill."

developing performance requirements shall take into consideration available resources and anticipated consequences of a cyber attack." This sounds like a cost-benefit-analysis requirement—which would be a good idea. But it might also be merely a watered-down risk assessment with a predetermined conclusion. The main criticism of this section is likely to be that implementation will simply cost too much. The U.S. Chamber of Commerce believes as much, though Secretary of Homeland Security Janet Napolitano disagrees. The truth is that nobody has any real idea.[19]

Though superior to a command-and-control system of rules, the problem with the novel performance standards approach is that the legislation is merely an agreement to agree. It is a command to begin a process that identifies standards of cybersecurity protection. No one knows what those standards might be in the end, and until the standards are defined, it is impossible to know how owners will achieve them. Thus, no estimates can reasonably predict what the costs of compliance will be. They might be cheap and easy to implement if all it takes is to "air gap" some critical systems. On the other hand, they might be extremely expensive and complex if the only way to achieve compliance is to deploy a suite of sophisticated intrusion-detection systems.[20]

The mandate to create a performance requirement has a number of caveats that are intended to moderate their stringency, such as consultation with industry, deferral to existing best practices, and consideration of cost. But, ultimately, the commitment to a performance standard is a great unknown.

Finally, since cyberspace is currently an offense-dominated space, it is likely that the most effective method of dealing with cyber vulnerabilities is to prepare for failure, that is, to establish plans for continuity of operations.[21] It is fair to characterize the bill as focused far more on attack prevention than it is on recovery from attack, since the only real mention of resilience is in section 105(b)(1)(C). There, the bill briefly mentions that the performance requirements are to include rules requiring owners to "develop or update continuity of operations and incident response plans."

Enforcement. Section 105(c) contains the enforcement provisions of the bill. They require owners of covered critical infrastructure to annually prove that they have taken adequate steps to satisfy the cybersecurity performance requirements.[22] Either self-certification or third-party assessments will be accepted; though, since the third-party assessment industry is virtually non-existent at the moment, self-certification is likely to be the norm at least initially.

This section also states that the DHS regulations are to allow civil enforcement action and monetary penalties against operators of covered infrastructure who do not comply with the regulations and "remediate the violation within an appropriate time." What an "appropriate time" means is still unknown, since the legislation is essentially a command to DHS to start crafting rules.

The Regulatory Time Line. Stewart Baker testified that "a company that simply exercises rights conferred by the title could delay any cybersecurity measures for eight to ten years after enactment."[23]

There are two ways to think about that sort of time line. One is to suggest that it is too long and that, therefore, government needs authority to act more quickly. The other, conservative view is to realize that the regulatory process is too slow for this cyber environment and that the process and possible results are not worth the time, money, and effort spent trying to implement them. Either way, the regulatory reality is daunting.

19. Chris Strohm, "Napolitano Counters Industry on Cost of Cybersecurity Bill," Bloomberg Businessweek, February 21, 2012, at *http://www.businessweek.com/news/2012-02-16/napolitano-counters-industry-on-cost-of-cybersecurity-bill.html* (March 5, 2012).
20. Rosenzweig, "The Regulatory Provisions of the Cybersecurity Act of 2012."
21. *Ibid.*
22. Stephen M. Spina and J. Daniel Skees, "Cybersecurity Act of 2012 Introduced," *The National Law Review*, February 21, 2012, at *http://www.natlawreview.com/article/cybersecurity-act-2012-introduced* (March 5, 2012).
23. Stewart Baker, "Securing America's Future: The Cybersecurity Act of 2012," testimony before the Committee on Homeland Security and Government Affairs, U.S. Senate, February 16, 2012, at *http://www.hsgac.senate.gov/hearings/securing-americas-future-the-cybersecurity-act-of-2012* (March 5, 2012).

First: Do No Harm

The proposed Cybersecurity Act of 2012 attempts to craft a sound solution to a critical problem, but fails to fully achieve that goal. As is, it may also cause more harm than good. A better method would be to approach cybersecurity step by step. Congress should:

- **Preserve the cyber threat information-sharing provisions.** The focus of any cyber legislation should be the protection and promotion of sharing cyber threat information. The bill removes legal barriers and ambiguities that would otherwise prevent private-sector actors from sharing information about current threats with other private-sector actors and the government. It also creates a cybersecurity exchange so that different actors can share threat information in one place. These changes should be kept in the bill since they will give private and government entities greater access to threat information so that they can better prepare and respond to threats.

- **Maintain limited liability for sharing threat information.** The Cybersecurity Act of 2012 encourages information sharing by heavily limiting the liability that private actors face when they share information in accordance with this bill. If actors do not fear a lawsuit for sharing threat information in good faith, they will be more likely to share. These provisions might scare some privacy groups, but more than adequate oversight is given. Provisions limiting liability will greatly increase cyber threat sharing and should be kept intact in this bill.

- **Reconsider the regulatory regime.** In its current form, the Cybersecurity Act of 2012 creates too many regulatory costs and unknowns. The costs that these regulations might place on the economy are simply unknown at this point (since they have yet to be written), but they could easily be enormous. Furthermore, technology develops at such a fast rate that the regulations might quickly become outdated or untenable. Regulations are likely to hurt more than help and should be avoided until the results of information sharing are seen.

What Lies Ahead

The authors of the Cybersecurity Act of 2012 are to be commended for wisely promoting information sharing and even attempting to avoid the usual pitfalls of regulation by using a novel, outcome-oriented process. This attempt, however, falls short, and the regulatory program will be the main field of conflict in the next few weeks.

There seems to be an emerging consensus that information sharing is important, but not that a regulatory program is needed. As Senator John McCain (R–AZ) said, the Republican alternative bill will "aim to enter into a cooperative relationship with the entire private sector through information sharing, rather than an adversarial one with prescriptive regulations."[24] It remains to be seen whether the disagreement over a regulatory structure means that the Senate will also be unable to agree on the much-needed information-sharing provisions.

—Paul Rosenzweig *is a Visiting Fellow in the Center for Legal & Judicial Studies and in 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.*

24. Strohm, "Napolitano Counters Industry on Cost of Cybersecurity Bill."