The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3626 | JUNE 5, 2012

Ensuring Cybersecurity: More Red Tape Is Not the Answer

James L. Gattuso

Over the past several years, U.S. businesses and the American economy have faced an unprecedented surge of new regulations, ranging from new health care mandates and environmental rules to Dodd–Frank financial industry controls to "net neutrality" rules on communications providers.[1] Now Congress is considering imposing yet another new set of burdens on American enterprise.

Under legislation now pending in the Senate, S. 2105—sponsored by Senators Joe Lieberman (I–CT) and Susan Collins (R–ME)—an unspecified number of U.S. industries would be required to comply with government-crafted cybersecurity "performance requirements." The cost of this new mandate is unknown but is likely to be large in terms of direct compliance and lost innovation and growth in the affected industries. Cybersecurity is important, and threats to security are real, but Congress should carefully consider whether more regulatory mandates provide an effective solution.

Putting Government in Charge of Cybersecurity. Few doubt that cybersecurity (the protection of a computer system from unauthorized access or attack) is a serious issue. With threats ranging from individual hackers to state-sponsored espionage to terrorists, preserving cybersecurity is a constant—and constantly changing—challenge. Recognizing the harm that cyberattacks can do to their bottom lines, private-sector enterprises under threat have long made cybersecurity a priority. The government, of course, has a fundamental role in protecting security, but there is little evidence that it special knowledge or capability to address the threats. In fact, in the management of its own computer systems, the government has been no better—and arguably worse—than the private sector.[2]

Despite this, the proposed Cybersecurity Act of 2012 could effectively put the federal government—specifically the Department of Homeland Security (DHS)—in charge of U.S. cybersecurity efforts. Under the legislation, the DHS Secretary is required to identify "critical infrastructure" vulnerable to cyber threats (a decision to be made with the "input" of the infrastructure's owners). These would be "critical" assets and systems for which damage could cause "mass casualties," "mass evacuations," or "catastrophic damage to the economy."

At first glance, this wording seems narrow, limiting the "critical infrastructure" designation to a few key facilities and systems,[3] but the language is actually much broader and more ambiguous. "Mass causalities," for instance, specifically includes events with an "extraordinary" number of fatalities, but how many fatalities are "ordinary"? Are five deaths ordinary? Are 10 extraordinary?[4]

Similarly, "catastrophic damage to the economy" includes "failure or substantial disruption" of "a U.S.financial market" or "transportation system." Does that include the disruption of any exchange, no matter how small? The failure of a single derivatives exchange? Is every transportation system covered? If a municipal bus system could be closed for a week, does that qualify the system as "critical infrastructure" even if other modes of transportation are still available?

Past practice indicates that DHS would interpret this language to

This paper, in its entirety, can be found at **http://report.heritage.org/ib3626**

Produced by the Thomas A. Roe Institute for Economic Policy Studies

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

include a large array of industries. In fact, under an existing presidential directive, DHS is already required to designate "critical infrastructure" and has identified no fewer than18 market sectors that, in its view, meet the requirements.[5]

Performance Requirements. Once its assets are designated as "critical infrastructure," a firm would be subject to DHS-written "performance requirements" that would require it to remedy any perceived risks or other cybersecurity shortcomings identified by DHS. Owners would also be required to come up with plans to "enhance" the security of their operations. The specifics of the plans are largely left to the private owners to decide, but the owners would be required to justify their plans periodically to the regulators' satisfaction. In reviewing their plans, infrastructure owners would be required to use "third-party assessors" who in turn would be registered and approved by DHS.

No Cost Estimates. Neither the costs nor the benefits of these new rules have been estimated. In March, Senators Ron Johnson of Wisconsin (R) and John McCain of Arizona (R) asked Homeland Security Secretary Janet Napolitano, a strong proponent of the pending legislation, for a cost-benefit analysis of the proposed rules. Her two-paragraph answer included no cost estimates and only illustrative estimates of the benefits. She cited a figure of $28 billion to $340 billion in current annual costs to the economy from cyberattacks and a seemingly random estimate that a shutdown of the electrical grid in a major city would cost the economy $1 billion per day.[6]

There was no estimate of the total potential threat, no estimate of the extent to which the legislation would reduce the threat, and not even a guess about the cost of complying with the new regulations.

Admittedly, estimates of the effects may be difficult to calculate, and many of the benefits and costs may be non-quantifiable. Yet it is striking that there has been so little effort to analyze the proposal. This is even more startling given the fact that much of S. 2105 depends upon DHS analyses and judgments similar to a formal regulatory impact analysis, which is routinely required from agencies before new rules are adopted.

Section 102, for instance, requires DHS, within 90 days after passage of the bill, to conduct a top-level assessment of security threats, including the extent of possible harm to health and safety as well as the effect on the economy. Section 103 requires DHS to prioritize threats by sector, and Section 104(g) requires DHS to take into account available resources. Such analysis is essential; regulators cannot make informed choices without it. Congress should insist on obtaining it before—rather than after—enacting the new mandates into law.

With or without such a formal analysis, policymakers should view proposed mandates with a skeptical eye. No matter how carefully regulations are designed, regulators cannot have the knowledge necessary to craft solutions for every network (even with the required "input" of the owners), and they are subject to political pressures that can distort the process.

Ultimately, the cost of an overly restrictive regulatory plan may be a reduction in security. The more that firms are required to follow government-mandated plans and priorities, the less flexibility and innovation they can bring to solving the unique security problems they each face. In effect, by mandating cybersecurity measures, the U.S.may end up hobbling its strongest weapons in the war against cyber threats.

Wrong Regulations Would Hurt Security. Imposing new federal regulations on American enterprise not only is a costly way to ensure cybersecurity, but also, by blunting private-sector innovation and flexibility, could be

1. See James L. Gattuso and Diane Katz, "Red Tape Rising: Obama-Era Regulation at the Three-Year Mark," Heritage Foundation *Backgrounder* No. 2663, March 13, 2012, http://www.heritage.org/research/reports/2012/03/red-tape-rising-obama-era-regulation-at-the-three-year-mark.
2. See Paul R. 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.
3. The legislation specifically exempts commercial information technology products, including hardware or software, and information technology products or services if the designation is based solely on a finding that it is being used or can be used in a critical infrastructure. More generally, it exempts systems or assets based "solely on the First Amendment." The extent of these exemptions is unclear. For instance, is broadcasting "solely" based on the First Amendment?
4. See also 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.
5. See U.S. Department of Homeland Security, "Sector-Specific Plans," http://www.dhs.gov/files/programs/gc_1179866197607.shtm (accessed June 5, 2012).
6. Janet Napolitano, "Response to Questions and Requests from Senator McCain and Senator Johnson as Outlined in Their March 22 Letter."

counterproductive to those efforts. Before imposing any cybersecurity mandates on the private sector, policymakers must ensure that they do not impose excessive burdens and that they will strengthen efforts to ensure security in cyberspace.

*—**James L. Gattuso** is Senior Research Fellow in Regulatory Policy in the Thomas A. Roe Institute for Economic Policy Studies at The Heritage Foundation.*