The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3777 | NOVEMBER 15, 2012

Obama's Cyber Executive Order: More Government Control of the Network

Paul Rosenzweig

The Administration has now released a draft executive order (EO) on cybersecurity,[1] and with President Obama's recent re-election, the likelihood that the EO will be issued has only increased. Furthermore, Senate majority leader Harry Reid (D–NV) has promised to bring the similarly flawed Cybersecurity Act of 2012 up for another vote.

When the EO is issued, it is likely to be a significant step—and probably in the wrong direction. Republicans and Democrats in both the Senate and the House of Representatives rejected a regulatory approach to cybersecurity, but the new EO pushes a "voluntary" standard-setting model backed by existing regulatory authority, comparable to the Cybersecurity Act of 2012.

While the scope of the existing regulatory authority is ambiguous, the Administration has signaled its intention to push as far as existing rules allow—and perhaps further. Who, after all, will sue to stop the government from protecting against cyber threats? Backed by the threat of regulation and promises of further incentives and a federal procurement preference, this order will likely be very significant and very costly while not providing important cybersecurity solutions, such as effective information sharing.

Setting Ambiguous, Outdated Standards. The EO begins by giving the Secretary of Homeland Security just 150 days to identify critical infrastructure where a cyber incident "could reasonably result in a debilitating impact on national security, national economic security, or national public health and safety."

The defining word—*debilitating*—is highly ambiguous. Most of the legislative drafts for cybersecurity legislation that have been considered have used the words *catastrophic* or *extraordinary* to define the scope of harm that is to be avoided. Both seem to be intended to limit somewhat the ambit of government cyber regulation to those portions of the national infrastructure that are truly significant and national in scope. Both are much narrower than *debilitating* in what they connote.

The Oxford English Dictionary, for example, defines *debilitating* as "to render weak; weaken; enfeeble." That seems a fair bit short of "catastrophic" or "extraordinary" and suggests that the scope of the federal cyber regulation under the EO will be very broad indeed.

On the standard-setting side of the equation, the EO directs the director of the National Institute of Standards and Technology (NIST) to create something it calls the Cybersecurity Framework. NIST is highly regarded and has ample standard-setting authority already. On the other hand, the Cybersecurity Framework would be a "flexible and repeatable" approach intended to "help owners and operators of critical infrastructure identify, assess, and manage cyber risk and to protect privacy and civil liberties."

Such objectives are broad enough to encompass almost anything that NIST decides it wants to put in—which means, that, once again, no one has any idea what the U.S. is going to get at the end of the process. It could be amazingly expensive or totally toothless and costless. About the only thing that would not be in the standards is the specification of a particular technological solution.

This paper, in its entirety, can be found at **http://report.heritage.org/ib3777**

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

NIST, however, would have only 180 days to publish a preliminary draft of the framework, with a final draft due to the *Federal Register* in a year. Creating major regulatory standards in one year is virtually impossible for the federal bureaucracy, but even at that pace, it is far too slow; by the time these rules are supposed to be finished and promulgated, computer speeds will have nearly doubled, meaning new threats and new vulnerabilities. A static approach to cybersecurity is necessarily ill-prepared to face these new cyber dangers.

"Voluntary" Standards. Beyond merely setting standards, the EO also makes three proposals in an attempt to coerce industry to follow these "voluntary" standards. After all, identifying critical infrastructure and standards is all well and good, but what if nobody follows the federal lead?

First, the Secretary of Homeland Security would encourage adoption of the framework by the owners of critical infrastructure. Exactly what incentives this would entail is completely undefined and left to the Secretary. Importantly, the EO has acknowledged that it cannot provide the one thing that private industry wants most: protection against liability if they suffer a cyber loss, notwithstanding the adoption of the framework.

The second part of the effort looks to have more teeth. Each sector-specific agency would be required to report to the President within 120 days on the extent of its existing regulatory authority to mandate cybersecurity for the industry for which it is responsible. The EO then says that within one year of the order being issued, agencies would be "encouraged" to propose regulations to mitigate cybersecurity risks. And when the President "encourages," the agencies will surely respond.

Third, buried at the end of the EO is the single piece of news that is likely to be its most effective part. Within 90 days, the Secretary of Defense and the director of the General Services Administration are to report to the President on whether or not a federal acquisition preference can be granted to vendors that meet cybersecurity standards, presumably the EO's Cybersecurity Framework. If feasible, this preference would be a huge carrot to incentivize voluntary compliance for anyone doing business with the federal government. Since many large vendors have or strive to have federal business, voluntary compliance would become effectively compulsory.

Regulatory Unknown Versus Nimble Solutions. In short, even at this stage, it is *still* impossible to know the answers to most of the questions Heritage has been asking about cybersecurity:

- How much would it cost?
- What "critical infrastructure" is covered?
- Would the standards be outdated before they take effect
- What would investors and innovators do?
- Does the government have the requisite expertise?
- Are the standards really voluntary?
- Why does anyone think the federal government can develop good standards?[2]

What is known for sure, however, is that the EO and similar legislative proposals portend a massive expansion of federal responsibility for cyber networks even as the federal government continues to have many cybersecurity failures of its own.[3] Congress therefore should:

- Scrutinize the executive order if it is issued and, where possible, modify it to prevent it from stifling innovation;
- Reject potentially costly efforts to create a new regulatory system for cybersecurity that would likely harm innovation and create a culture of compliance rather than true security; and
- Debate real cybersecurity solutions that include low-cost, high-benefit policies such as information sharing that help fight the newest cybersecurity threats.

1. Paul Rosenzweig, "Thoughts on September Draft Cybersecurity Executive Order," Lawfare, November 2, 2012, http://www.lawfareblog.com/2012/11/thoughts-on-the-september-draft-cybersecurity-executive-order/ (accessed November 7, 2012).
2. Paul Rosenzweig "Cybersecurity Legislation: Questions That Need to Be Answered," Heritage Foundation *Issue Brief* No. 3685, July 30, 2012, http://www.heritage.org/research/reports/2012/07/questions-on-cybersecurity-that-need-to-be-answered.
3. 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.

A Step in the Wrong Direction. The U.S. needs responsive, nimble cybersecurity defenses and policies that will not come from more regulations or government-set standards. The Administration and Congress should consider this before starting down the wrong path with either an executive order or legislation.

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