The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3727 | SEPTEMBER 13, 2012

Congress Should Not Enable Executive Orders on Cybersecurity

Paul Rosenzweig

The discussion over improving U.S. cybersecurity has moved from a debate over different pieces of legislation to speculation and expectation that President Obama will issue an executive order. Congress repeatedly declined to adopt a regulatory approach to cybersecurity, yet the Administration has drafted an executive order that begins the development of a regulatory system.

There is language in the pending continuing resolution (H. J. Res. 117) that appropriates funds that might be used to fund implementation of the cybersecurity executive order. This is a case of stealth government. Congress should be careful not to provide a blank check for an executive order that has not been published yet and could implement measures that Congress refused to put into law. That is the wrong approach to deciding Washington's appropriate role in strengthening the nation's cybersecurity.

A Regulatory Approach Is Wrong for Cybersecurity. Over the past year, the House of Representatives chose not to adopt a regulatory approach to cybersecurity, and the Senate was unable to pass its regulatory bill, the Cybersecurity Act of 2102. Many lawmakers in the House and the Senate simply do not believe regulations make much sense in cybersecurity, and they are exactly right. However, President Obama has a history of ignoring the views of legislators and imposing his will through executive order.

In cybersecurity, regulations have several critical drawbacks. One is that regulations will likely harm innovation. If the government says that companies need to have specific security measures, then cybersecurity investors and innovators will focus their work on the regulation-approved approaches—to the detriment of possibly better approaches that are not approved by the regulations.

In addition, regulations are simply too slow and too static to keep up in the cyber realm. The average time it takes to write a major regulation is 24–36 months. Computing capacity and power, on the other hand, double every 18–24 months. If the writing of regulations began now, they would be focused on today's threats. In 24–36 months, when the regulations came out, computing capacity will have doubled or tripled, with a whole new array of dangerous threats.

Finally, regulations encourage compliance at the cost of real security. In many government programs, the regulated parties often do whatever is needed to check the boxes but perhaps little more. Any solution to cybersecurity should be nimble and adaptive, not a mere to-do list for fighting yesterday's threats.

An Executive Order Ignores Congress and the Deliberative Process. Through recent leaks, various news sources over the past week were able to view a draft of the cybersecurity executive order that is being considered. The information from these sources appears to indicate that many of the concerning elements that caused the Cybersecurity Act to fail, such as its regulatory approach, are included in the cyber executive order.

The executive order uses "voluntary" regulations and standards to improve cybersecurity. Unlike a legislative approach, with an executive order there are few, if any, incentives the government can provide.

This paper, in its entirety, can be found at **http://report.heritage.org/ib3727**

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

It is hard to imagine that any organization would voluntarily ask the Department of Homeland Security (DHS) to regulate it.

Nevertheless, there is also concern that an executive order would encourage regulators, like the Federal Energy Regulatory Commission, to simply use their pre-existing authority to make these voluntary regulations mandatory. The executive order also creates a voluntary information-sharing system, but it lacks key protections, such as liability protection, which only Congress can grant. Without liability protection, few entities will share information for fear of being sued.

Instead of an incomplete executive order, Congress needs to adopt a comprehensive approach to cybersecurity by providing key things such as liability protection. Perhaps the worst effect of an executive order is that it might slow congressional action on cybersecurity. Some Members may be inclined to take a step back, since in their minds the President has already taken action to improve security.

Continuing Resolution May Enable a Cyber Executive Order. Some Members of Congress are worried about a small provision in the 2013 continuing resolution that contains language that provides over $1 billion to DHS's Infrastructure Protection and Information Security program. What exactly all this money will be used for is unknown.

One possible use is to implement the President's cyber executive order. The money needed to implement the new information-sharing and regulatory system, believed to be in the executive order, would have to be transferred from another program or be appropriated by Congress. On page 22 of the House's continuing resolution, $1.17 billion is given to DHS over and above normal DHS funding. Of that $1.17 billon, over $600 million is simply unaccounted for. The bill vaguely assigns this money to DHS for "Infrastructure Protection and Information Security." Furthermore, $218 million is assigned to Federal Network Security, which might be another vehicle for setting standards and regulation—exactly what the executive order is aiming to do. The language is so loose that the only real stipulation is that it be used "for operations necessary to establish and sustain essential cybersecurity operations."

As a result of such broad language, over $820 million would be made available for implementing an executive order, even though only a draft is being circulated. While it is unlikely that the money was added for the explicit purpose of funding an executive order, congressional leaders should not enable President Obama by providing such large sums of money without specifying how those funds should be used.

What Congress Should Do. Congress should:

- Remove unneeded cybersecurity funding in the continuing resolution or specify its uses,
- Reject a regulatory approach to cybersecurity, and
- Consider information sharing.

Do Not Facilitate a Flawed Executive Order. Congress was unable to pass a bill with a regulatory approach to cybersecurity. Given that President Obama may issue a cybersecurity executive order in the near future, Congress should not enable him to do it anyway.

*—**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.*