The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3852 | FEBRUARY 14, 2013

Obama's Cybersecurity Executive Order Falls Short

Paul Rosenzweig and David Inserra

In his State of the Union address, President Obama announced that he had signed an executive order (EO) on cybersecurity. The order uses a standard-setting approach to improve cybersecurity. However, such a model will only impose costs, encourage compliance over security, keep the U.S. tied to past threats, and threaten innovation.

While the EO does take some positive steps in the area of information sharing, these steps are hamstrung by the EO's inability to provide critical incentives such as liability protection. As a result, this order could result in few modest changes, or it could result in substantial negative effects.

The Scope of the Order. The EO uses a very broad definition of critical infrastructure, defining it as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Such a broad definition could be understood to include systems normally considered outside the cybersecurity conversation, such as agriculture. While there is no way of knowing how far implementation will actually go, this broad definition is certainly concerning.

Inhibited Information Sharing. In Section 4, the EO attempts to expand information sharing in several noteworthy ways. It calls for the federal government to quickly move unclassified information to the private sector and increase the number of security clearances given to appropriate owners of covered infrastructure. Additionally, the EO expands already existing information-sharing systems such as the Defense Industrial Base (DIB) Enhanced Cyber Services and Cyber Security/Information Assurance Program. These objectives are worthwhile, and the President should be applauded for including them.

However, these worthwhile pursuits will not be very effective because the EO must rely completely on existing authorities. Essentially, it directs government agencies to do a better job of sharing information than they already are. And where it does expand programs, such as with the DIB, these efforts will not be effective without additional incentives and protections to get more businesses involved. These include liability, Freedom of Information Act (FOIA), and regulatory-use protections.

The problem is that the EO cannot provide these important protections—they can be created only by Congress. As a result, many businesses will be reluctant to share their information for fear that their proprietary information could be endangered by a FOIA request or that an honest mistake might lead to a lawsuit being filed against them. Regarding other private-to-private or private-to-government solutions, the EO is silent.

Although the information-sharing provisions are limited, the privacy protections for this limited sharing are actually where they should be. The EO calls for consultation with privacy officers and oversight reports on the order's implementation. While some may find this provision weak, effective oversight is the best way to respect privacy concerns

This paper, in its entirety, can be found at **http://report.heritage.org/ib3852**

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

while not limiting information sharing that enhances the nation's security.

Standards and Mandatory Regulations. The true backbone of President Obama's EO is a regulatory framework set up in Sections 8 through 10. The EO directs the National Institute of Standards and Technology (NIST) to develop a "set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks." This "Cybersecurity Framework" is an attempt to collect cybersecurity best practices and standards of conduct in one place. NIST has only 240 days to complete this monumental task.

NIST is instructed to conduct an open, consultative process that develops a comprehensive framework. This framework seeks

> to provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.... The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services.

Completing such a task in 240 days is unrealistic.

Putting such timing concerns aside, how will the framework actually operate? Section 8 leaves it to sector-specific agencies to provide guidance for the voluntary adoption of the standards by their respective industries. Additionally, the Department of Homeland Security will "coordinate the establishment of a set of incentives to promote participation" and adoptions of the framework. To date, however, no one has been able to come up with incentives strong enough to entice businesses to take up new standards, which indicates that strong enough incentives might not exist.

Of course, no one knows what the framework will ultimately include. If it recommends that the private sector do what it is already doing, then it really does not do anything new. If it has new recommendations, these will be adopted only if the recommendations are truly worthwhile and if the incentive system manages to overcome businesses' concerns. While possible, this scenario remains very unlikely.

The real teeth to this system, however, are found in Section 10. This section effectively directs all the sector-specific agencies to take the voluntary framework and make it mandatory for their sectors through either existing rules or additional rulemaking.

While these agencies might have some understanding of industry concerns, mandatory regulations are still mandatory and will impose costs. Additionally, regulations tend to promote an attitude of compliance, not security, and in the case of cybersecurity, this means compliance with outdated regulations. With technology and cyber threats constantly evolving, regulations will always be stuck in the past.

Finally, mandatory regulations will go a long way toward souring any public-private partnership that the EO seeks in earlier sections. After all, a partnership does not usually involve forcing one side to do what the other one wants.

Coercion May Frighten Businesses into Action. The EO has one truly innovative policy: a confidential program that will identify the critical cyber infrastructure "where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."

This is a subset of the earlier broader critical infrastructure definition. Infrastructure owners who are identified as operating cyber critical infrastructure will be notified of that fact and entitled to challenge the notification. Once designation is final, nothing else happens.

However, if some cyber disaster later happens to one of those secretly identified companies that had not implemented the framework, the federal government would likely say, "We told you so." The bad press and potential lawsuits that could come from such an announcement would inspire fear so powerful that this provision will certainly be perceived as overly coercive.

How Congress Can Do Better on Cybersecurity. President Obama has signed his cybersecurity EO because he believes this is the best way forward on cybersecurity. Instead of following this flawed standards-based approach, however, Congress should replace the EO with strong information-sharing provisions, including robust liability, FOIA, and regulatory-use

protections. Such protections would enable strong and dynamic cybersecurity efforts.

*—**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, and **David Inserra** is a Research Assistant in the Allison Center at The Heritage Foundation.*