haynesboone
Setting precedent.

Haynes and Boone's Newsroom

President Obama Signs Cybersecurity Executive Order

02/19/2013

Ronald W. Breaux, Emily Westridge Black, Timothy Newman

President Obama recently signed an executive order focused on improving the security of the nation's infrastructure from cyber attack. Borrowing concepts from failed legislative efforts, the executive order ("Order") calls for increased information sharing between the federal government and the private sector and provides for the development of a voluntary cybersecurity program for owners and operators of critical infrastructure.

The Order provides for rule development and a comment process and does not require immediate action by the private sector. However, companies that are likely to be affected by the Order – including companies in the telecommunications, transportation, and banking/financial sectors, along with utilities companies and government contractors – would be well advised to track the implementation of the Order. They may soon have increased access to cyber threat information from various government agencies and may also find themselves incentivized, or even required, to adopt the cybersecurity framework being developed pursuant to the Order.

Increased Information Sharing

First and foremost, the Order aims to "increase the volume, timeliness, and quality of cyber threat information" the federal government shares with the U.S. private sector, creating two channels of information sharing. The Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence are ordered to develop protocols by which their respective agencies will share unclassified cyber threat information with any targeted entities. These agencies are also ordered to develop protocols for sharing *classified* threat information with owners and operators of critical infrastructure that are authorized to receive classified reports. "Critical infrastructure" is defined broadly in the Order to include "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."

The Order also calls for the expansion of the Enhanced Cybersecurity Services program ("ECS"). In its current form, the ECS is a voluntary program that allows defense industrial base companies and their commercial service providers to gain access to classified cyber threat information in exchange for satisfying certain cybersecurity requirements. Pursuant to the Order, the program will be expanded to include critical infrastructure owners and operators and their commercial service providers.

Finally, the Order calls for the Secretary of Homeland Security to expedite security clearance approvals for critical infrastructure entities and expand existing programs that place private sector subject-matter experts in temporary federal agency employment. This latter measure is designed to educate the government regarding the contents, structure, and types of cyber threat information that is most usefu to owners and operators of critical infrastructure.

Cybersecurity Framework

In addition to improving current information-sharing practices, the Order also aims to bolster current cybersecurity efforts by critical infrastructure owners and operators. Over the next year, the Director of the National Institute of Standards and Technology ("NIST") will oversee the development of a cybersecurity framework to include a "set of standards, methodologies, procedures, and processes that

align policy, business, and technological approaches to address cyber risks." The framework will be developed with the assistance of government agencies and the private sector, subject to a public review and comment process, and will be updated regularly by the NIST.

For now, adoption of the cybersecurity framework will be voluntary for owners and operators of critical infrastructure. The Order instructs the Secretaries of Homeland Security, Treasury, and Commerce to make recommendations to the president regarding an incentive program that will encourage adoption of the framework by the private sector. However, the Order indicates that the framework could evolve into a mandatory standard or at least color future regulation by government agencies. The Secretary of Defense and the Administrator of General Services, in consultation with the Secretary of Homeland Security and the Federal Acquisition Regulatory Council, are ordered to make recommendations to the president regarding the "relative merits of incorporating security standards into acquisition planning and contract administration." Moreover, the Order instructs government agencies with responsibility for regulating critical infrastructure entities to report to the president regarding their authority to "establish requirements based on the Cybersecurity Framework" as it relates to high-risk critical infrastructure entities. These provisions signal that the NIST's cybersecurity framework is likely to have an impact on the practices of high-risk entities and government contractors in the future.

The Impact of the Order

Although the Order does not require immediate action by the private sector, entities in critical infrastructure sectors of the economy are advised to track its implementation. The Order will result in increased information sharing with the private sector, and it may result in increased regulatory requirements regarding cybersecurity. Moreover, the Order contemplates private sector involvement in crafting the NIST's cybersecurity framework, and lobbying efforts could have an impact on the incentives that will accompany adoption of the framework. Even if the Order has little impact on a particular business or sector, it will certainly impact the broader national cybersecurity discussion going forward.

To read the executive order, click here.

For more information, please contact one of these Haynes and Boone attorneys:

Ronald W. Breaux	Bill Morrison	Randall E. Colso
214.651.5688	214.651.5018	214.651.5665
ron.breaux@haynesboone.com	bill.morrison@haynesboone.com	randy.colson@haynesb

John Podvin	Emily Westridge Black	Timothy Newma
214.651.5059	214.651.5221	214.651.5029
john.podvin@haynesboone.com	emily.westridgeblack@haynesboone.com	timothy.newman@haynes