Client Alert

February 2013

Obama Administration Releases Highly Anticipated Cybersecurity Executive Order

On February 12, 2013, the Obama Administration released an executive order, Improving Critical Infrastructure Cybersecurity (the "Executive Order"), which is focused primarily on government actions to support critical infrastructure owners and operators in protecting their systems and networks from cyber threats. The Executive Order requires administrative agencies with cybersecurity responsibilities to (1) share information in the near-term with the private sector within the scope of their current authority and to develop processes to address cyber risks; and (2) review and report to the President on the sufficiency of their current cyber authorities. The requirements to review and report to the President likely will serve to pressure Congress to pass more comprehensive legislation that should, inter alia, address issues that an executive order cannot, such as the provision of liability protection, incentives for compliance, and regulatory authority to compel compliance.

The Executive Order likely will impact companies in the following significant ways:

First, based on a Department of Homeland Security-developed process, there will be an increase in government notification to the private sector of cyber threats and recommended remediation activities. These notifications will flow from greater government coordination and companies should be prepared to act on the information they receive to mitigate risk. Additionally, the Department of Homeland Security ("DHS") will expand a current program, presently focused on sharing classified cyber threat information with defense companies, to include a broader group of critical infrastructure companies. This expanded program will be known as "Enhanced Cybersecurity Services."

Second, the Executive Order requires the development of risk-based cybersecurity standards, methodologies, procedures and processes, a so-called "Cybersecurity Framework," that can be used voluntarily by critical infrastructure companies to address cyber risks. The Cybersecurity Framework also may be used by secondary actors (such as insurance companies and auditors) to evaluate these risks. The Cybersecurity Framework will be developed using a consultative-based model involving an advisory committee led by the DHS (the Critical Infrastructure Partnership Advisory) and organized by an infrastructure sector that will include heavy involvement from the private sector. The Executive Order contemplates that the DHS and other agencies will incentivize companies' compliance with these "voluntary" standards in a variety of ways. One example included in the Executive Order is the call for a review of the federal procurement process to create a preference for vendors who meet the Cybersecurity Framework standards.

The Executive Order also will steer certain private sector companies to comply voluntarily with the Cybersecurity Framework by including them on a DHS-created list of "Critical Infrastructure at Greater Risk." It directs the DHS to use a risk-based, consultative approach to identify critical infrastructure where a cybersecurity incident could reasonably have a catastrophic regional or national effect. DHS will notify companies on the list and provide them with "the basis for the determination" allowing companies to request reconsideration of their inclusion on the list.

In addition to its impact on the private sector, the Executive Order also directs federal agencies to review the Cybersecurity Framework and determine the sufficiency of the existing regulatory requirements to

© 2013 Hunton & Williams LLP

address current and projected risks. One potential impact of this federal agency review may be to put Congress on notice of the need for additional legislation.

After yesterday's issuance of the Executive Order, the Administration's next steps will include (1) beginning to work in earnest across government and with the private sector in establishing the Cybersecurity Framework, (2) increasing cyber threat notifications, and (3) accomplishing the broad objectives of the Executive Order, including greater protection of our nation's infrastructure. These efforts cannot be accomplished without substantial input from the owners and operators of critical infrastructure.

Contacts

Lisa J. Sotto
lsotto@hunton.com

Lawrence J. Bracken II
lbracken@hunton.com

John J. Delionado
jdelionado@hunton.com

Maida O. Lerner
mlerner@hunton.com

Aaron P. Simpson
asimpson@hunton.com

Evan D. Wolff
ewolff@hunton.com

© 2013 Hunton & Williams LLP. Attorney advertising materials. These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create an attorney-client or similar relationship. Please do not send us confidential information. Past successes cannot be an assurance of future success. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials.

© 2013 Hunton & Williams LLP