COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Defense, Homeland & National Security

February 14, 2013

PRESIDENT OBAMA ISSUES EXECUTIVE ORDER ON "IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY"

SUMMARY

President Obama announced in his State of the Union message to Congress on February 12, 2013, that he had signed an Executive Order ("EO") addressing the cybersecurity of critical infrastructure. The issuance of the EO, which has been in the works over the last several months, represents a clear step by the White House to attempt to fill what it perceives as a crucial gap left by Congress's failure to pass cybersecurity legislation. The White House has emphasized the importance of cybersecurity to both national and business security, and President Obama in the State of the Union specifically cited the threats to corporate secrets, the power grid, financial institutions, and air traffic control systems as justifications for the EO. As set forth below, the EO seeks to improve cybersecurity through several mechanisms, including increasing information sharing from the government to the private sector, strengthening the cyber posture of critical assets, and establishing a Cybersecurity Framework for businesses designated as critical infrastructure.

PRIMARY IMPACTS ON THE PRIVATE SECTOR

With respect to the private sector, the EO's relevance and impact can be divided among three broad categories of businesses: (1) companies designated as critical infrastructure pursuant to the EO; (2) other sector-specific regulated entities; and (3) other businesses that neither constitute critical infrastructure nor operate in a sector that has a direct federal regulator.

Critical Infrastructure

The EO's impact will be greatest for companies designated as critical infrastructure. Section 9 of the EO specifies that within 150 days of the EO's issuance, the Secretary of Homeland Security "shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." The list of "identified critical infrastructure" will be updated annually going forward. Section 9 also contains a carve-out, providing that "commercial information technology products or consumer information technology services" cannot be designated as critical infrastructure.

Critical infrastructure entities may face direct regulation by their sector-specific agency based on the Cybersecurity Framework described in Section 7 of the EO. Section 7 specifies that the Director of the National Institute of Standards and Technology will lead the development of a Cybersecurity Framework "to reduce cyber risks to critical infrastructure." The Framework will include "a set of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks" and "shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible." The EO specifies that the Framework's

guidance to critical infrastructure owners and operators will be "technology neutral" and will enable critical infrastructure "to benefit from a competitive market for products and services that meet the standards, methodologies, procedures and processes developed to address cyber risks." The Framework will be subject to "an open public review and comment process," with a preliminary version to be published within 240 days and a final version to be issued within one year of the EO.

After issuance of the Framework, the EO directs the Secretary of Homeland Security and sector-specific agencies to establish a "voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure" (Sec. 8). The Secretary of Homeland Security is further directed to "coordinate establishment of a set of incentives" to promote participation by owners and operators of critical infrastructure in the Framework program.

Section 10 of the EO goes beyond the voluntary program described in Section 8. Section 10 directs sector-specific agencies that regulate critical infrastructure to report to the President on "whether the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure" and "any additional authority required."

Other Regulated Entities

Entities that do not qualify as critical infrastructure but are nonetheless regulated by sector-specific agencies may also be impacted by the EO. As noted above, Section 8 of the EO establishes a voluntary critical infrastructure cybersecurity program to encourage adoption by critical infrastructure of the Cybersecurity Framework, but it also specifies that sector-specific agencies may "develop implementation guidance or supplemental materials to address sector-specific risks and operating environments." Any such guidance or materials would not necessarily be limited to critical infrastructure within the agencies' purview, and any requirements that an agency adopts for critical infrastructure within its sector could be extended to all entities the agency regulates. Similarly, pursuant to Section 10, agencies may seek additional authority to establish requirements based on the Cybersecurity Framework, and there is no provision limiting such authority to critical infrastructure.

Thus, regulated entities potentially could find themselves directly regulated by sector-specific agencies that employ their regulatory authority to apply guidance or standards based on the Cybersecurity Framework more broadly to the sector, not just to companies, assets, or facilities deemed critical infrastructure.

Other Businesses

The EO should not directly impact businesses that are not subject to sector-specific regulators. However, time will tell whether the EO ultimately leads to a broader set of standards for cybersecurity that would be deemed by courts or other regulators to define a *de minimis* set of reasonable practices. In particular, Section 7 of the EO directs the NIST to incorporate "voluntary consensus standards and industry best practices" into the Cybersecurity Framework. The Framework must be "prioritized, flexible, repeatable, performance-based, and cost-effective" — all terms that are intended to provide flexibility to industry — and it could help define a new standard for industry more broadly.

In addition, non-critical infrastructure entities may choose to participate in the voluntary critical infrastructure cybersecurity program contemplated by the EO. Specifically, Section 8 directs the Secretary of Homeland Security to establish a program to support adoption of the Cybersecurity

Framework, not just by critical infrastructure owners and operators, but also by owners and operators of "any other interested entities." The interest of non-critical infrastructure entities in joining the program may depend on the set of incentives that the Secretary of Homeland Security is directed to coordinate and establish to promote participation in the program. The EO itself does not make clear what might be included in the incentives, but possibilities include liability protection for participating parties or leveraging the insurance market to create incentives for participation.

INFORMATION SHARING

In addition to the Cybersecurity Framework and other critical infrastructure provisions, Section 4 of the EO aims to "increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities." The EO directs the Attorney General, Secretary of Homeland Security, and the Director of National Intelligence to issue instructions to "ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity." The scope of threat information subject to disclosure is fairly narrow in that it must "identify a specific targeted entity," but the potential dissemination of the information is broad and not limited to critical infrastructure.

Section 4 also directs the Secretary of Homeland Security, Attorney General, and Director of National Intelligence to establish a process to disseminate classified reports on cyber threats related to specific targeted entities to critical infrastructure entities with the requisite security clearances. In support of this direction, the Section requires the Secretary of Homeland Security to expedite processing of security clearances for personnel employed by critical infrastructure owners and operators.

In addition, Section 4 directs the Secretary of Homeland Security, in coordination with the Secretary of Defense, to "establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors" within 120 days of the EO's issuance. The program is a voluntary program, currently administered by DHS. The EO explains that the program "will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure." Notably, this Section extends participation beyond critical infrastructure companies to, for example, contractors who serve such companies.

PRIVACY

Section 5 of the EO addresses privacy and civil liberties protections. Section 5 directs agencies to coordinate their activities under the EO with their agency's privacy and civil liberties official. It also directs the Department of Homeland Security's Chief Privacy Officer and Officer for Civil Liberties to produce a report addressing risks posed by programs undertaken pursuant to the EO and ways to mitigate identified risks. The report will be produced annually, and the responsible DHS officials are required to consult the Privacy and Civil Liberties Oversight Board and to coordinate with the Office of Management and Budget.

We are well-positioned to assist clients in understanding the impact of the Executive Order on their operations and in considering whether to participate in the programs the Order contemplates.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Defense, Homeland & National Security practice:

Michael Chertoff	202.662.5060	mchertoff@cov.com
David Fagan	202.662.5291	dfagan@cov.com
James Garland	202.662.5337	jgarland@cov.com
Kristen Eichensehr	202.662.5312	keichensehr@cov.com