CLIENT UPDATE

CRITICAL INFRASTRUCTURE CYBERSECURITY: U.S. GOVERNMENT RESPONSE AND IMPLICATIONS

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

WASHINGTON, D.C.
Satish M. Kini
smkini@debevoise.com

Renee M. Cipro
rmcipro@debevoise.com

2013 has begun with an acute focus on cyberthreats and cybersecurity. In particular, concern about the safety of U.S. critical infrastructure has grown in the wake of cyber intrusions targeted at a wide range of industries – including construction, energy, transportation, information technology and financial services – that have been used to bring down corporate websites, steal valuable intellectual property and gain access to non-public personal information on thousands of individuals. Intrusions have been linked to state actors including Iran, which U.S. authorities believe has been targeting U.S. firms in reaction to U.S. sanctions programs, and the Chinese military, as well as to criminals and so-called "hacktivists."

President Obama addressed these concerns in his State of the Union address and simultaneously issued a much-anticipated Executive Order entitled "Improving Critical Infrastructure Cybersecurity."[1] Last week, the White House released a strategy report that outlined new federal efforts, including trade restrictions and diplomatic steps, against countries that commit corporate espionage. Meanwhile, a new version of the controversial Cyber Intelligence Sharing and Protection Act ("CISPA") has been re-introduced in the U.S. House of Representatives. CISPA, which was passed by the House in 2012 but was not enacted by the Senate due principally to privacy concerns,

---

[1] Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11739 (Feb. 19, 2013).

would permit companies to share information with the federal government relating to cyber-security threats and provide protection from liability for such sharing.

In this Update, we focus most closely on President Obama's Executive Order. We first review what the Executive Order may mean for firms operating in critical industries and then provide a broader summary of the Order.

Key Implications of the Executive Order

- Requirements for Information Sharing. The Executive Order contains directives for the federal government to disseminate information about cyberthreats to "critical infrastructure" companies (a broad concept that could cover almost any firm of significance in the economy) and others. Importantly, unlike CISPA, the Executive Order calls for "one-way" information sharing and does not require industry to share information with the government. Nonetheless, critical infrastructure firms likely will need to take affirmative steps to participate fully in the information sharing: Firms will need to obtain appropriate security clearances for personnel in order to receive classified information from the government and may need to develop protocols for handling and safeguarding government threat and technical reports.
- Imposition of Standards. The Executive Order directs the federal government to develop a set of standards, procedures and processes to help critical infrastructure firms to identify, assess and manage cyber risks. Although the Order describes the standards as "voluntary," the Order directs the Department of Homeland Security ("DHS") to develop incentives to encourage participation with the standards and requires annual reports on the level of participation by critical infrastructure entities. Accordingly, critical infrastructure firms may find themselves under pressure to adopt government-developed standards, which are "voluntary" in name only. In addition, the voluntary standards may be a prelude to further developments: this week, the White House announced plans to submit priorities for cybersecurity legislation to Congress.
- Shaping the Standards. The Executive Order provides few details about the cyber-security framework to be developed but does call for "an open public review and comment process." Firms – particularly in financial services, information technology and other industries that already have relatively advanced cyber-security standards in place – will want to participate in the process by which this framework is developed, to ensure that standards are workable and accord with existing practices. The development process is already commencing; the National Institute of Standards and

Technology ("NIST") has put out an extensive request for information regarding risk-management practices, standards and guidelines.[2]

- Potential Liability. Firms that fail to adopt standards developed under the Executive Order or that fail to take countermeasures based on government-supplied threat information may be exposed to various regulatory and litigation risks if they subsequently experience data and cyber-security breaches. Regulators or private litigants (possibly in the form of class-action plaintiffs) could argue that any such firm disregarded industry standards and government-issued red flags and did not take reasonably prudent measures to address vulnerabilities.

Summary of the Executive Order

The Executive Order seeks to improve sharing of cyber-security information and to foster the development of risk-based cyber-security standards in collaboration with the owners and operators of critical infrastructure.

Defining Critical Infrastructure. The Executive Order provides an expansive definition of "critical infrastructure," including "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, economic security or public health and safety. A Presidential Policy Directive entitled "Critical Infrastructure Security and Resilience," which accompanied the Executive Order, highlights the expansiveness of the term by identifying 16 different industries that constitute "critical infrastructure": chemicals, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waster, transportation systems, water and waste water systems.

The Executive Order instructs the DHS Secretary, within 150 days, to identify critical infrastructure at the greatest risk of a cyber-security incident that would result in "catastrophic regional or national effects on public health or safety, economic security, or national security." In an apparent bow to privacy concerns, DHS is instructed to exclude commercial information technology and consumer information technology services.

Sharing Information with Critical Infrastructure Firms. New information sharing programs established under the Executive Order will provide both classified and

---

[2] *See* Developing a Framework To Improve Critical Infrastructure Cybersecurity, 78 Fed. Reg. 13024 (Feb. 26, 2013) (seeking comments by April 8, 2013).

unclassified information about threats to U.S. critical infrastructure companies. The DHS Secretary, the Attorney General and the Director of National Intelligence are required to issue instructions to ensure timely production of unclassified reports of cyberthreats to targeted U.S. companies.

In addition, critical infrastructure entities also will enjoy greater access to classified information of cyberthreats as a result of (i) expedited processing of security clearances for personnel employed by critical infrastructure entities, and (ii) the establishment of a voluntary information sharing program that will expand the existing Enhanced Cyber-Security Services Program to provide classified cyber-threat information and technical information beyond the defense-industrial base to all eligible entities in critical infrastructure sectors.

Cyber-Security Framework. The Executive Order instructs NIST, an agency within the Commerce Department, to work collaboratively with industry to develop a technology-neutral, flexible and cost-effective cyber-security framework that incorporates existing international standards, practices and procedures. The framework will be designed to help owners and operators of critical infrastructure assess, manage and mitigate cyber risks.

As noted above, NIST has already commenced its work in response to the Executive Order. On February 26, NIST asked for responses to 33 questions regarding risk-management, best and industry practices; the questions seek information on how organizations assess risks, what cyber-security approaches are used and what limitations exist with respect to these approaches and how approaches relate to international standards. NIST indicates that responses to these questions will help it to develop the framework. In addition, NIST indicates that its outreach will include interactive workshops with industry and academia.

Per the Executive Order, executive branch agencies with responsibility for regulating the security of critical infrastructure are required to review the framework for sufficiency and to develop industry-specific implementation guidance, as necessary. In addition, a voluntary program to support adoption of the framework will be developed by the DHS in cooperation with sector-specific agencies ("SSAs") and sector coordinating councils representing industry. The Treasury Department is the SSA for the financial services industry.

The Order directs DHS to establish a set of incentives to promote participation in the program. DHS, the Treasury Department, and the Commerce Department are each required to make recommendations to the President analyzing the benefits and

effectiveness of such incentives and whether the incentives would require legislation or can be provided to participants under existing law and authorities.

Privacy. Recognizing the privacy concerns that caused CISPA and similar legislative efforts to stall in Congress, the Executive Order is careful to address privacy safeguards. Executive branch agencies must coordinate their activities under the order with senior agency officials for privacy to ensure that the appropriate "protections are incorporated." In addition, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS must assess the privacy and civil liberties risks of the functions undertaken by DHS and recommend ways to minimize or mitigate such risks.

Conclusion

The Executive Order could have broad implications for many U.S. firms. In addition to being watchful as the Executive Order's directives are implemented, critical infrastructure firms may want to take the Order as a prompt to review and update their own policies and practices with regard to cybersecurity.

* * *

Please do not hesitate to contact us with any questions.

March 1, 2013