PDF

Cybersecurity Order Creates Challenges, Uncertainties for Key Sectors of the Nation's Infrastructure

February 15, 2013

Issue: On February 12, 2013, President Obama issued an Executive Order ("Order") allowing for national standards and increased information sharing to enhance the cybersecurity of the Nation's "critical infrastructure." The Order could have a sweeping impact on private sector companies deemed to be "critical infrastructure," including those in communications, select manufacturing, energy, financial services, food and agriculture, health care and public health, information technology, transportation, and other industries identified in the accompanying Presidential Policy Directive on cybersecurity.[1] Private participation is voluntary, although government "incentives," preferential treatment for governmental contractors that adhere to the Order, and potential regulatory requirements all could mean that some critical infrastructure companies would have no effective choice but to participate.[2] The Order comes nearly three months after the Senate failed to pass a more comprehensive measure, the Cybersecurity Act of 2012, which the President strongly supported.

Identification of critical infrastructure. The Order directs the Secretary to use a risk-based approach to identify the Nation's critical infrastructure within 150 days. The test will identify critical infrastructure "where a cybersecurity incident could result in catastrophic regional or national effects on public health or safety, economic security, or national security."[3'] The Order does not allow the Secretary to identify "commercial information technology products" and "consumer information

technology" as critical infrastructure, which means certain popular technology companies will not be affected. The Secretary will develop a process for "stakeholders," owners and operators of critical infrastructure, as well as the sector-specific agencies regulating them, to provide information relevant to the classification process. Companies operating within any of the targeted sectors will learn from the Secretary of Homeland Security ("Secretary") whether they have been classified as owners or operators of critical infrastructure covered under the Order. The Secretary will also ensure that identified owners and operators are provided with the basis for the decision to include them and allow the company an opportunity to request a reconsideration of its classification.[4]

Creation of national standards. The Order directs the National Institute of Standards and Technology ("NIST") to develop, through a public comment process, a set of baseline standards, methodologies, procedures, and practices for addressing and reducing cyber risks, to be called the "Cybersecurity Framework." In developing the Cybersecurity Framework, NIST must "incorporate voluntary consensus standards and industry best practices to the fullest extent possible."[5] The President has set a rapid timeline: a preliminary version of the Cybersecurity Framework must be published within 240 days, and a final version will be published within one year.[6]

Sector-specific regulation. The Order directs any sector-specific agency responsible for regulating the security of critical infrastructure to determine whether it can adopt the Cybersecurity Framework under its existing authority.[7] Sector-specific agencies must report to the President whether additional authority is required to meet those needs within 90 days of the release of the preliminary Cybersecurity Framework.[8]

Expansion of information sharing. Under the Order, a Department of Defense two-way, information-sharing program will be dramatically expanded to allow the voluntary participation of all owners and operators of critical infrastructure.[9] The Secretary and Attorney General will be responsible for the rapid dissemination of both classified and unclassified reports to critical infrastructure entities authorized to receive them. Although the purpose of the program is to share "cyber threat" information, the Order does not indicate what specific information private entities would in turn share with federal authorities.

Why You Should Care: The Executive Order on cybersecurity is intended to protect industries critical to national security, economic security, public health and safety. It is unclear, however, whether the Order better addresses concerns raised by those who successfully opposed the Cybersecurity Act of 2012, including that it would impose onerous requirements on businesses without effectively improving cybersecurity. While the Order indicates that compliance with the Cybersecurity Framework will be voluntary, and that the Framework will reflect industry best practices, the President also has made clear that he believes the need for robust, new national standards is vital. Affected industries can expect

increased pressure to participate as the Administration develops its incentives program and as sector-specific regulators determine which aspects of the Cybersecurity Framework can be adopted under existing regulatory authority.

The Executive Order creates new legal challenges for companies engaged in information sharing with federal authorities. The Order does not indicate what specific types of information will be requested from a critical infrastructure company, how such information will be used, and to what extent it will may be disclosed to third parties, including to other private-sector participants, state and local law enforcement, or in response to a FOIA request. Nor does the Order indicate whether a company's sensitive privileged or trade secret information will be sought through this program. The legal consequences of sharing privileged information has been a source of major concern for members of the financial services industry.

The Order may also create downstream litigation risks for companies that choose to participate. Unlike the Cybersecurity Act of 2012, the Order does not include a statutory defense for participating companies based on good faith compliance with the law. It is unclear how the Order interacts with existing federal privacy laws, such as the Right to Financial Privacy Act or the Communications Privacy Act, which ordinarily limit a company's ability to disclose certain types of information to government authorities. Nor is it clear what types of potentially costly technical security measures companies may be required to implement to protect the classified and sensitive information to be shared through this program, or what liabilities await a participating company that, despite these efforts, experiences a security breach.

Finally, the Order provides little in the way of certainty of expectations moving forward. As mentioned in our December alert on the Cybersecurity Act of 2012, unlike legislation, an Executive Order may be changed at any time by the President, without the consent of Congress.

Companies that are concerned about the increased regulatory burdens of being classified as an owner or operator of a critical industry should consider how they can shape the development of the Cybersecurity Framework. They may also wish to take advantage of any public input process for determining which entities will be classified as owners or operators of critical infrastructure and what the contents of the Cybersecurity Framework will be. Any company considering voluntary adoption of the Cybersecurity Framework or participation in the information-sharing program should carefully weigh the risks and potential costs. In any event, companies should fully expect that this Executive Order is only the opening salvo in what will be a long-term and comprehensive restructuring of our nation's cyber and information security policies and practices

If You Want Further Information: The complete texts of the President's Executive Order and accompanying Presidential Policy Directive are here and here, respectively. The complete text of the Cybersecurity Act of 2012, which did

not pass the Senate, is available here.

If You Want Further Analysis: Contact Randy Edwards, redwards@omm.com

[1] See Exec. Order, Improving Critical Infrastructure Cybersecurity ("Order"), § 2 (Feb. 12, 2013); Presidential Policy Directive ("PPD-21"), Critical Infrastructure Security and Resilience (Feb. 12, 2013), at 10-11.
[2] Order § 8(e).
[3] Id. § 9(a).
[4] Id. § 9.
[5] Id. § 7(a).
[6] Id. § 7.
[7] Id. § 10(a).
[8] Id. § 9(a).
[9] Id. § 4.
