Privacy and Information Governance Client Alert

PRESIDENT OBAMA ISSUES EXECUTIVE ORDER ON CYBERSECURITY; Cyber Threat To Critical Infrastructure A Matter Of National Security

by Mary Ellen Callahan, Daniel Chudd, Douglas Sondgeroth and Rukku Singla

After highlighting in his State of the Union address the growing national security threat cyber attacks pose to the American economy, President Barack Obama issued on February 12, 2013 an Executive Order ("Order") designed to improve significantly the nation's cybersecurity, focusing both on identifying and mitigating cyber threats to both critical infrastructure and the federal government while devising strategies to safeguard the country by addressing those threats. The Order, entitled "Improving Critical Infrastructure Cybersecurity," establishes that the President considers cyber threats "one of the most serious national security challenges" the United States currently faces, and that national and economic security depend upon a coordinated federal response to those threats. The Order is of critical importance for businesses in all industries, especially those that contract with the government, both because of the significant threats cyber attacks pose and because the effort to improve the nation's cybersecurity will involve virtually all major federal agencies. Attorneys from Jenner & Block's Privacy and Information Governance, Government Contracts, and Complex Commercial Litigation practice groups have prepared this Client Alert to review and analyze the Order and its ramifications.

Background

The Critical Infrastructures Protection Act of 2001, 42 U.S.C. § 5195c(e), defines critical infrastructure as "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 is directed at protecting this critical infrastructure through increased awareness of cybersecurity vulnerabilities and threats.

Public awareness and visibility into the scope and breadth of cyber intrusions has increased the call for greater information sharing from the federal government to owners and operators of critical infrastructure. The recent U.S. intelligence assessment, National Intelligence Estimate, identified several foreign countries – including but not limited to China, Russia, Israel, and France – for those countries' engagement in cyber-espionage. State-sponsored intrusions may have affected a number of critical infrastructure sectors in the United States, including energy, finance, information technology, aerospace, and automotives. Recent reports have also revealed cyber attacks from China on several

©2013 Jenner & Block LLP. 353 N. Clark St. Chicago, IL 60654-3456. Jenner & Block is an Illinois Limited Liability Partnership including professional corporations. This publication is not intended to provide legal advice but to provide information on legal matters. Transmission is not intended to create and receipt does not establish an attorney-client relationship. Readers should seek specific legal advice before taking any action with respect to matters mentioned in this publication. Masthead image from the Collection of the Supreme Court of the United States. Attorney Advertising. Prior results do not guarantee a similar outcome.

newspaper outlets, including the *Washington Post* and the *Wall Street Journal*, seeking sources and other confidential information. There has also been an increase in attention to hacktivist attacks targeting both government and private sector entities. These events demonstrate that cyber threats are varied and diverse, which highlights the desire of some companies to better understand the scope and impact of these cyber risks through information sharing from the federal government.

The Order's Key Provisions

The Order contains a variety of specific directions and requirements for federal agencies, but it primarily directs federal agencies to cooperate to accomplish three things over the next year: (1) share cybersecurity information among federal agencies and affected owners and operators of critical infrastructure; (2) establish a framework to reduce cyber risk; and (3) identify critical infrastructure at greatest risk. In tackling these priorities, federal agencies are to ensure that privacy and civil liberties are protected and collaborate with the private sector and other interested parties. The Order involves nearly all major federal security agencies, but the work of implementing it falls chiefly to the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) of the Department of Commerce.

Cybersecurity Information Sharing

One of the Order's chief aims is to foster information sharing from the government to the private owners and operators of critical infrastructure regarding cyber threats. Because a substantial portion of the threat information government possesses may be classified, Section 4 of the Order first provides that within 120 days of the Order, the Attorney General, DHS Secretary, and the Director of National Intelligence must each provide instructions so that intelligence, law enforcement, and other federal communities can prepare unclassified reports of specific cyber threats. To facilitate information sharing, the DHS Secretary and the Attorney General, in coordination with the Director of National Intelligence, must in turn establish a process so these unclassified reports can be "rapidly" disseminated to any U.S. entity that is specifically targeted. The Secretary and the Attorney General shall also work with the Director to create a system for tracking these reports and shall also expedite the process for issuing security clearances to the personnel of the owners and operators of critical infrastructure.

A Framework To Reduce Cyber Risk

The Order also requires the Director of NIST to develop a cybersecurity framework ("Framework") to reduce cyber risk and help owners and operators of critical infrastructure identify, assess, and manage that risk. Section 7 of the Order provides that the Framework will include a set of standards, methodologies, procedures, and processes addressing cyber risk based on voluntary consensus standards and industry best practices. In developing the Framework, the Director must engage in a public review and comment process, which includes consulting relevant stakeholders, such as other government agencies and owners and operators of critical infrastructure. The Director must publish a preliminary Framework within 240 days, and the final Framework within a year of the Order. Within 90 days of the preliminary Framework – i.e., early 2014 – all agencies with responsibility for regulating critical infrastructure must report to the President whether they have existing regulatory authority to establish requirements based on the Framework. If existing regulatory requirements are insufficient, agencies must propose new requirements within 90 days of the publication of the final Framework.

The Order does not have the force of legislation and it does not extend an agency's power beyond what is stated in existing law. Some Sector-Specific Agencies, however, such as the Department of Defense (DoD), already have authority to create cybersecurity incident information sharing standards through the FY 2013 National Defense Authorization Act. Similarly, on June 29, 2011, the DoD issued a proposed Department of Defense Federal Acquisition Regulation Supplement (DFARS) rule entitled "Safeguarding Unclassified DoD Information," which included, among other things, a requirement that defense contractors handling certain critical, though unclassified, information report cyber-intrusions to the DoD. These Sector-Specific agency requirements and proposed

requirements will retain the same legal status as before the Order was signed.

The DHS Secretary is instructed in the Order to establish a Voluntary Critical Infrastructure Cybersecurity Program to encourage owners and operators of critical infrastructure to adopt the Framework. The Order requires that within 120 days of the Order, the Secretaries of DHS, Treasury, and Commerce must recommend what incentives they can provide under existing authority to owners and operators to adopt the Framework, as well as any incentives that would require legislation. Similarly, the Secretary of Defense and the Administrator of General Services must recommend within 120 days of the Order the benefits of changing the federal procurement process to include preferences for vendors who meet cybersecurity standards. The voluntary program, the development of potential incentives for adopting the Framework, and any modifications to the procurement process will be crucial issues for many in the private sector in coming months.

The President simultaneously issued Presidential Policy Directive 21, Critical Infrastructure Security and Resilience, revising the directive on the Department of Homeland Security's and Sector-Specific Agencies' relationships with state, local, and tribal governments, and the public-private partnerships on physical and cyber threats to critical infrastructure. These combined releases highlight the holistic approach this Administration is taking toward infrastructure threats.

The information sharing relationships between the federal government and the companies involved in critical infrastructure will initially rely at least in part on these ISACs created for each of the 16 critical infrastructure industries. In the past, the robustness and effectiveness of the ISACs has varied widely, depending on the leadership, the type of industry, and the understanding of the industry-wide threat. The ISACs may not be sufficient vehicles for the increased information sharing envisioned by the Order, therefore alternative channels (including significantly increased direct government communications with individual high risk companies in the critical infrastructure) may develop.

Identifying The Greatest Risks

Within 150 days, the DHS Secretary will identify at-risk 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." Working with other agencies, the DHS Secretary shall "confidentially notify" owners and operators of critical infrastructure that they have been identified as having infrastructure at the greatest risk. The owners and operators will also be provided with relevant threat information. If the Order's timing is realized, companies likely could expect to receive these notifications and threat information by the fall of this year.

Integrating Security With Privacy and Civil Liberties

In addition to the three main tasks identified above, other notable provisions of the Order indicate an overarching effort to balance the need for security with protecting civil liberties and privacy. As a result, federal agencies are instructed in Section 5 to ensure that privacy and civil liberty protections are incorporated into their activities. The DHS's Chief Privacy Officer and Officer for Civil Rights and Civil Liberties are also instructed to recommend to the Secretary ways to minimize or mitigate any potential privacy and civil liberty risks the Order presents. Similarly, the Order contemplates that agencies implementing the Order will engage in an open, consultative process that will solicit comments and advice from a variety of constituencies, including government, the private sector, academics, and outside experts.

The Order also emphasizes the Fair Information Practice Principles (FIPPs), the widely-accepted framework of defining principles used to assess and mitigate privacy and civil liberties impacts of information systems, processes, or programs. The FIPPs were originally developed as the basis of the Privacy Act of 1974, and most recently incorporated into White House's National Strategy for Trusted Identities in Cyberspace (April 2011). The FIPPs are eight interdependent principles – Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and

Integrity, Security, and Accountability and Auditing. These principles form a framework that can be applied to most types of information collection, use or disclosure; the exact implementation of each principle, however, will vary based upon context. Therefore, they provide an objective set of principles to evaluate privacy and civil liberties impacts of cybersecurity programs, while permitting agencies to apply those principles in the context of their differing authorities and missions.

Ramifications

Because of the wide-ranging provisions of the Order and serious threats posed by potential cyber attacks, the Order is a significant development for numerous reasons. First, in addition to the fact that the President chose to highlight cybersecurity in the State of the Union, the Order and its involvement of nearly all major federal security agencies demonstrates that combating cyber threats is a top priority in the President's second term. Second, the aggressive schedule for implementing the Order and developing the Framework over the next year promises that federal agencies will be very focused on this process and that significant regulatory changes may be coming soon. Third, while many aspects are subject to continued development, the possible changes to the federal procurement process and the incentives for private companies to "voluntarily" adopt the Framework could have a significant effect on companies in many industries.

Fortunately, the Order contemplates that as agencies implement the Order, the government wishes to collaborate with owners and operators of critical infrastructure to address these threats and to develop a "partnership" in addressing cybersecurity. If these aspects of the Order are realized, whether through ISACs or other fora, it will afford various stakeholders the chance to work with the government to respond to cybersecurity concerns and give them a seat at the table in the development of new standards and frameworks in this critical area.

For further information, please contact:

Mary Ellen Callahan
Partner
Tel: 202 639-6064
Email: mecallahan@jenner.com

Douglas Sondgeroth
Partner
Tel: 312 840-7605
Email: dsondgeroth@jenner.com

Daniel Chudd
Partner
Tel: 202 639-6863
Email: dchudd@jenner.com

Rukku Singla
Associate
Tel: 202 637-6344
Email: rsingla@jenner.com