Advisory

FEBRUARY 2013

If you have any questions about this Advisory, please contact:

JOHN KENNEDY
203.363.7640
jkennedy@wiggin.com

JONATHAN MEDALSY
212.551.2637
jmedalsy@wiggin.com

White House Issues Cybersecurity Executive Order

On February 12, 2013, President Barack Obama signed an Executive Order, titled "Improving Critical Infrastructure Cybersecurity" (the "Order"), aimed at bolstering U.S. cybersecurity through voluntary best practices developed by federal agencies in collaboration with industry stakeholders. The President officially announced the long-awaited Order, as well as a related document, the "Presidential Policy Directive on Critical Infrastructure Security and Resilience," during his annual State of the Union address, in which he also attempted to galvanize Congress toward legislative action on the same issue.

BACKGROUND

The Administration's Order comes in the wake of a political stalemate that has belied previous efforts to advance cybersecurity legislation through Congress. A comprehensive cybersecurity bill (S. 3414) introduced in 2012 by a group of key Senate chairmen, including Joseph Lieberman (I-Conn.) and Susan Collins (R-Maine), and backed by the White House, encountered tough obstacles and eventually failed to pass a Senate vote. In light of congressional fumbling, the White House disclosed several months ago that it was weighing the possibility of taking unilateral action via Executive Order. This idea, backed by leading Senate Democrats, including John D. Rockefeller IV (D-W.Va.) and Dianne Feinstein (Calif.), came to fruition on Tuesday night.

STRUCTURE AND IMPLEMENTATION OF THE ORDER

The Order focuses on two operative concepts: (1) information sharing and (2) the implementation and adoption of risk-based standards. In order to achieve the latter of these goals, the Order calls for a partnership between government agencies and the owners and operators of "critical infrastructure."[1] Through a "risk-based" identification process, such government agencies are directed to confidentially notify owners and operators of critical infrastructure that they have been identified as such, and to ensure that identified owners and operators are provided the basis for the determination and an opportunity to request a reconsideration.

INFORMATION SHARING

To better equip U.S. companies to handle cybersecurity threats, the Order directs federal agencies to produce unclassified reports of cyber threats to U.S. companies and mandates the expansion of a pre-existing, voluntary information-sharing program involving the Departments of Defense and Homeland Security. Pursuant to such program, federal agencies are permitted to disclosure certain classified reports to eligible critical infrastructure companies and commercial service providers that offer services to critical infrastructure.

CONTINUED ON NEXT PAGE

White House Issues Cybersecurity Executive Order CONTINUED

RISK-BASED STANDARDS: THE CYBERSECURITY FRAMEWORK

The Order directs the National Institute of Standards and Technology (part of the Commerce Department) (the "NIST) to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). Through an open, consultative process among sector-specific federal agencies, owners and operators of critical infrastructure and other industry stakeholders, the NIST is expected to develop a set of standards and procedures to align policy, business and technological approaches to cyber risks. The goal of such framework is to help owners and operators of critical infrastructure identify, assess and manage cyber risks, while mitigating any impact on business confidentiality, and protecting privacy and civil liberties. The NIST must also meet certain milestones, as is set forth in further detail in the timeline below, such as the publication of preliminary version of the Cybersecurity Framework within 240 days of the date of the Order.

The Department of Homeland Security, in coordination with sector-specific agencies, such as the Department of Energy, is expected to establish a program to assist companies with implementing the Cybersecurity Framework and to design a set of incentives to promote participation in such program.

Finally, the Order directs regulatory agencies "with the responsibility for regulating the security of critical infrastructure" to assess whether existing cybersecurity requirements are sufficient given current and projected cybersecurity risks. To the extent that any existing requirements are inefficient or ineffective, such agencies must propose new prioritized, risk-based regulations based on the Cybersecurity Framework.

RESPONSES TO THE ORDER

Reactions to the Order are a mixed bag. Certain industry experts, such as Jody Westby, CEO of consultancy Global Cyber Risk, worry that placing the brunt of the responsibility on government agencies could result in an unwieldy framework of mandatory standards for critical infrastructure companies. Some also believe that the Administration is overreaching and usurping power from the Legislative Branch.

Others, such as Alan Paller, director of research at the SANS Institute cybersecurity firm, believe that the Order is a step in the right direction, but that it accomplishes too little. To be sure, the Administration itself called the Order a "down payment on legislation." For example, providing liability protections in exchange for participating in the standards program or sharing threat data with the government must be approved by Congress. Visit http://www.wiggin.com/Files/24248_Executive%20Order%20Timeline%20February%202014.pdf to view the Executive Order Timeline.

[1] The term "critical infrastructure" is defined as infrastructure systems and assets so vital to the United States that their incapacity would have a debilitating impact on national security, economic security, or public health and safety. The Department of Homeland Security website provides a list of critical infrastructure sectors, including: communications, energy, transportation systems, food and agriculture, defense industrial base, banking and finance, healthcare, information technology, and postal and shipping.