KING & SPALDING

Client Alert

Government Advocacy and Public Policy Group

February 15, 2013

President Obama Issues Executive Order on Cybersecurity

On February 12, 2013, President Obama issued a long-anticipated Executive Order concerning cybersecurity entitled Improving Critical Infrastructure Cybersecurity. The Executive Order marks a major milestone in the Federal Government's effort to guard against the growing cyber threat, but by its terms the Executive Order is inherently limited. In his State of the Union address, President Obama called on Congress to pass legislation "to give our government a greater capacity to secure our networks and deter attacks."

Overview of the President's Executive Order

The President's Executive Order seeks to address cybersecurity concerns with a series of largely voluntary measures designed to increase information sharing from the Government and to develop industry best practices through voluntary mechanisms and incentives. The key components of the Order include:

- A broad definition of "critical infrastructure" that would include, among others, financial institutions, communications, information technology, energy, agriculture, pharmaceuticals, and the defense industrial base;
- Improving voluntary information sharing of government information to the private sector;
- Establishing a consultative process to coordinate improvements to cybersecurity concerning critical infrastructure;
- Creating a baseline framework of best practices to reduce cyber risks and voluntary critical infrastructure programs; and
- Studying mechanisms to encourage adoption of voluntary federal standards, including changes to federal procurement policy.

Aiming to Improve Sharing of Cyber Threat Information

The Executive Order seeks to improve the manner by which the Federal Government shares cyber threat information with private sector entities so that the private sector "may better protect and defend themselves against cyber threats." The Order seeks to improve such information sharing *from* the Government in three ways. First, it requires the Secretary of Homeland Security, the Attorney General, and the Director of National Intelligence to streamline their procedures, while maintaining protection of law enforcement

For more information, contact:

Eleanor Hill
+1 202 626 2955
ehill@kslaw.com

Ted Hester
+1 202 626 2901
thester@kslaw.com

J.C. Boggs
+1 202 626 2383
jboggs@kslaw.com

Tom Spulak
+1 202 661 7948
tspulak@kslaw.com

Dan Donovan
+1 202 661 7815
ddonovan@kslaw.com

Alexander K. Haas
+1 202 626 5502
ahaas@kslaw.com

King & Spalding
Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

www.kslaw.com

and intelligence sources, methods, operations, and investigations, to ensure timely production of unclassified and, if possible, classified reports of cyber threats to any specific targeted entity. Second, it seeks to expand the Enhanced Cybersecurity Services program, beyond the defense industrial base, to all critical infrastructure sectors by directing the Secretary of Homeland Security, in coordination with the Secretary of Defense, to establish procedures to do so within 120 days. The Enhanced Cybersecurity Services program is a voluntary program of the Departments of Homeland Security and Defense that permits the Federal Government to provide classified cyber threat and technical information to either a participating company or its commercial services provider to counter malicious cyber activity. Finally, the Order directs the Secretary of Homeland Security, in consultation with agencies, the private sector, and other experts, to identify, through a risk-based approach, those critical infrastructure sectors at greatest risk and where a "cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."

Reducing Cyber Risks to Critical Infrastructure

The Executive Order seeks to reduce the risks of cybersecurity incidents to critical infrastructure through two chief actions. First, the Order creates a "consultative process," to be established by the Secretary of Homeland Security, to coordinate improvements to the cybersecurity of critical infrastructure. To further this objective, the Order directs the Secretary to consider the views of other agencies, various sector-specific coordinating councils, the Critical Infrastructure Partnership Advisory Council, experts, *and* critical infrastructure owners and operators. Second, the Order requires the Director of the National Institute of Standards and Technology (NIST) to lead the development of a "Cybersecurity Framework" that would include best practices, standards, and a technical approach that incorporates "voluntary consensus standards and industry best practices to the fullest extent possible" to be set forth in a guidance that is technology neutral. The purpose of this framework is to help the owners and operators of critical infrastructure identify and manage risks posed from cyber threats and encourage continued collaboration of products and services to reduce and address cyber risks. This framework is to be developed through the consultative process established in Section 6 of the Order and an "open public review and comment process" with a preliminary framework to be published within 240 days and a final framework within one-year.

Voluntary Critical Infrastructure Cybersecurity Program and Incentives to the Private Sector

The President's Order also creates a new "Voluntary Critical Infrastructure Cybersecurity Program" that focuses on three principal goals. First, the Order seeks to create a "voluntary program to support adoption of the Cybersecurity Framework"—to be developed by Director of NIST—by cybersecurity owners and operators. To advance participation in this voluntary program, the Order requires, within 120 days, the Secretary of Homeland Security to coordinate the establishment of unspecified "incentives" to encourage participation in this voluntary program and separate recommendations from the Secretaries of Treasury and Commerce that analyze the "benefits and relative effectiveness of such incentives, and whether the incentives would require legislation." Second, in a move that could ultimately affect all federal contractors, subcontractors, and their supply chains, the Order directs a review of federal procurement policy, acquisition planning and contract administration to consider the "feasibility, security benefits, and relative merits of incorporating security standards" into the federal procurement process. Finally, the Order mandates creation of sector-specific implementation guidance for the Cybersecurity Framework.

What's Next

The President's Executive Order is quite clear that it neither alters nor limits "any authority or responsibility of an agency under existing law" and must be implemented "consistent with requirements and authorities to protect intelligence and law enforcement sources and methods." Congressional action would be needed to provide industry with liability protection to improve two-way information sharing. Without liability protection, private sector sharing of cyber threat information may raise concerns about litigation risks or loss of government contracts. Similarly, only Congress could ameliorate industry concerns over engaging in collective action that could be viewed as creating friction with prohibitions in Federal antitrust law. Finally, congressional action would be necessary to establish federal baseline standards that would preempt conflicting state requirements (either in legislation or state tort actions) and provide certainty and protection to industry.

Congress has already picked up the contentious debate from the 112th Congress over the terms of cybersecurity legislation. House Select Intelligence Committee Chairman Mike Rogers (R-MI) and Ranking Member Dutch Ruppersberger (D-MD) this week re-introduced their cybersecurity bill, H.R. 624, which focuses on information sharing, and held a hearing to examine cyber threats on Thursday, February 14. H.R. 624 is identical to a bill that passed the House last year but that Senate Democrats criticized, citing privacy concerns and arguing that the bill doesn't go far enough by prescribing only voluntary measures. Senate Homeland Security and Governmental Affairs Committee Chairman Tom Carper (D-DE) has also announced his intention to hold a hearing soon, perhaps jointly with the Senate Intelligence and Commerce, Science and Transportation panels, on cybersecurity legislation that would supplement the Executive Order. Meanwhile, new chairman of the House Homeland Security Committee Mike McCaul (R-TX) has announced plans to introduce his own legislation that would "enhance coordination between the private sector and government in order to protect our critical infrastructure."

Recommendations

As federal agencies work to implement the Executive Order and the 113th Congress moves forward with multiple cybersecurity proposals, the business community needs to ensure they are in compliance with the Order and effectively communicate their positions to members of Congress. Understanding these new policies and monitoring future developments will enable companies to prepare for further changes. For the fifth consecutive year, King & Spalding's government relations practice was recognized by *Chambers USA*: America's Leading Lawyers for Business, and was selected by *U.S. News and World Report* as the "Law Firm of the Year" for government relations in 2012, based on the positive feedback of clients and peers regarding the firm's work in this area. King & Spalding has one of the nation's most active and respected government relations practices and is particularly well-equipped to advise and assist companies on these important data security issues.

If you have any questions regarding the Executive Order on cybersecurity or related issues, please contact Eleanor Hill at +1 202 626 2955 or Alexander Haas at +1 202 626 5502.