KIRKLAND ALERT

February 2013

Executive Order on Cybersecurity Begins Standard-Setting Process

On February 12, 2013, President Obama signed a much-anticipated Executive Order on Improving Cybersecurity for Critical Infrastructure (the "EO"). The EO signals the Obama Administration's commitment to make cybersecurity a priority during President Obama's second term and will likely have significant impact on a broad range of industries. As the accompanying Presidential Policy Directive makes clear, companies in 16 industry sectors may qualify as critical infrastructure, including: chemical; communications; critical manufacturing; dams; defense contractors; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

The EO takes three steps that warrant close and immediate attention from owners or operators of businesses in those sectors that may qualify as critical infrastructure.

First, the EO directs the National Institute of Standards and Technology to develop a Cybersecurity Framework that would provide standards for cybersecurity for critical infrastructure. Adoption of the standards in this Framework by the private sector is described as "voluntary." But given the express direction in the EO for regulators to develop "incentives" for companies to comply and the further direction for agencies with responsibility for cybersecurity to determine whether, in light of the new Cybersecurity Framework, existing regulations are sufficient, the EO seems to foreshadow a regulatory push toward adoption of the Framework. As a result, preparing immediately to participate in the public comment process that will develop the Cybersecurity Framework should be a high priority for companies that seek to avoid overly burdensome or impractical standards.

Second, the EO significantly expands a mechanism for the Government to share cyber-threat information, including classified information, with the private sector. Increased access to information should be a boon to most critical infrastructure companies. Once again, though, while participation in the program is voluntary, as a practical matter, it may become difficult for companies operating critical infrastructure to decline to participate in a program that disseminates such threat information.

Third, the EO calls for identifying critical infrastructure that is "at Greatest Risk." Companies placed in that category can likely expect to be the primary focus of regulatory "incentives" and, subsequently, any formal regulations requiring adherence to the standards developed in the Cybersecurity Framework. As a result, companies should prepare now to participate in the EO's proposed "consultative process" to ensure input into any decision affecting them in the development of the Greatest-Risk list.

1. Cybersecurity Framework — "Voluntary" Standards for Cybersecurity

The EO calls for the National Institute of Standards and Technology ("NIST," part of the Commerce Department) to lead the development of a framework for reducing cyber risks to critical infrastructure — the "Cybersecurity Framework." Sec. 7(a). The Cybersecurity Framework will include "a set of standards, methodologies, procedures, and processes" for addressing cybersecurity threats. The EO specifies that there must be an "open public review and comment process" used in developing the Framework. Sec. 7(d). While the EO directs that the Framework should "incorporate voluntary consensus standards and industry best practices to the fullest extent possible," *id.*, it leaves open the possibility that regulators developing the Framework will opt for more

onerous standards. Similarly, the EO directs that the Framework should be "consistent with voluntary international standards," but only "when such international standards will advance the objectives of this order." *Id.* The EO thus contemplates standards that may exceed any voluntary industry consensus.

Under the timetable set by the EO, developing the Cybersecurity Framework will be a fast-moving process. The NIST is directed to publish a preliminary version within 240 days and a final version within one year. Sec. 7(e). On Wednesday, February 13, 2013, the NIST had already issued a set of questions that it will include in its official Request for Information, to be published in the Federal Register.

Although the EO states that compliance with the Cybersecurity Framework is "voluntary," for several reasons, owners and operators of critical infrastructure may soon find that declining to adopt the Framework will become difficult or impossible as a practical matter.

First, the EO directs the Secretary of Homeland Security to "coordinate establishment of a set of incentives" designed to promote private sector adoption of the Cybersecurity Framework. Sec. 8(d). The EO thus requires Executive Branch agencies to identify "incentives" that are within their current authority and also calls upon them to identify "incentives" that "would require legislation." *Id.* The EO clearly contemplates an effort to use whatever regulatory authority may be brought to bear to encourage adoption of the Cybersecurity Framework. Many regulators may already have sufficient authority to make it difficult for businesses under their jurisdiction to opt out of the Framework. Regulators of financial institutions, for example, have focused on cybersecurity issues for years and could conclude that data security policies and procedures that fail to live up to the Framework create material weaknesses in the financial institution requiring remedial measures.

Second, the EO directs agencies with responsibility for regulating the security of critical infrastructure to determine, after the preliminary Cybersecurity Framework is published, whether they have "clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks." Sec. 10(a). It also specifies that, if any such agency determines that current regulatory requirements are "insufficient" in light of the Framework, the agency should propose additional regulatory action to address the deficiency. Sec. 10(b). The EO thus seems to contemplate, at least to some extent, the eventual imposition of standards from the Cybersecurity Framework via regulation.

For all these reasons, although the Cybersecurity Framework is billed as "voluntary," it may quickly become difficult or impossible for owners or operators of critical infrastructure to escape it. As a result, owners and operators should view the public comment process mandated by the EO as a critical opportunity to influence the standards and build a record supporting the standards they desire.

2. Information Sharing

The EO contains two significant initiatives on information sharing. First, it directs the Secretary of Homeland Security, the Attorney General, and the Director of National Intelligence to establish mechanisms to ensure the "timely production of unclassified reports," Sec. 4(a) of cyber-threat information that identifies a particular U.S. target and to establish a process that "rapidly disseminates" such reports "to the targeted entity." Sec. 4(b). Second, it directs the Secretary of Homeland Security to act within four months (120 days) to "establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors." Sec. 4(c). That program was originally established solely for the Defense Industrial Base. Its expansion to all critical infrastructure sectors will allow "eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure" to receive "classified cyber-threat and technical information from the Government." *Id.* As a result, this provision may substantially improve the threat information available to the private sector, in comparison to unclassified tearlines. To implement this program, the EO directs the Secretary to "expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators." Sec. 4(d).

The EO characterizes the Enhanced Cybersecurity Services program as a "voluntary information sharing program." Most owners and operators are likely to see participation in an information flow *from* the government *to* the private sector as a benefit. And as a practical matter, it may become difficult to decline participation in a government program offering state-

of-the-art cyber-threat information.

As expected, the EO makes no substantial attempt to increase information sharing *from* the private sector *to* the Government. An effective mechanism for encouraging such disclosures would require protection from liability for companies providing the information, and that protection would require legislation. The Administration resorted to this EO precisely because Congress has been unable to pass legislation on this subject. Several proposed bills addressing cybersecurity died in the last Congress. The Cyber Intelligence Sharing and Protection Act (CISPA) was the most expansive in removing legal hurdles preventing private companies from sharing cyber-threat information with the government. The sponsors of that bill have already announced that they intended to reintroduce it. In the wake of the EO, however, the prospect for progress on any cybersecurity legislation in the current Congress seems uncertain.

3. Critical Infrastructure "At Greatest Risk"

The EO also directs the Secretary of Homeland Security to identify critical infrastructure that is "at Greatest Risk," that is, "infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." Sec. 9(a). After a process that includes consultation with industry to identify critical infrastructure meeting that standard, the Secretary must confidentially inform owners and operators of their designation. For obvious reasons, the list is not made public. The EO expressly exempts "any commercial information technology products or consumer information technology services" from being designated on the list. It thus appears that creators of widely used software and providers of information services (presumably including companies like Google) are exempt.

The only express consequences of being placed on the Greatest-Risk list are that the President will receive an annual report addressing the extent to which owners and operators on the list are adopting the Cybersecurity Framework and that agencies will particularly consider the list in assessing whether or not their current cybersecurity regulatory requirements are sufficient. Secs. 8(c), 10(a). The EO evidently envisions that being on the list will impose additional burdens, however, because it expressly directs the Secretary of Homeland Security both (1) to ensure that owners and operators are "provided the basis" for putting them on the list, and (2) to establish a process under which an owner or operator can request reconsideration of the designation. Sec. 9(c). Providing that mechanism suggests a tacit recognition that "incentives" and other regulatory authority for encouraging adoption of the Cybersecurity Framework will be focused most intently on infrastructure on the Greatest-Risk list, thus placing owners and operators on that list under burdens that they may prefer to avoid.

If you have any questions about the matters addressed in this *Kirkland Alert*, please contact the following Kirkland authors or your regular Kirkland contact.

Patrick F. Philbin
Kirkland & Ellis LLP
655 Fifteenth Street, N.W.
Washington, D.C. 20005
www.kirkland.com/pphilbin
+1 (202) 879-5030

Seth Traxler
Kirkland & Ellis LLP
300 North LaSalle
Chicago, IL 60654
www.kirkland.com/straxler
+1 (312) 862-2241

John A. Eisenberg
Kirkland & Ellis LLP
655 Fifteenth Street, N.W.
Washington, D.C. 20005
www.kirkland.com/jeisenberg
+1 (202) 879-5902

Todd M. Friedman
Kirkland & Ellis LLP
601 Lexington Avenue
New York, NY 10022
www.kirkland.com/tfriedman
+1 (212) 446-4786