WILTSHIRE & GRANNIS LLP

REGULATORY ADVISORY
15 FEBRUARY 2013

PRESIDENT ISSUES CYBERSECURITY EXECUTIVE ORDER:

Agencies Take Preliminary Implementation Steps; Regulatory Burdens Loom

On February 12, 2013, President Obama issued a broad Executive Order designed to enhance physical and cybersecurity protections for critical infrastructure. The President also issued a Presidential Policy Directive ("PPD") to implement the Executive Order. The PPD provides for increased coordination between government and industry regarding physical and cybersecurity, and resilience of critical infrastructure, noting, in particular, the vital role that communications networks play in such infrastructure. When fully implemented, the Executive Order and PPD will impose significant new regulatory burdens on owners of terrestrial wireless and wireline, undersea cable, and satellite networks. They also create regulatory uncertainty regarding the meaning of "virtual" infrastructure, to which the new requirements will apply, and introduce tension into the commercial relationships between such infrastructure owners and providers of so-called "over-the-top" services, given exemptions granted to "commercial information technology products or consumer information technology services." To influence the implementation of these requirements and minimize regulatory burdens, critical infrastructure owners will need to participate in the standards-development and other implementation proceedings already begun by various U.S. Government agencies. They will also need to continue to monitor and influence cybersecurity legislation.

The Obama Administration has long contemplated issuing an Executive Order and PPD due to concerns about cyber risks and Congress' inability to resolve differences in cybersecurity legislation over liability protection for providers. This Executive Order and PPD create an initial cybersecurity framework. The potential for Congressional action still exists and may be increased as a result of the Administration's actions; several Chairmen with jurisdiction have introduced bills and expedited hearing schedules in light of the PPD.

The Executive Order and PPD direct the Department of Homeland Security ("DHS") and the National Institute for Standards and Technology ("NIST") to, among other things:

- create policies and procedures to increase information sharing about cyber threats;
- develop a "Cybersecurity Framework" to reduce risk to critical infrastructure; and
- create a voluntary, incentives-driven cybersecurity program for critical infrastructure to share threat information with the U.S. Government.

The Executive Order and PPD define "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 Executive Order and PPD provide little specific information about how DHS and NIST will fulfill their new obligations, or the degree to which they will consult with industry stakeholders in designing the Cybersecurity Framework or cybersecurity information-sharing program.

Several elements in the Executive Order and PPD underscore the need for industry to engage early and often with relevant agencies.

- The Executive Order and PPD identify DHS, not the Federal Communications Commission ("FCC"), as the sector-specific agency responsible for developing and implementing the Cybersecurity Framework and cybersecurity information-sharing program for the communications sector. Although the PPD directs the FCC, to the extent legally permitted, to partner with DHS in this work, the Executive Order and PPD create a system where the decision-making agencies are not those with the greatest communications-sector expertise or established working relationships.
- As expected, the cybersecurity information-sharing program lacks liability protection for industry; such protection almost certainly will require Congressional action.
- Although the program is formally "voluntary," the Executive Order requires agencies to report annually on which owners and operators are participating—a "name and shame" provision—and encourages agencies to devise incentives to encourage participation. In practice, program participation will seem all but mandatory for many providers.
- The Department of Defense ("DOD") and the General Services Administration ("GSA") must also recommend how to incorporate the program into federal procurement processes—further underscoring the essentially mandatory nature of the program. Federal law already requires industry to provide cybersecurity information to GSA and DOD. The Executive Order, however, is likely to increase ongoing reporting obligations for federal contracts and to create new compliance risks.
- The Executive Order directs agencies regulating critical infrastructure security to review their regulatory authority to implement the Cybersecurity Framework and cybersecurity information-sharing program. Where needed, the agencies shall propose any additional authority required. The agencies will likely conduct additional rulemakings to propose penalties for failure to participate in the voluntary cybersecurity program.

The lack of clarity with respect to the scope of the Executive Order raises particular concerns. The Executive Order creates obligations regarding both physical and virtual or cyber infrastructure, but excludes from its scope "commercial information technology products or consumer information technology services." As a result, the Executive Order clearly reaches physical network and infrastructure providers, but may not clearly reach edge, application, and over-the-top providers. The Executive Order thus may complicate commercial arrangements between network or physical infrastructure providers and edge or over-the-top providers, and create ambiguity about cybersecurity obligations and accountability.

1. Executive Order Summary

- *Information Sharing*: The Executive Order directs federal agencies to share unclassified reports of cyber threats with U.S. companies. DHS must provide classified government cyber threat and technical information to eligible critical infrastructure companies.

- *Framework to Reduce Cyber Risk to Critical Infrastructure*: The Executive Order requires NIST to work with industry to develop a set of industry best practices (the "Cybersecurity Framework") to reduce cyber risks to critical infrastructure. A preliminary version of the Cybersecurity Framework is due within 240 days of the Executive Order and a final version within one year.
- *Regulatory Review*: The Executive Order directs federal agencies to review their regulations and propose new authority as needed to address current and projected cyber risks to critical infrastructure. The PPD designates DHS as the sector-specific agency for the communications sector, subject to consultations with the FCC.
- *Identifying Critical Infrastructure*: Within 150 days, DHS must "identify critical infrastructure where a cybersecurity incident could reasonably result" in catastrophic consequences. DHS must confidentially notify owners and operators of critical infrastructure that they appear on the list, and listed entities will have an opportunity to submit information and request reconsideration of their identification as high-risk critical infrastructure.

2. PPD Summary

- *DHS to Take Lead Role*: As in the Executive Order, the PPD designates DHS as the primary authority in coordinating the federal government's actions to improve the security of critical infrastructure. The PPD instructs DHS to establish and operate two national critical infrastructure centers—one for physical infrastructure and one for cyber infrastructure.
- *Directives to FCC*: The PPD instructs the FCC to identify communications infrastructure and communications-sector vulnerabilities and to work with industry to address those vulnerabilities. The PPD also instructs the FCC to work with industry to develop best practices to promote the security and resilience of critical communications-sector infrastructure. Because the FCC is an independent regulatory agency, however, the PPD is not binding on the FCC. Given its establishment in 2010 of a Cybersecurity and Communications Reliability Division, the FCC can be expected to follow that call.
- *Information Sharing*: The PPD requires all levels of government and critical infrastructure owners and operators to timely exchange information on threats and vulnerabilities, including information that allows for the development of a situational awareness capability during incidents.

Given the number of entities involved and the timelines provided in the Executive Order, agencies likely will feel significant pressure to move quickly. Industry should therefore plan to engage quickly and proactively with FCC, DHS, NIST, and the Congressional Committees overseeing them in order to ensure that the policies and procedures created do not result in overly burdensome or costly reporting and compliance obligations.

3. Initial Implementation Steps by NIST and DHS

NIST began preparing for implementation of the Executive Order and PPD long before the White House issued final versions of those documents, thereby underscoring the need for early industry engagement. On February 13, 2013, NIST announced that it will soon publish in the *Federal Register* a Request for Information ("RFI") to stakeholders, including critical infrastructure owners and operators, asking them to share: (1) current cybersecurity risk management practices; (2) current use of existing cybersecurity standards and best practices; and (3) specific industry practices concerning, among other things, encryption and key management, asset identification and management, and security engineering practices. Once published, stakeholders will have 45 days to respond to the RFI.

On February 12, 2013, NIST and DHS entered into a Memorandum of Agreement ("MOA") that sets forth their collaboration plan for cybersecurity issues. Under the MOA, NIST agrees, among other things, to enable DHS participation in NIST-led engagements with industry. DHS agrees to consult with NIST on the metrics it intends to use to measure the effectiveness of cybersecurity programs.

4. Congressional Initiatives

Congressional action on cybersecurity remains likely. Representatives Mike Rogers (R-MI) and Dutch Ruppersberger (D-MD) reintroduced the Cyber Intelligence Sharing and Protection Act ("CISPA"), which passed the House but not the Senate in the last Congress. The House Permanent Select Committee on Intelligence already held a hearing on the bill on February 14, 2013. Before passing any legislation, however, Congress must first resolve several key contentious issues, including whether to mandate specific cybersecurity standards, and provide privacy protections and liability protection to industry. Representative Mike McCaul (R-Tex.), Chairman of the House's Homeland Security Committee, and Senator Tom Carper (D-Del.), Chairman of the Senate's top homeland security committee, have both expressed their intent to hold hearings on cybersecurity in the coming weeks.

* * * * *

For more information regarding cybersecurity issues or W&G's national security practice, please contact **Kent Bressie** at +1 202 730 1337 or kbressie@wiltshiregrannis.com, **Tricia Paoletta** at +1 202 730 1314 or tpaoletta@wiltshiregrannis.com, **Madeleine Findley** at +1 202 730 1304 or mfindley@wiltshiregrannis.com, or the W&G lawyer with whom you regularly work.

This client advisory is not intended to convey legal advice. It is circulated to our clients as a convenience and is not intended to reflect or create an attorney-client relationship as to its subject matter.