Skadden
PRIVACY & CYBERSECURITY UPDATE
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
& AFFILIATES
06.25.13

Cybersecurity Update: Key US and EU Regulatory Developments

In recent months, federal and state governments have taken an increasingly active role in reviewing cybersecurity issues within the private sector. There has been a flurry of activity as different government bodies discuss new review processes and information-sharing guidelines, and the promulgation of new regulatory requirements. We foresee the following three key developments:

- An expansion of disclosure obligations with respect to cybersecurity incidents;
- A potential increase in regulatory compliance obligations for network security practices, especially in heavily regulated industries; and
- Increased involvement by agencies and law enforcement officials in network security incidents, requiring companies to manage a diverse set of requests for information.

Executive Branch

In February, President Obama issued an executive order on cybersecurity[1] outlining various steps for agencies to take. This included a requirement that the National Institute of Standards and Technology (NIST) commence work on a Cybersecurity Framework (Framework) for operators of critical infrastructure, such as the energy and telecommunications sectors. Weeks later, NIST published a request for information (RFI) on critical infrastructure cybersecurity practices and released its initial analysis of the responses it received in May.[2] An annotated preliminary version of the Framework is expected in July, and an official draft of the Framework will be released for public comment in October.

The Department of Homeland Security (DHS) is concurrently developing a set of incentives to encourage voluntary adoption of the Framework by the private sector. In addition, various sector-specific agencies will be assessing the current network security practices of the entities they regulate. If these agencies have the appropriate regulatory authority and determine that the entities they regulate are critical but lack adequate protection, they will take steps to foster better network security, which might include increased regulation.

Significantly, "critical infrastructure" remains undefined, and therefore the extent to which the NIST Framework applies to specific industries is unclear. For example, NIST has requested that respondents focus on a few key critical infrastructure sectors, such as telecommunications, energy and financial services, while DHS, in its response to the NIST RFI, referenced "16 critical infrastructure sectors,"[3] reflecting the DHS view that critical infrastructure needs to be defined broadly.

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact **Stuart D. Levi,** 212.735.2750, stuart.levi@skadden.com or your regular Skadden contact.

* * *

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

Four Times Square
New York, NY 10036
Telephone: 212.735.3000

WWW.SKADDEN.COM

[1] The White House — Office of the Press Secretary, Executive Order: Improving Critical Infrastructure Cybersecurity, Feb. 12, 2013 (Cybersecurity Executive Order); *see also* Antoinette C. Bush, Stuart D. Levi, Ivan A. Schlager, John M. Beahn and Joshua F. Gruenspecht, "President Issues Cybersecurity Executive Order," *Skadden Privacy & Cybersecurity Update*, Feb. 13, 2013.

[2] *See Initial Analysis of Cybersecurity Framework RFI Responses*, NIST, at http://csrc.nist.gov/cyberframework/nist-initial-analysis-of-rfi-responses.pdf (May 15, 2013); *see also Developing a Framework to Improve Critical Infrastructure Cybersecurity*, Notice and Request for Information, 78 Fed. Reg. 13024 (Feb. 28, 2013).

[3] *See White Paper: DHS Response to the NIST Cybersecurity Framework Request for Information*, at http://csrc.nist.gov/cyberframework/rfi_comments/052813_dhs_nist_framework_response_white_paper.pdf (May 28, 2013).

On a separate track, the General Services Administration, along with the Department of Defense and DHS, has started reviewing network security auditing in government procurement processes, as also was required under the Cybersecurity Executive Order.[4] Companies can expect that the government will use its procurement processes as an indirect means to improve vendors' security practices. Congress is slowly endorsing this approach. For example, in March, it required a few select government agencies to make an "assessment of any associated risk of cyber-espionage or sabotage" before acquiring new information technology systems.[5]

Additional sector-specific standards are developing outside the NIST Framework as regulatory agencies begin to address network security:

- In May, the new SEC chairman issued a letter indicating her intent to have staff review whether "further action" on cybersecurity disclosures is required in SEC filings.[6]
- In April, NIST released a revised version of SP 800-53,[7] its official standards for federal government cybersecurity controls and an unofficial security reference for the private sector.
- Also in April, the Federal Energy Regulatory Commission issued a proposed rule codifying the latest version of the energy sector Critical Infrastructure Protection standards.

Cybersecurity Legislation Hits a Potential Roadblock

In April, the House of Representatives passed the Cyber Intelligence Sharing and Protection Act (CISPA),[8] a bill reintroduced with small changes from the previous session of Congress. CISPA would allow the government to share certain classified intelligence related to cybersecurity threats with private sector entities. In addition, it would allow private sector entities to share with federal agencies or other private sector entities information about threats to their own network security. As this information sharing might otherwise breach other laws, including federal privacy and antitrust laws, CISPA clarifies that such sharing is permitted "[n]otwithstanding any other provision of law."

Passage of CISPA suggested a potential for compromise between the White House and House Republicans on the passage of information-sharing cybersecurity legislation without the need to enact new regulatory authorities. In a demonstration of Democratic support, this latest version of CISPA received nearly 50 more Democratic House votes than its predecessor. In addition, the White House indicated a willingness to pursue private sector cybersecurity standards through existing powers and the Cybersecurity Executive Order, backing away from its prior position that cybersecurity legislation must include new regulatory authorities.[9] While threatening to veto the current version of CISPA, the White House signaled that it might accept a version with additional protections for civil liberties and narrowed limitations on liability for the sharing of information.

However, recent leaks regarding government surveillance programs that collect telecommunications information about private citizens may have clouded the prospects for CISPA and similar legislation, such as the FBI's reported proposal to require Internet communications services to build wiretap-ready products or face fines.[10] Such legislation is now likely to face harsher scrutiny. In addition, the Senate has indicated that it will again address information sharing as part of a broader package of cybersecurity reforms, including additional reforms to federal agency information security requirements and codification of the regulatory efforts undertaken as part of the Cybersecurity Executive Order.

[4] *Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition*, Request for Information, 78 Fed. Reg. 27966 (May 13, 2013).

[5] Consolidated and Further Continuing Appropriations Act of 2013, Pub. L. No. 113-6, Div. B § 516 (2013).

[6] See Christopher Matthews, "White Asks SEC Staff for Cyber Disclosure Briefing," *The Wall Street Journal*, May 13, 2013.

[7] *See* National Institute of Standards and Technology, NIST Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations (2013).

[8] H.R. 624 (2013).

[9] *See* Ellen Nakashima, "White House Backs Off Mandatory Cybersecurity Standards for Companies," *Washington Post*, April 26, 2013.

[10] Charlie Savage, "U.S. Weighs Wide Overhaul of Wiretap Laws," *New York Times*, May 7, 2013.

State Governments

Historically, given the lack of omnibus federal legislation, state governments have taken the lead in data security. Therefore, it is not surprising they are taking an active role in network security as well. Both New York and California have launched task forces to advise state agencies on statewide cybersecurity practices.[11] In May, the New York Department of Financial Services issued a request for information from insurance companies as part of a review of network security practices in the insurance industry.[12] We expect state governments to continue to expand efforts to address cybersecurity.

European Union

In February, the European Commission published its proposed directive on network and information security.[13] The proposed directive takes a more prescriptive approach to the issue by asking EU governments to establish national reporting authorities with the power to regulate network security in the technology services, energy, financial services, transportation and health care industries. These authorities would have the power to require entities to establish risk management measures and to review private sector risk management policies. They also would serve as central clearinghouses for the reporting of information security breaches and would be empowered to audit and issue binding instructions to regulated entities. Members of the European Parliament and member states have received the proposed directive with skepticism, asking whether a more voluntary and flexible approach might better suit the disparate needs of European governments. The proposed directive continues to be debated before the European Council, and its path forward remains unclear.

What Companies Should Consider

The foregoing is just a brief overview of recent developments in cybersecurity. Companies should monitor ongoing developments, and participate in forums that allow companies to provide their input on how cybersecurity regulation should be shaped. This is especially true in critical infrastructure sectors such as energy, financial services and defense contracting, where the chances of regulation being enacted are greatest. Finally, companies should routinely review their internal data and network security practices — and ensure that their executives understand the cybersecurity risk profiles.

[11] *See* Colin Wood, *California Launches Cybersecurity Task Force*, Emergency Management, May 20, 2013; “New York Regulator Asks Insurers About Readiness for Cyber Threats,” Insurance Journal, May 29, 2013.

[12] *See* “New York Regulator Asks Insurers About Readiness for Cyber Threats,” *Insurance Journal*, May 29, 2013.

[13] *See* Pierre Servan-Schreiber, Stuart D. Levi, Shari L. Piré and Joshua F. Gruenspecht, “Flaming Worms, Stuxnets and Other Cyber Threats — The European Union’s Response,” *Skadden Privacy & Cybersecurity Update*, April 8, 2013.