Skadden PRIVACY & CYBERSECURITY UPDATE

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
& AFFILIATES

03.05.13

NIST Issues Request for Information on Critical Infrastructure Cybersecurity Practices

On February 26, following close on the heels of the recent executive order setting forth the administration's approach to the regulation of critical infrastructure network security,[1] the National Institute of Standards and Technology (NIST) released an initial public notice and request for information (the NIST Notice).[2] The release of the NIST Notice is the first action in a year-long process through which NIST will develop the new voluntary framework for private sector critical infrastructure cybersecurity called for in the executive order (the Framework). **The comments requested in the NIST Notice provide the first opportunity for private sector operators of critical infrastructure to provide direct input into the crafting of the Framework**.

What Companies Are Affected?

The NIST Notice for the first time begins the task of empirically defining the set of critical infrastructure to be addressed in the Framework. In particular, NIST asks commenters for their input on infrastructure that supports their critical organizational assets and calls out five specific sectors upon which organizations may be relying:

- telecommunications;
- energy;
- financial services;
- water, and
- transportation.

Firms in those five sectors and in other sectors with the potential to be deemed "critical infrastructure" should pay close attention to the development of the Framework.

Changes in Regulatory Standards for Operating Information Technology and Networks

Critical infrastructure operators may want to consider treating the Framework as a *de facto* regulatory regime. While the Framework will not be legally binding in its own right, the administration has started to assess other legal authorities it possesses that could be used to persuade operators to adopt NIST's suggestions. The executive order asked various sector-specific regulatory agencies to review their regulatory power to impose the recommendations established by NIST. The executive order also required the Department of Homeland Security to create a list of designated critical infrastructure operators of particular importance and to provide that list to the sector-specific regulatory agencies. To the extent their existing regulatory powers allow it, those agencies may then impose a set of regulatory controls based on the Framework

[1] The White House — Office of the Press Secretary, *Executive Order: Improving Critical Infrastructure Cybersecurity*, Feb. 12, 2013. For more information, *see Skadden Privacy and Cybersecurity Update: President Issues Cybersecurity Executive Order*, Feb. 13, 2013.

[2] *Developing a Framework to Improve Critical Infrastructure Cybersecurity*, Notice and Request for Information, 78 Fed. Reg. 13024-13028 (Feb. 28, 2013).

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or your regular Skadden contact.

Stuart D. Levi
New York Office
212.735.2750
stuart.levi@skadden.com

Antoinette C. Bush
Washington, D.C.
202.371.7230
antoinette.bush@skadden.com

Ivan A. Schlager
Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

John M. Beahn
Washington, D.C.
202.371.7392
john.beahn@skadden.com

Joshua F. Gruenspecht
Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com

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

1440 New York Avenue, NW
Washington, D.C. 20005
Telephone: 202.371.7000

WWW.SKADDEN.COM

on the designated critical infrastructure operators. Moreover, in order to encourage adherence to the Framework, the administration has indicated that it will soon release an updated proposal for cybersecurity legislation that will include limitations on liability from network security incidents for those critical infrastructure operators that adopt the Framework.[3] In addition, critical infrastructure operators are likely to face inquiries from regulatory agencies such as the SEC and even potential lawsuits should they fall victim to a cyber incident after failing to adopt the practices suggested by the Framework or a similar set of cybersecurity best practices.

It is not yet clear how far-reaching the standards and guidelines promulgated by NIST are likely to be, but the NIST Notice suggests that the final Framework will include:

- a consultative process to assess cybersecurity-related risks;
- a menu of management, operational and technical security controls;
- a consultative process to identify security controls that will address risks and protect data;
- a set of metrics, methods, and procedures to assess and monitor the effectiveness of security controls;
- a comprehensive risk management approach; and
- a menu of privacy controls.

In addition, the draft Framework is expected to "build on NIST's ongoing work with cybersecurity standards and guidelines."

Next Steps

In-house counsel at companies that fall into one of the critical infrastructure sectors should promptly begin to assess their current network security practices. In addition, such companies may want to consider providing input into the regulatory process in order to shape this new regulatory regime. The NIST Notice requests comment on several questions in three broad areas: cybersecurity risk management practices; use of frameworks, standards, guidelines and best practices; and specific industry practices. The first set of questions asks for input on the general cybersecurity threat and how organizations measure it; the organizational policies, practices and tools deployed to mitigate that risk; and the existing regulatory requirements to manage cybersecurity risk. The second set asks for input on the usage, robustness and applicability of existing public and private cybersecurity standards. The third set asks for input on which cybersecurity practices may be broadly applicable across sectors and which may be specific to a given industry. **Comments in response to this initial notice must be submitted by April 8th**.

As the Framework development process continues, there will be additional opportunities to comment and provide feedback. Skadden, Arps can assist companies that wish to avail themselves of opportunities both to provide formal comment and to participate informally in the NIST process. Skadden practice groups with experience in various aspects of cybersecurity include Privacy and Data Security, Communications and CFIUS/National Security.

[3] *See* Eric Engleman & Jordan Robertson, *Obama to Share Cybersecurity Priorities With Congress*, Bloomberg, Feb. 27, 2013, http://www.bloomberg.com/news/2013-02-27/obama-to-share-cybersecurity-priorities-with-congress.html.