Skadden

PRIVACY & CYBERSECURITY UPDATE

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

09.18.13

NIST Cybersecurity Framework: Discussion Draft Update

On September 11-13, the National Institute of Standards and Technology (NIST) hosted its fourth Cybersecurity Framework Workshop to solicit feedback on its recently released partial draft (Discussion Draft) of the NIST Cybersecurity Framework (the Framework).[1] The Discussion Draft is the latest verson of the Framework that President Obama ordered NIST to develop in his February 12 executive order addressing the regulation of critical infrastructure network security.[2] The Discussion Draft offers the first substantive look at the Framework and thus the potential impact on companies that adopt it.

The Discussion Draft

The Discussion Draft presents a Framework that is open-ended in a variety of ways. For example, organizations may choose which standards to apply to meet their functional requirements, and how comprehensive their implementation of those standards should be. NIST has emphasized this as an important feature, noting that "[t]he Framework is not a one-size-fits-all approach for all critical infrastructure organizations."

The Framework is composed of three parts:

- The ***Framework Core*** consists of five essential functions that NIST considers part of a comprehensive view of cybersecurity risk:
  - identifying which systems, assets and data require protection;
  - protecting those systems, assets and data by implementing appropriate safeguards;
  - detecting the occurrence of cybersecurity events;
  - responding to cybersecurity events detected; and
  - recovering capabilities impaired through a cybersecurity event.

  The ***Framework Core*** then further subdivides these functions into categories and subcategories and provides cross-references to a number of different standards from both industry and government that address each subcategory within those functions. Organizations can review these references and select the standard that best addresses their particular needs.

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
212.735.2750
stuart.levi@skadden.com

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

[1] National Institute of Standards and Technology, *Discussion Draft of the Preliminary Cybersecurity Framework*, Aug. 28, 2013, at http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf.

[2] The White House – Office of the Press Secretary, *Executive Order: Improving Critical Infrastructure Cybersecurity*, Feb. 12, 2013. The Executive Order, which touched on a variety of cybersecurity topics, directed NIST to develop a Framework — in effect, a voluntary standard — that includes a set of "standards, methodologies, procedures, and processes" to help owners and operators of critical infrastructure identify, assess and manage cyber risk. This includes identifying cross-sector security standards and guidelines applicable to critical infrastructure as well as areas for improvement that should be addressed through future collaboration.

- The ***Framework Implementation Tiers*** describe the level of sophistication an organization applies to each Framework Core function. There are four tiers, ranging from partial, in which an organization does not have a formal risk management process, to adaptive, in which an organization regularly incorporates new information into its approach. Organizations that adopt the Framework determine a desired tier at each function and category level based on organizational goals, expected reduction in cybersecurity risk and feasibility of implementation. For example, an organization may evaluate its risk profile and choose to put more resources into robust recovery from cybersecurity events and fewer into asset protection.
- Once an organization selects tiers across all functions and categories, it has developed a ***Framework Profile*** — a cybersecurity risk mitigation response strategy. It can then regularly compare its then-current Framework Profile to its target version and take action as required.

  The Framework may become more structured than the current draft. NIST has highlighted seven areas regarding which it hopes to receive additional input over the next months as the first full draft is completed and public notice and comment begins:

  - authentication;
  - automated indicator sharing;
  - conformity assessment;
  - data analytics;
  - international aspects, impacts, and alignment;
  - privacy; and
  - supply chains and interdependencies.

Some of these areas — such as privacy — represent significant concerns for companies involved with critical infrastructure. If NIST attempts to address these complex substantive topics, the Framework may develop into a more prescriptive set of standards.

Incentives for compliance with the Framework also remain unclear. In August, the Department of Homeland Security (DHS) made public a preliminary list of incentives that the government might offer companies that opt to comply with the Framework. However, it is still far from clear how those incentives may be deployed in practice. Only after the sector-specific regulatory agencies submit their reports after the release of the NIST preliminary draft in October 2013 will the White House know what incentives and disincentives those agencies can offer under their existing regulatory authorities.

Next Steps

- The full preliminary Framework draft is scheduled for release in October 2013.
- Action on cybersecurity will begin to shift to various sector-specific regulatory agencies. Ninety days after the release of the preliminary draft, the executive order requires these agencies to report on their ability to mitigate risks to critical infrastructure industries by adopting regulations based on the Framework. Additional regulations may follow, depending on the agencies' findings. In addition, certain external events, such as a foreign cyberattack on U.S. infrastructure, will enhance the chances that sector-specific agencies propose more prescriptive regulations.
- At the same time, the DHS will continue its work on developing incentives to encourage the voluntary adoption of the Framework by owners and operators of critical infrastructure.
- Release of the final Framework is scheduled for February 2014.

Throughout this period, NIST is expected to continue engaging the private sector and requesting input. In-house counsel at companies may want to consider providing input into the regulatory process to shape any forthcoming regulatory regime.

Skadden continues to follow the cybersecurity regulatory process within NIST and other agencies as it unfolds and can assist clients in understanding the applicability of the Framework to their companies and its implications within their industries.