Skadden PRIVACY & CYBERSECURITY UPDATE
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP & AFFILIATES
10.25.13

NIST Cybersecurity Framework: Preliminary Draft Issued

On October 22, the National Institute of Standards and Technology (NIST) issued its Preliminary Cybersecurity Framework (the Preliminary Framework).[1] The Preliminary Framework represents the first full draft of the Cybersecurity Framework (the Framework) that President Obama ordered NIST to develop in his February 12, 2013, executive order addressing the regulation of critical infrastructure network security.[2]

As its name suggests, this document provides a framework that companies can use to guide their evaluation of their cybersecurity practices, to develop a plan to reduce their risks and to respond to security breaches. While the Preliminary Framework does not propose new cybersecurity standards, the executive order mandates that agencies use the Framework (once it is finalized) as the basis for reviewing critical infrastructure cybersecurity within regulated sectors. The executive order also asks those agencies to consider whether they have the legislative authority to enact any regulations that might be required. As a result, companies in regulated critical infrastructure industries should understand the basic contours of the Preliminary Framework.

Preliminary Framework Basics

The Preliminary Framework — which hews closely to the discussion draft of the Framework released in late August (the Discussion Draft) — remains open-ended, with little specific guidance on steps companies should take to improve their security posture. Instead, the Preliminary Framework lists various existing standards companies might adopt. For example, when advising that companies use separate testing environments for system development, the Preliminary Framework lists sections of the COBIT, ISO 27000 series and NIST SP 800 series standards that offer more specific suggestions on implementing such environments.[3]

The Preliminary Framework, like the Discussion Draft on which it is based, is composed of three parts — a Framework Core, the Framework Implementation Tiers and the Framework Profile. The Framework Core lists the five security functions that a cybersecurity-conscious organization should consider, then breaks each one into categories and subcategories that should be addressed. The Framework Implementation Tiers provide companies with different tiers they

1 National Institute of Standards and Technology, *Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework*, Oct. 22, 2013, at http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.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.

3 COBIT is the Control Objectives for Information and Related Technology, and ISO 27001 is a product of the International Organization for Standardization. Both are commonly applied private sector cybersecurity standards. The NIST standards are required for certain government information technology systems but also widely referenced in the private sector.

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

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

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

might fall into depending, in part, on how proactive they are in assessing risk. Finally, the Framework Profile is a tool organizations can use to apply the Framework Implementation Tiers to the functions under the Framework Core and develop a comprehensive cybersecurity strategy.

For more information on the basic composition of the Preliminary Framework, please refer to our recent mailing on the Discussion Draft, available here.[4]

Notable Changes From the Discussion Draft

Although the Preliminary Framework closely tracks the Discussion Draft, there are a few important changes to note. Unlike the Discussion Draft, the Preliminary Framework is the first version to identify specific critical infrastructure industries. The draft indicates that "critical infrastructure" includes all 16 sectors designated as such by the presidential directive that accompanied the original executive order, including:

- chemical
- commercial facilities
- communications
- critical manufacturing
- dams
- defense industrial base
- emergency services
- energy
- financial services
- food and agriculture
- government facilities
- healthcare and public health
- information technology
- nuclear services
- transportation systems
- water systems

Specific identification of these sectors likely lays to rest the possibility that the Framework will adopt a narrower definition of critical infrastructure.

In addition, the Preliminary Framework clarifies that critical infrastructure operators should employ the Framework not only to address information technology security, but also industrial control system (ICS) security. Companies in critical infrastructure sectors that use ICSs, including energy, nuclear services and transportation, should be aware of the potential for new regulation of those systems.

While the Preliminary Framework offers more specificity regarding covered entities and systems, it is more general than the Discussion Draft in defining the functions in the Framework Core. For example, where the Discussion Draft suggested that operators prepare to detect anomalies by "[i]dentify[ing] and determin[ing] normal organizational behaviors and expected data flow of personnel, operational technology, and information systems," the Preliminary Framework merely recommends that "[a] baseline of normal operations and procedures is identified and managed." Relaxed guidelines such as this one may broaden the applicability of the Framework, but also increase the vagueness of the list of categories and subcategories to implement.

The Preliminary Framework also adds new language explicitly recommending that critical infrastructure operators consider the associated appendix addressing protections for privacy and civil liberties. That appendix offers a set of privacy and civil liberties issues corresponding to the

---

4 Stuart D. Levi, Ivan A. Schlager and Joshua F. Gruenspecht, "NIST Cybersecurity Framework: Discussion Draft Update," *Privacy & Cybersecurity Update*, Sept. 18, 2013.

categories and subcategories of the Framework Core. The Preliminary Framework suggests that potential privacy issues should be considered when preparing to address each corresponding category when designing a cybersecurity strategy.

Going Forward

The Framework is not yet complete, although NIST appears increasingly unlikely to make major modifications. While the release of the Preliminary Framework was delayed by the government shutdown, NIST has indicated that it intends to continue to adhere to the schedule laid out in the executive order and will release the first official edition of the Framework in February 2014.

The official release of the Preliminary Framework commences the next step of the process set forth in the executive order. Ninety days after the release, the executive order requires applicable agencies to report on their ability to mitigate risks to critical infrastructure industries by adopting regulations based on the Preliminary Framework. Some critical infrastructure regulators are already considering how best to implement appropriate aspects of the executive order under their existing authorities.[5]

In addition to the creation of the Framework itself, NIST and the Department of Homeland Security continue to revise and develop incentives to encourage companies voluntarily to adopt the Framework. One much-discussed incentive is liability protection for those who adopt the Framework. Such protection could prove important since creative class action plaintiffs may try to assert in a data breach case that the Framework is a *de facto* standard, and that the entity suffering the breach failed to adhere to it.

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 and subsequent sector-specific regulations to their companies and the implications within various industries.

---

5 Remarks by Thomas J. Curry, Comptroller of the Currency, Before the Exchequer Club, Washington, D.C., Sept. 18, 2013.