crowell moring

CLIENT ALERT

Overview of NIST Preliminary Cybersecurity Framework for Executive Order No. 13636 – Improving Critical Infrastructure Cybersecurity

Oct.25.2013

I. Introduction

On October 22, 2013, the Department of Commerce's National Institute of Standards and Technology (NIST) issued its Preliminary Cybersecurity Framework.[1] This Framework is an element of the February 2013 Executive Order directing NIST to develop a framework for managing cybersecurity risk.[2]

While still preliminary, this Framework has emerged after a series of public workshops and an information request that have already provided considerable public input. After the preliminary Framework is published in the Federal Register, a 45-day public comment period will commence, followed by a planned release of the official Framework in February 2014.

II. Key Issues for the Preliminary Cybersecurity Framework

Identifying the cyber threat as "one of the most serious national security challenges we must confront," the Executive Order directed NIST to lead the development of a framework that "shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks." In seeking to implement this direction, the 44-page Preliminary Cybersecurity Framework addresses a number of issues that will be subject to further public discussion and comment.

A. Potential Applicability of the Cybersecurity Framework

The Framework can have broad applicability, as dictated by the Executive Order. In particular, federal agencies and government contractors will likely be affected by the Framework, given that the Executive Order tasked the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary of the Department of Homeland Security (DHS) and the Federal Acquisition Regulatory Council, with making recommendations "on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration."

In addition, DHS is in the process of developing a program that would encourage and incentivize voluntary adoption of these standards. This program is in addition to DHS's authority under the Executive Order to notify specific companies that are determined to be at high risk. Finally, the Framework may have broader implications as it is used by other government agencies and third parties such as the insurance industry and the judiciary.

B. Framework Objectives and Core take a Flexible, Cost-Effective Approach

The Executive Order specified that the Framework must provide "a prioritized, flexible, repeatable, performance-based, and cost-effective approach" to identifying, assessing, and managing cybersecurity risks. The Framework adopts a risk-based approach consistent with many of the existing cybersecurity standards.

The Framework also identifies integral roles for senior executives in making decisions on how to address cybersecurity needs and threats. In short, the Framework treats cyber risk management not simply as an issue confined to the Information Technology (IT) department, but instead as a broader issue that must include senior executives of the organization.

One components of the Framework that has caused much discussion relates to the "Framework Implementation Tiers." Using a four-tier approach, NIST sought to "describe an increasing degree of rigor and sophistication in cybersecurity risk management practices." An organization may be concerned with the this aspect of the Framework as it could raise their external profile by noting vulnerabilities in their networks, thereby causing reactions from government agencies or potential threat actors. For example, the Framework defines the Tier 1 "risk management process" as being "an ad hoc and sometimes reactive" approach to addressing cyber risk, while the Tier 1 "integrated program" reflects "limited awareness of cybersecurity risk."[3]

The main thrust of the Framework is described in the "Framework Core" which describes a set of activities and references that are outcome based and focused on specific actions at all levels of the organization. These functions and categories are not new, but instead have roots in existing information security standards. The functions include the following.

- **Identify** – which includes: managing assets (personnel, systems, and facilities) and data flows; understanding the business environment in which the entity operates; implementing policies and procedures to ensure appropriate security and legal compliance; conducting a risk assessment; and managing risk appropriately.
- **Protect** – which includes: controlling access to information and facilities; informing and training employees and partners; securing data consistent with the organization's risk strategy; implementing policies and procedures to secure data (including policies regarding change control, backups, physical security, data destruction, incident response plans, etc.); maintaining and repairing operational and information system components; and adopting technical solutions to support data security efforts.
- **Detect** – which includes: adopting processes to detect anomalous activities in a timely manner and respond appropriately; engaging in ongoing monitoring efforts to detect cybersecurity events and identify vulnerabilities; and implementing (and routinely testing) policies and processes to detect security events.
- **Respond** – which includes: implementing a response plan during or after an event; ensuring that event response activities are coordinated between internal and external stakeholders; analyzing the cause and impact of the incident; containing and eradicating incidents; and incorporating lessons learned into updated response plans.
- **Recovery** – which includes: utilizing a plan to restore systems (and routinely testing that plan); improving recovery plans by incorporating lessons learned; and managing public relations in a coordinated fashion as well as repairing reputations after an event.

III. Next Steps

The preliminary Framework raises a number of important issues for the private sector, including the following:

- How broadly may the Framework apply?
- What are the Framework's core objectives?
- How does risk management factor into the Framework?
- What are the expected roles for senior executives?
- What are the different tiers for cybersecurity programs?
- How do the security "functions" compare to current standards?

The eighteen critical infrastructure sectors already cover huge portions of the public and private sectors, including banking and finance, chemical, communications, critical manufacturing, defense industrial base, energy, government facilities, healthcare, information technology, and transportation systems. Even beyond critical infrastructure, the Framework may drive standards and practices for government contractors and other major sectors of the economy. For this reason, organizations that may be affected by the Framework have both an opportunity – and good business reasons – to provide input into the process while NIST is still receiving comments and questions from other parties.

As the discussion about the Framework continues to evolve, we will continue to track these developments, identify key issues affecting the private sector, and provide comments during the process.

[1] NIST announced the Preliminary Cybersecurity Framework on its website. http://www.nist.gov/itl/cybersecurity-102213.cfm. The Preliminary Framework is available at http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

[2] Exec. Order No.13636, 78 Fed. Reg. 11739 (Feb. 19, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[3] This version of the Framework has modified the numbering of the Tiering system which now begins with "Tier 1" rather than "Tier 0."

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com