Published on *The National Law Review* https://natlawreview.com

New Cybersecurity Framework Revealed

Article By:

Gregory T. Parks

Ezra D. Church

The framework provides standards and best practices for identifying, assessing, and managing cybersecurity risk.

Now that the **Obama administration** has unveiled the final version of its anticipated **Cybersecurity Framework** (the Framework),[1] companies should begin to evaluate how it may apply to their businesses. The Framework, issued on February 12, is aimed at developing common practices and a consistent approach for protecting critical infrastructure from cybersecurity threats. Although the Framework is voluntary, businesses, especially those that may be part of the "critical infrastructure," should consider these guidelines in developing and reviewing their own information technology policies and practices.

Background

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure and that "[r]epeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity," on February 12, 2013, President Barack Obama issued Executive Order 13636, which called for standards and best practices that address cybersecurity threats.[2] Specifically, the Executive Order directed that the National Institute of Standards and Technology (NIST) lead the development of a "framework to reduce cyber risks to critical infrastructure," including "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and control, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk." The resulting Cybersecurity Framework was issued by the NIST on February 12, 2014.

Framework Overview

Building on existing standards, guidelines, and practices employed by government and industry, the Framework does not provide rules for addressing cybersecurity but does provide a taxonomy and methodology for identifying and responding to cyber risk. The hope, expressed in the Framework, is that organizations will use the "common language" to assess their current risk management processes and cybersecurity program and identify opportunities to improve and that organizations without an existing program will use the Framework to create one. The Framework is composed of

three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles.

1. The Framework Core (Core): The Core identifies the key activities needed to ensure cybersecurity and is composed of four elements: Functions, Categories, Subcategories, and Informative References. The Framework provides discussion and examples for these activities, including helpful tables and a cataloging system that assigns a unique identifier to the different elements.

- The Functions express the basic activities describing an operational culture that addresses cybersecurity risk—Identify, Protect, Detect, Respond, and Recover.
- The Categories are the subdivisions of a Function. For example, the Identify Function might include the following Categories: Asset Management, Business Environment, and Governance.
- Subcategories further divide a Category into specific outcomes that support the activities in each Category. For example, the Subcategories of Asset Management might include "Physical devices and systems are inventoried" and "Organizational communication and data flows are mapped."
- Finally, Informative References identify the specific sections of policies, standards, or guidelines applicable to the activities in each Subcategory. The Framework references globally recognized standards, and the NIST has developed a compendium of those standards gathered through the Framework's development.

2. The Framework Implementation Tiers (Tiers): The Tiers describe the increasing degree of rigor and sophistication in cyber risk management practices. They range from Partial (Tier 1), where an organization's risk management practices are not formalized and where risk is managed on an ad hoc and often reactive basis, to Adaptive (Tier 4), where the organization has a comprehensive and organizationwide cybersecurity program that can be adapted, based on lessons learned and predictive indicators, and where the organization actively shares information with partners. The Framework acknowledges that selecting the right Tier involves considering the organization's current risk management practices, the threat environment, legal and regulatory requirements, business and mission objectives, and organizational constraints. Although organizations identified as Partial (Tier 1) "are encouraged to consider moving toward Tier 2 or greater," the Framework recognizes that some organizations cannot or need not reach Tier 4, stating that "[p]rogression to higher Tiers is encouraged when such a change would reduce cybersecurity risks and be cost effective."

3. The Framework Profile (Profile): The Profile involves aligning the Functions and related activities described in the Core with an organization's specific business requirements, risk tolerance, and resources to establish a roadmap for reducing cyber risk. Because many organizations are complex and have different functions and roles within the critical infrastructure, they may have a variety of Profiles. A comparison of current and target Profiles can help identify cybersecurity gaps and establish a plan to address them.

The Framework also recognizes the need to address individual privacy and civil liberties implications that may arise from cybersecurity operations, particularly when personal information is used, collected, processed, maintained, or disclosed in connection with an organization's cybersecurity activities. Such issues play a critical role in "creating greater public trust." The Framework requires organizations to consider, where appropriate, ways in which their cybersecurity program incorporates principles such as the following:

- Minimizing data in the collection, disclosure, and retention of personal information related to a

cybersecurity breach or other event
- Using limits outside of cybersecurity activities
- Having transparency for certain cybersecurity activities
- Requiring individual consent and redress for adverse impacts that arise from using personal information
- Maintaining data quality, integrity, and security

The Framework applies to organizations that participate in the "critical infrastructure," which is defined broadly in the Executive Order as "systems and assets, whether physical or virtual, so vital to the security of the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The Framework urges application to organizations "regardless of size, degree of cybersecurity risk, or cybersecurity sophistication." The Executive Order specifically identifies 16 critical infrastructure sectors, including chemical, communications, critical manufacturing, dams, defense, emergency services, energy, financial services, food and agriculture, healthcare, information technology, transportation, and water and wastewater systems.

Finally, the Executive Order required the NIST to maintain and develop the Framework on an ongoing basis, and the NIST has said that the Framework is intended to be a "living document," even titling it "Version 1.0." The NIST issued a simultaneous roadmap that discusses next steps and identifies key areas for cybersecurity development, such as authentication, automated indicator sharing, data analytics, and supply-chain management.[3]

Implications

The Framework is voluntary, and that point has been emphasized both within the Framework and in the press releases and discussions surrounding its release. However, particularly in the wake of recent high-profile data breaches, businesses—particularly those that may be part of the critical infrastructure—should consider the Framework as they develop their own policies and procedures to address cybersecurity. As defined by the Executive Order, that term would likely apply to a wide range of industries, including financial services, technology, energy, retail, food, and health sciences.

---

[1]. View the Framework here.

[2]. View Executive Order 13636 here.

[3]. View the roadmap here.

National Law Review, Volume IV, Number 108