Proposed Changes to the NIST Cybersecurity Framework

By Jay Brudz, Kenneth K. Dort and Lee G. Petro

The National Institute of Standards and Technology (NIST) issued an update to its Framework for Improving Critical Infrastructure Cybersecurity (“Framework”) on January 10, 2017. The updated draft Version 1.1 (“Draft”) was issued after NIST’s review of public and private-sector feedback on Version 1.0. The updated Draft includes improvements but is intended to remain a voluntary cyber risk management tool that organizations can customize.

By way of background, NIST released Version 1.0 of the Framework in February 2014 pursuant to Executive Order 13636. At that time, NIST simultaneously published a companion document, NIST Roadmap for Improving Critical Infrastructure Cybersecurity (“Roadmap”), in which it tasked the Framework drafters to identify “areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations.” The Roadmap identified several high-priority areas that are reflected in Version 1.1, such as (i) Supply Chain Management, (ii) Authentication, and (iii) Information Sharing. The updated Draft also addresses the issue of cybersecurity measurement and metrics based on feedback received on Version 1.0 and drawing from the technical expertise found in a number of NIST’s recently issued Special Publications.

The updated Draft is intended to be compatible with Version 1.0. As such, the five Framework Core Functions remain the same – Identify, Protect, Detect, Respond and Recover. Additionally, new Categories, Subcategories, and enhanced guidance have been incorporated in the updated version of the Framework.

The Categories, Subcategories and enhanced guidance are highlighted below:

1. Cyber Supply Chain Risk Management. The updated Draft presents new risk management considerations for an organization’s product and service supply chains. Based on clear directives in the Roadmap and comments, NIST adopted several measures to promote supply chain risk management (SCRM). For example, Section 3.3 asks organizations to (i) identify third-party vendors who have access to their security infrastructure; (ii) determine appropriate cyber governance and contractual standards; and (iii) enforce cyber risk management requirements with vendors.

SCRM is prominently featured in the updated Draft as a new Category within the Identity Function. The SCRM Category consists of five Subcategories for organizations to establish management processes with stakeholder buy-in, identify and prioritize vendors, implement measures for vendors, monitor vendors, and coordinate incident response planning and penetration testing. The updated Draft reflects an improved approach to manage external risks due to vendors and points to helpful industry-backed standards as guidance (e.g., COBIT5 and CISP CSC 4.8).

Notes:

2. Note, the Framework consists of the three components. First, the Core involves a common matrix of cybersecurity activities (i.e. designated Functions, Categories and Subcategories based on industry standards and guidelines), outcomes, and informative references that organizations can follow to manage cybersecurity risks. Second, Profiles enable organizations to align their cyber activities with business objectives and operational needs. Third, Implementation Tiers can be used by organizations to assess their approaches to managing cybersecurity risks. Framework for Improving Critical Infrastructure Cybersecurity, Version 10, National Institute of Standards and Technology (February 2014), available at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-2014.pdf


5. The five Core Functions of the Framework represent a high-level view of the basic activities involved in cybersecurity risk management: (i) Identify; Organizations understand and review their assets, business environment, and governance structure and assess their cybersecurity risks; (ii) Protect; Organizations develop and implement safeguards to limit or contain a cybersecurity event; (iii) Detect; Organizations develop and implement processes to timely discover cybersecurity events; (iv) Respond; Organizations create response plans and conduct activities to mitigate and contain a cybersecurity event; and (v) Recover; Organizations timely restore systems and recover from a cybersecurity event.

6. “Categories” are defined by the Framework as “subdivisions of Functions into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities.”

7. “Subcategories” are defined by the Framework subsets of Categories into specific outcomes of technical and/or management activities,” which “help support achievement of the outcomes in each Category.”
The Cyber SCRM considerations are now applied to the Frameworks’ Implementation Tiers, ranging from Partial (Tier 1) to Adaptive (Tier 4). For example, organizations who meet the most sophisticated Tier 4 criteria must exhibit a highly-responsive approach to cybersecurity based on real-time information and institutional knowledge. Whereas Tier 1 organizations, who have only informal or reactive cybersecurity practices in place, are either unable to anticipate cyber supply chain risks or lack the processes to manage them.

2. Information Sharing. The updated Draft adds guidelines for organizations to incorporate information sharing into their cybersecurity risk management activities. Following the passage of the Cybersecurity Information Sharing Act in December 2015, as well as the popularity of industry-specific Information Sharing and Analysis Centers (ISACs), organizations are increasingly looking to partners in the private sector and the government to exchange cyber threat intelligence. Besides playing a proactive role in the Risk Assessment Subcategory (ID.RA-2) and the incident response Communications Subcategory (RS.CO-5), the updated Draft incorporates information sharing practices into the Implementation Tiers – assessing how organizations participate externally. For example, a Tier 4 organization “actively shares information with partners to ensure that accurate, current information is being distributed consumed to improve cybersecurity before a cybersecurity event occurs.” Additionally, NIST urges organizations to adopt policies that consider the privacy implications when sharing information with external partners or ISACs, particularly when personally identifiable information is involved.

3. Cybersecurity Measurement. Another new section in the updated Draft is devoted to measuring and demonstrating cybersecurity. Section 4.0 outlines how the Framework can be used to illustrate different aspects of an organization’s cybersecurity posture to stakeholders through the use of metrics and measures. Whereas cyber “metrics” are a qualitative attribute “used to facilitate decision making and improve performance and accountability” (e.g., the effectiveness of an organization’s incident response plan), the updated Draft defines “measures” as “quantifiable, observable, objective data supporting metrics” (e.g., the percentage of systems within an organization that are not patched or impact measures for the consequences of cyber incidents).

The updated Draft encourages correlating cybersecurity measurement and business outcomes because it “may provide meaningful insight as to how changes in granular security controls impact the completion of business objectives.” Organizations are asked to design measures and metrics “with business requirements and operating expense in mind,” to inform accuracy and precision. Recognizing the difficulty of understanding these cause-and-effect relationships, NIST suggests organizations use and compare current versus target Framework Profiles (i.e. aligning the Framework with business needs, risk allowance, and resource constraints) to conduct a risk-based gap analysis.

4. Authentication. The updated Draft also renamed the “Access Controls” Category to a more expansive title, “Identity Control and Access Control.” Notably, (i) Subcategory PR.AC-1 was adjusted to consider wider identity management issues, including credentials for authorized devices, users, and processes; and (ii) a new Subcategory PR.AC-6 has been added for authenticating identities. Furthermore, Version 1.1 renews the Roadmap’s call for organizations to adopt multi-factor authentication and identity proofing solutions.

The proposed changes to the Framework address key industry concerns raised by public comment to Version 1.0, as well as those previously released in the Roadmap. NIST will seek additional feedback and hold a public workshop (expected in Fall 2017) before finalizing Version 1.1. Comments to the proposed changes will be accepted until April 10, 2017, and can be sent to NIST.

Drinker Biddle will continue to monitor the discussions and will provide future updates on the Draft.

Information Privacy, Security and Governance Team

Jay Brudz
Partner
Washington
(202) 230-5195
Jay.Brudz@dbr.com

Kenneth K. Dort
Partner
Chicago
(312) 569-1458
Kenneth.Dort@dbr.com

Lee G. Petro
Of Counsel
Washington
(202) 230-5857
Lee.Petro@dbr.com

www.drinkerbiddle.com