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

# NIST Releases Updated Draft of Cybersecurity Framework

Article By:

Susan B. Cassidy

Moriah Daugherty

On December 5, 2017, the National Institute of Standards and Technology ("NIST") announced the publication of a second draft of a proposed update to the Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework"), Version 1.1, Draft 2. NIST has also published an updated draft Roadmap to the Cybersecurity Framework, which "details public and private sector efforts related to and supportive of [the] Framework."

## Updates to the Cybersecurity Framework

The second draft of Version 1.1 is largely consistent with Version 1.0. Indeed, the second draft was explicitly designed to maintain compatibility with Version 1.0 so that current users of the Cybersecurity Framework are able to implement the Version 1.1 "with minimal or no disruption." Nevertheless, there are notable changes between the second draft of Version 1.1 and Version 1.0, which include:

Increased emphasis that the Cybersecurity Framework is intended for broad application across all industry sectors and types of organizations. Although the Cybersecurity Framework was originally developed to improve cybersecurity risk management in critical infrastructure sectors, the revisions note that the Cybersecurity Framework "can be used by organizations in any sector or community" and is intended to be useful to companies, government agencies, and nonprofits, "regardless of their focus or size." As with Version 1.0, users of the Cybersecurity Framework Version 1.1 are "encouraged to customize the Framework to maximize individual organizational value." This update is consistent with previous updatesto NIST's other publications, which indicate that NIST is attempting to broaden the focus and encourage use of its cybersecurity guidelines by state, local, and tribal governments, as well as private sector organizations.

An explicit acknowledgement of a broader range of cybersecurity threats. As with Version 1.0, NIST intended the Cybersecurity Framework to be technology-neutral. This revision explicitly notes that the Cybersecurity Framework can be used by all organizations, "whether their cybersecurity focus is primarily on information technology ("IT"), cyber-physical systems ("CPS") or connected devices more generally, including the Internet of Things ("IoT"). This change is also consistent with previous updates to NIST's other publications, which have recently been amended to recognize that cybersecurity risk impacts many different types of systems.

Augmented focus on cybersecurity management of the supply chain. The revised draft expanded section 3.3 to emphasize the importance of assessing the cybersecurity risks up and down supply chains. NIST explains that cyber supply chain risk management (“SCRM”) should address both “the cybersecurity effect an organization has on external parties and the cybersecurity effect external parties have on an organization.” The revised draft incorporates these activities into the Cybersecurity Framework Implementation Tiers, which generally categorize organizations based on the maturity of their cybersecurity programs and awareness. For example, organizations in Tier 1, with the least mature or “partial” awareness, are “generally unaware” of the cyber supply chain risks of products and services, while organizations in Tier 4 use “real-time or near real-time information to understand and consistently act upon” cyber supply chain risks and communicate proactively “to develop and maintain strong supply chain relationships.” The revised draft emphasizes that all organizations should consider cyber SCRM when managing cybersecurity risks.

Increased emphasis on cybersecurity measures and metrics. NIST added a new section 4.0 to the Cybersecurity Framework that highlights the benefits of self-assessing cybersecurity risk based on meaningful measurement criteria, and emphasizes “the correlation of business results to cybersecurity risk management.” According to the draft, “metrics” can “facilitate decision making and improve performance and accountability.” For example, an organization can have standards for system availability and this measurement can be used at a metric for developing appropriate safeguards to evaluate delivery of services under the Framework’s Protect Function. This revision is consistent with the recently-released NIST Special Publication 800-171A, discussed in a previous blog post, which explains the types of cybersecurity assessments that can be used to evaluate compliance with the security controls of NIST Special Publication 800-171.

## Future Developments to the Cybersecurity Framework

NIST is soliciting public comments on the draft Cybersecurity Framework and Roadmap no later than Friday, January 19, 2018. Comments can be emailed to cyberframework@nist.gov.

NIST intends to publish a final Cybersecurity Framework Version 1.1 in early calendar year 2018.

National Law Review, Volume VII, Number 342

Source URL:https://natlawreview.com/article/nist-releases-updated-draft-cybersecurity-framework