wiley

NEWSLETTER

NIST Releases Draft 2 of Its Cybersecurity Framework Version 1.1

December 2017

On December 5, 2017, the National Institute of Standards and Technology (NIST) released the much-anticipated second draft of its Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (Framework Version 1.1 Draft 2 or Draft 2), along with a draft companion Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1 (Roadmap) and a Fact Sheet detailing its changes and process.

Draft 2 is intended to reflect the feedback that NIST received from stakeholders regarding Framework Version 1.1 Draft 1 (Draft 1), which was originally released in January 2017. The new Draft 2 makes significant changes to the section on cybersecurity measurements, in line with stakeholder feedback. Public comments on Framework Version 1.1 Draft 2 are due January 19, 2018. NIST intends to publish the final Framework Version 1.1 in early 2018.

NIST originally published the Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 (Framework Version 1.0) in February 2014. As NIST describes, the Framework is voluntary guidance for critical infrastructure organizations. It is based on existing standards, guidelines, and practices, and intends to help organizations to better manage and reduce cybersecurity risk and to foster risk and cybersecurity management communications.
The Framework Version 1.1 is meant to refine, clarify, and enhance the Framework Version 1.0. With this update, NIST is striving to cause as little disruption to implementation of the Framework as possible – meaning that current users of the Framework Version 1.0 should be able to easily implement Framework Version 1.1.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Madeleine M. Lottenbach
Associate
202.719.4193
mlottenbach@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

Key Updates

Draft 2 makes several key updates to Draft 1, including:

- Cybersecurity Measurements: NIST revises its new section on cybersecurity measurements significantly. It truncates the discussion, cutting it from four pages in Draft 1 to just over one page in Draft 2. It also changes the title of the section from "Measuring and Demonstrating Cybersecurity" to "Self-Assessing Cybersecurity Risk with the Framework" and emphasizes that self-assessments are linked to organizational objectives, highlighting flexibility and customization.
- Supply Chain Risk Management: NIST refines its addition of Supply Chain Risk Management (SCRM) from Draft 1, clarifying the section on communicating risks with stakeholders and incorporating that information into the Implementation Tiers.
- Authorization, Authentication, and Identity Proofing: NIST adds a new authentication subcategory and provides a number of authentication Informative References. Draft 2 further highlights authentication in the document, adding a reference to authentication in the Privacy and Civil Liberties section.
- Coordinated Vulnerability Disclosures: NIST adds a new subcategory regarding internal and external vulnerability disclosure programs. It also provides a number of vulnerability disclosure Informative References.
- Federal Alignment: Draft 1 had added a section detailing requirements of federal information systems. However, NIST removes that section in Draft 2, explaining that such statements are covered by other documents – including NISTIR 8170 – and therefore are not needed in the Framework.
- Application to the Internet of Things: NIST updates the scope of technologies covered by the Framework to "reflect security implications of a broadening use of technology." Draft 2 notes that members of each critical infrastructure sector perform functions supported by broad categories of technology, "including information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT)." While CPS was added in Draft 1, the application to IoT devices in Draft 2 is new.

"Roadmap" Updates

In addition to the updates to the Framework Version 1.1, NIST also published a draft update to the Framework's companion Roadmap. NIST first published a companion Framework Version 1.0 Roadmap in 2014. Like that document, the newly published draft "provides a description of anticipated future activities related to the Framework and offers stakeholders another opportunity to participate actively in the continuing Framework development process." Updates to the Roadmap for Version 1.1 include:

- Cyber-Attack Lifecycle
- Measuring Cybersecurity
- Referencing Techniques
- Small Business Awareness and Resources

- Governance and Enterprise Risk Management

NIST also has renamed several sections in the new Roadmap draft:

- “Authentication” has been renamed to be “Identity Management” to cover a broader range of technical topics.
- “Technical Privacy Standards” has been renamed to be “Privacy Engineering,” in line with NIST’s related Interagency Report 8062 – An Introduction to Privacy Engineering and Risk Management in Federal Systems.
- “Conformance Assessment” has been renamed to be “Confidence Mechanisms” to show a broader range of digital trust activities.