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

NIST Holds Webcast to Discuss Updates to Cybersecurity Framework

Article By:

Susan B. Cassidy

Moriah Daugherty

On December 20, 2017, the National Institute of Standards and Technology ("NIST") held a live webcast to discuss the draft updates to the Framework for Improving Critical Infrastructure Cybersecurity ("the Cybersecurity Framework") and the Roadmap for Improving Critical Infrastructure Cybersecurity ("the Roadmap"). Although the webcast is not currently available online, NIST plans to publish a recording of the live webcast in early January 2018.

During this webcast, NIST provided an overview of the updates to Version 1.1 of the Cybersecurity Framework ("Version 1.1"), which were analyzed in previous blog posts on Inside Privacy and Inside Government Contracts. The webcast included a discussion of the following topics:

Version 1.1 Reflects Significant Industry Feedback. NIST emphasized that in creating Version 1.1 that it considered feedback from industry including over 120 comments on the January 2017 draft and information gained from discussions among more than 500 participants at a May 2017 Workshop. NIST also noted that industry was seeking only minimal changes and wanted this version to be compatible with Version 1.0.

Version 1.1 Is Designed to Be Compatible with Version 1.0. Version 1.1 is designed to be compatible with Version 1.0, and additions—including new categories and subcategories—will not invalidate existing Version 1.0 work products.

The Cybersecurity Framework is Broadly Applicable. During the webcast, NIST noted that although the Cybersecurity Framework was always intended to be applicable to a wide-range of technology, Version 1.1 explicitly states that the Cybersecurity Framework is applicable to a wide range of technologies, including Information Technology ("IT"), Operational Technology ("OT"), Cyber-Physical Systems ("CPS") and the Internet of Things ("IoT"), as well as all phases of the system lifecycle.

In particular, NIST addressed Version 1.1's increased focus on supply chain risk management ("SCRM") and noted that Version 1.1's guidance was explicitly designed to align with NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and*

Organizations.

The Major Changes to Version 1.1. The primary changes to the Framework highlighted by NIST included: increased guidance for conducting self-assessments; enhanced explanation of how the Cybersecurity Framework can be applied to manage cybersecurity risks within supply chains and in acquisition decisions; language describing categories was refined to better account for authentication, authorization, and identity proofing; and a discussion of the revised integrated risk management implementation tiers.

Edits to the Roadmap Version 1.1. Roadmap Version 1.1 has also been edited and broadened in connection with the updates to the Cybersecurity Framework. In particular, NIST addressed the three new topics added to the Roadmap: Coordinated Vulnerability Disclosure, Governance and Enterprise Risk Management and Measuring Cybersecurity.

NIST is soliciting feedback on the draft Cybersecurity Framework and Roadmap Version 1.1 at cyberframework@nist.gov until January 19, 2017. NIST expects to issue final versions of the draft Cybersecurity Framework and Roadmap Version 1.1 in early 2018. Also in 2018, NIST expects to host a workshop to: share and understand use and best practices of the Cybersecurity Framework; determine early usage and utility of the Cybersecurity Framework and Roadmap Version 1.1; and engage in collaborative discussions related to Roadmap Version 1.1 topic areas.

National Law Review, Volume VII, Number 354