

# Fact Sheet

---

## December 2017 Proposed Update to Cybersecurity Framework

### Background

On December 5, 2017 NIST published the second draft of the proposed update to the Framework for Improving Critical Infrastructure Cybersecurity (a.k.a., draft 2 of Cybersecurity Framework version 1.1). This second draft update aims to clarify, refine, and enhance the Cybersecurity Framework, amplifying its value and making it easier to use. The new draft **reflects comments** received to date, including those from a public review process launched in January 2017 and a workshop in May 2017.

### Summary of Document Updates

Like Version 1.0 issued in February 2014, the proposed updates are the result of extensive consultation with the private and public sectors. This draft is intended to provide **a flexible, voluntary, and effective tool to help organizations better manage their cybersecurity risks**. Like the earlier proposed update, this draft is **fully compatible with Version 1.0** and can be used as the basis for communication between organizations. The update:

- Declares applicability of Cybersecurity Framework for "technology," which is minimally composed of Information Technology, operational technology, cyber-physical systems, and Internet of Things;
- Enhances guidance for applying the Cybersecurity Framework to supply chain risk management;
- Summarizes the relevance and utility of Cybersecurity Framework measurement for organizational self-assessment;
- Better accounts for authorization, authentication, and identity proofing; and
- Administratively updates the Informative References.

NIST also issued a proposed update to the Roadmap for Improving Critical Infrastructure Cybersecurity. This document is informed by public comments and **reflects ongoing and planned work relating to the Cybersecurity Framework and cybersecurity risk management more broadly**. The Roadmap:

- Describes future activities related to the Cybersecurity Framework and offers stakeholders another opportunity to participate actively in the continuing Cybersecurity Framework development process.
- Includes new topics of focus since the initial Roadmap version, including: the cyber-attack lifecycle, measuring cybersecurity, governance and enterprise risk management, referencing techniques for informative references, and small businesses awareness and resources.

### Public Comment Period

Public comments for draft 2 of Cybersecurity Framework version 1.1 and the draft Roadmap are due to NIST by 11:59PM on Friday, January 19, 2018 via [cyberframework@nist.gov](mailto:cyberframework@nist.gov). NIST anticipates finalizing Cybersecurity Framework version 1.1 in the Spring of 2018.