Public Draft: The NIST Cybersecurity Framework 2.0

National Institute of Standards and Technology

Released August 8, 2023

Note to Reviewers

This is the public draft of the NIST Cybersecurity Framework (CSF or Framework) 2.0.

The Framework has been used widely to reduce cybersecurity risks since its initial publication in 2014. Many organizations have told NIST that CSF 1.1 remains an effective framework for addressing cybersecurity risks. There is also widespread agreement that changes are warranted to address current and future cybersecurity challenges and to make it easier for organizations to use the Framework. NIST is working with the community to ensure that CSF 2.0 is effective for the future while fulfilling the CSF's original goals and objectives.

NIST seeks feedback on whether this draft revision addresses organizations' current and anticipated future cybersecurity challenges, is aligned with leading practices and guidance resources, and reflects comments received so far. In addition, NIST requests ideas on the best way to present the modifications from CSF 1.1 to CSF 2.0 to support transition. NIST encourages concrete suggestions for improvements to the draft, including revisions to the narrative and Core.

This draft includes an updated version of the CSF Core, reflecting feedback on the April discussion draft. This publication does not contain Implementation Examples or Informative References of the CSF 2.0 Core, given the need to frequently update them. Draft, initial Implementation Examples have been released under separate cover for public comment. NIST seeks feedback on what types of Examples would be most beneficial to Framework users, as well as what existing sources of implementation guidance might be readily adopted as sources of Examples (such as the NICE Framework Tasks, for example). NIST also seeks feedback on how often Implementation Examples should be updated and whether and how to accept Implementation Examples developed by the community.

As the CSF 2.0 is finalized, the updated Implementation Examples and Informative References will be maintained online on the NIST Cybersecurity Framework website, leveraging the NIST Cybersecurity and Privacy Reference Tool (CPRT). Resource owners and authors who are interested in mapping their resources to the final CSF 2.0 to create Informative References should reach out to NIST.

Feedback on this CSF 2.0 Public Draft, as well as the related Implementation Examples draft, may be submitted to cyberframework@nist.gov by Friday, November 4, 2023.

All relevant comments, including attachments and other supporting material, will be made publicly available on the NIST CSF 2.0 website. Personal, sensitive, confidential, or promotional business information should not be included. Comments with inappropriate language will not be considered.

This draft will be discussed at the third CSF workshop, which will be held this fall. **NIST does not plan to release another draft of CSF 2.0 for comment. Feedback on this draft will inform development of the final CSF 2.0 to be published in early 2024.**

NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE