Journey to the NIST Cybersecurity Framework 2.0

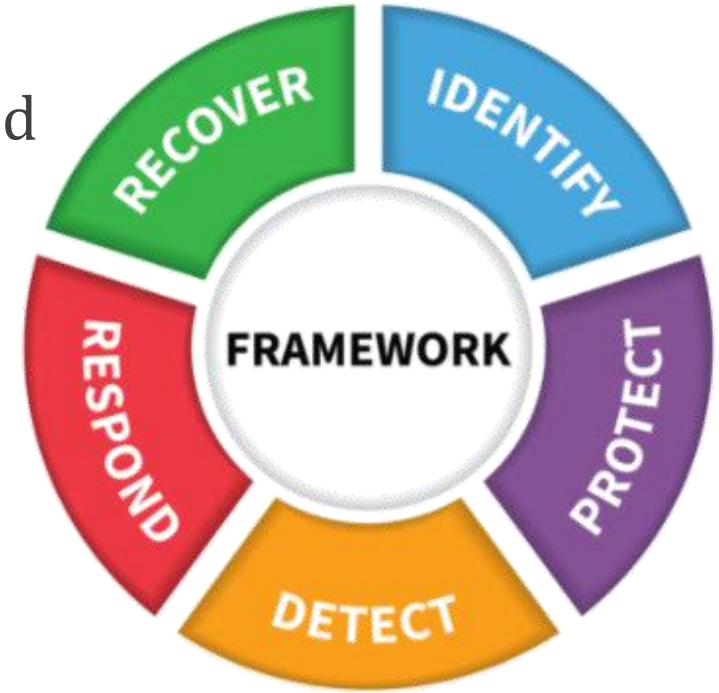
Cherilyn Pascoe
Senior Tech Policy Advisor & Lead, NIST CSF Program
February 28, 2023

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

Cybersecurity Framework Attributes

The NIST Cybersecurity Framework (CSF) helps organizations reduce their cybersecurity risks and is widely recognized as foundational to securing organizations & technology.

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Guided by many perspectives – private sector, academia, public sector
- Align legal/regulatory requirements and organizational and risk management priorities



A Look Back at CSF History

- February 2013 | Executive Order 13636: Improving Critical Infrastructure Cybersecurity
- **February 2014 | CSF 1.0**
- December 2014 | Cybersecurity Enhancement Act of 2014 (P.L. 113-274)
- May 2017 | Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (CSF required for federal agencies)
- **April 2018 | CSF. 1.1**
- April 2022 | NIST RFI on CSF Update Closed
- **Future | CSF 2.0**

CSF Update | Journey to CSF 2.0

- **NIST has begun the process of updating the CSF.** The update will address the evolving cybersecurity risk and standards landscape and make it easier for organizations to address risks. NIST is actively relying on and seeking diverse stakeholder feedback in the update process.

Ways to engage: www.nist.gov/cyberframework

CSF 2.0 Concept Paper: Changes

Potential Significant Changes in CSF 2.0

NIST seeks feedback on each of the approaches described below.

1. CSF 2.0 will explicitly recognize the CSF's broad use to clarify its potential applications
2. CSF 2.0 will remain a framework, providing context and connections to existing standards and resources
3. CSF 2.0 (and companion resources) will include updated and expanded guidance on Framework implementation
4. CSF 2.0 will emphasize the importance of cybersecurity governance
5. CSF 2.0 will emphasize the importance of cybersecurity supply chain risk management (C-SCRM)
6. CSF 2.0 will advance understanding of cybersecurity measurement and assessment

Please submit feedback by 3/3 to cyberframework@nist.gov.
The Concept Paper was discussed at Workshop #2 (2/15) and the in-person Working Sessions (2/22 & 2/23).

Concept Paper: Calls to Action

Ways in which the community can contribute to improvements to CSF 2.0 and associated resources.

- ❑ Share International Resources
- ❑ Provide Mappings
- ❑ Share Example Profiles
- ❑ Submit CSF Resources
- ❑ Share Success Stories
- ❑ Share Use of the CSF in Measuring and Assessing Cybersecurity
- ❑ Comment on Performance Measurement Guide for Information Security

CSF 2.0 Next Steps

NIST will rely on significant feedback to inform the update

- Public workshops and events –
  - Recently held **Journey to CSF 2.0 Workshop #2** (*virtual)* on February 15, 2023, and **Journey to CSF 2.0 Working Sessions** *(in-person)* February 22-23, 2023
  - Stay tuned for a workshop this Fall!
- Comment on drafts –
  - Comment on **CSF 2.0 Concept Paper** by 3/3/2023 via cyberframework@nist.gov
  - Stay tuned for CSF 2.0 draft this summer
- Continuing to seek and develop CSF resources, success stories, mappings to other frameworks and standards

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

STAY IN TOUCH

CONTACT US


NIST.gov


@NISTcyber