


NIST Cybersecurity Framework 2.0

An abstract graphic representing a network or data flow. It features a complex web of interconnected nodes and lines. The nodes are represented by small circles in various colors (blue, green, yellow, orange) and are connected by thin, glowing lines. The background is a dark blue gradient with subtle, wavy patterns and a soft glow emanating from the center of the network.

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.

- Risk-based cybersecurity outcomes – the “what”, not “how” or “who”
- Review priorities and gaps; align legal/regulatory requirements and organizational and risk management priorities
- Common and accessible language
- Connected to and based on international standards
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Guided by many perspectives – private sector, academia, public sector



Governmental Policies on CSF

Adapted in several countries and regions

- United States (federal and state)
- **The White House National Cybersecurity Strategy (March 2023): <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>**
 - “Regulations should be performance-based, leverage existing cybersecurity frameworks, voluntary consensus standards, and guidance – including the Cybersecurity and Infrastructure Security Agency (CISA)’s Cybersecurity Performance Goals and the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity – ...”
- Italy
- Poland
- Israel
- Japan
- Uruguay
- And more



Examples highlighted on the NIST International Cybersecurity and Privacy Resource Site:
<https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources>

A Look Back at CSF History

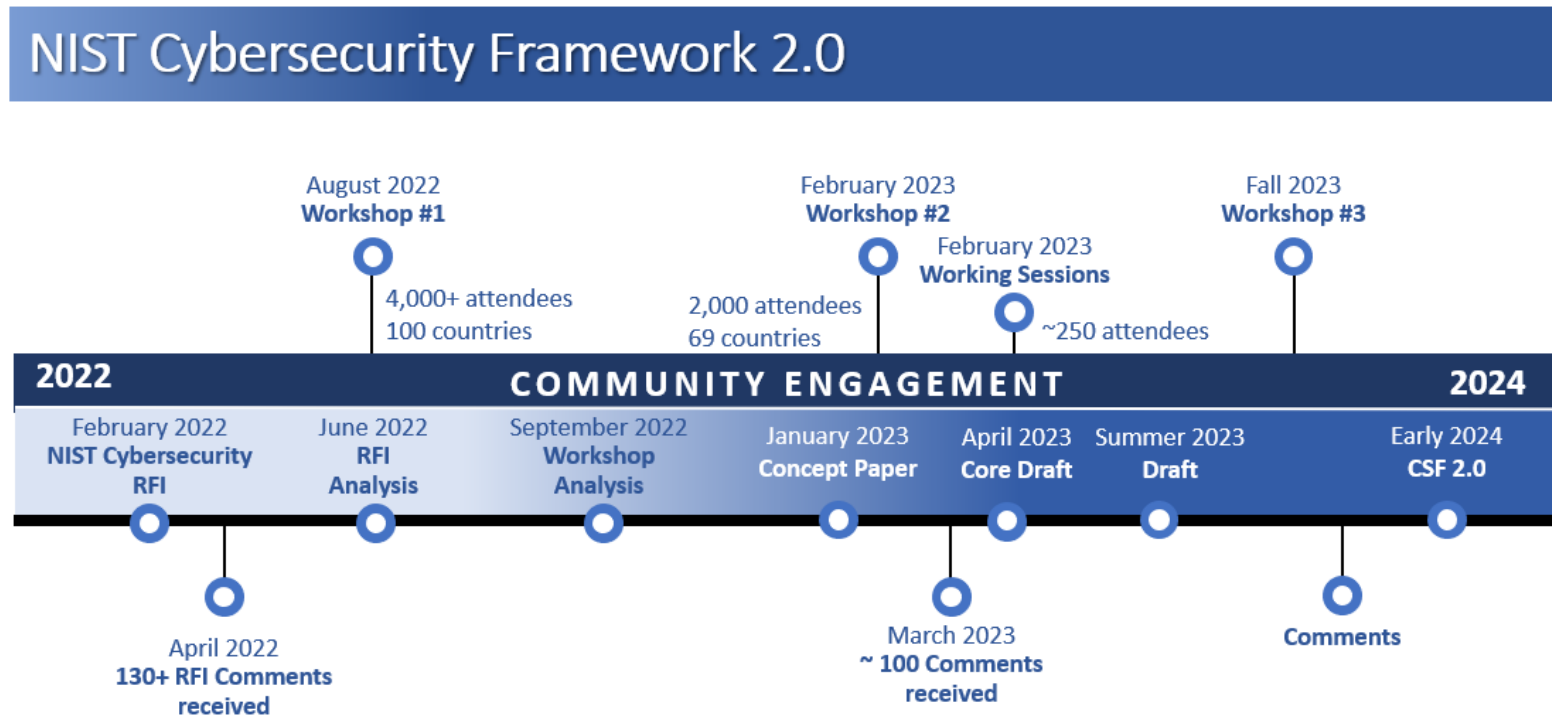
- February 2013 | Executive Order 13636: Improving Critical Infrastructure Cybersecurity
- **February 2014 | CSF 1.0**
- December 2014 | Cybersecurity Enhancement Act of 2014 (P.L. 113-274)
- May 2017 | Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (CSF required for federal agencies)
- **April 2018 | CSF. 1.1**
- April 2022 | NIST RFI on CSF Update Closed
- **Early 2024 | 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 community engagement to build CSF 2.0.



Ways to engage: www.nist.gov/cyberframework

Potential Significant Changes in CSF 2.0

The NIST CSF 2.0 Concept Paper outlines the goals of NIST CSF 2.0:

1. Explicitly recognize the CSF's broad use to clarify its potential applications
2. Remain a framework, providing context and connections to existing standards and resources
3. Include updated and expanded guidance on Framework implementation
4. Emphasize the importance of cybersecurity governance
5. Emphasize the importance of cybersecurity supply chain risk management (C-SCRM)
6. Advance understanding of cybersecurity measurement and assessment

All comments received to the Concept Paper are available on the CSF website.

The Concept Paper was discussed at Workshop #2 (2/15) and the in-person Working Sessions (2/22 & 2/23).

Increases focus on:

- Cybersecurity outcomes applicable to all organizations
- Cybersecurity governance
- Cybersecurity supply chain risk management
- Continuous improvement of cybersecurity risk management
- Leveraging people, process, and technology
- Resilience of security architecture
- Cybersecurity incident response management



CSF 2.0 Discussion Draft Revised Core



NIST Cybersecurity Framework 2.0		
Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

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

NIST is relying on feedback to inform the update

- **Public workshops and events**

- Stay tuned for the third and final CSF 2.0 Workshop this Fall!
- Find recordings of CSF Workshop #1 (August 2022) and #2 (February 2023) online.



- **Comment on drafts**

- Provide comments on the CSF 2.0 Discussion Core.
- Look for CSF 2.0 draft this summer!
- All comments received on the NIST RFI and the CSF 2.0 Concept Paper can be found online.

- **Continuing to seek and develop CSF resources, success stories, and mappings to other frameworks and standards.**

Contact information: cyberframework@nist.gov | **Ways to engage:**
www.nist.gov/cyberframework