

# Journey to the NIST Cybersecurity Framework 2.0: Workshop #2

**Cherilyn Pascoe**

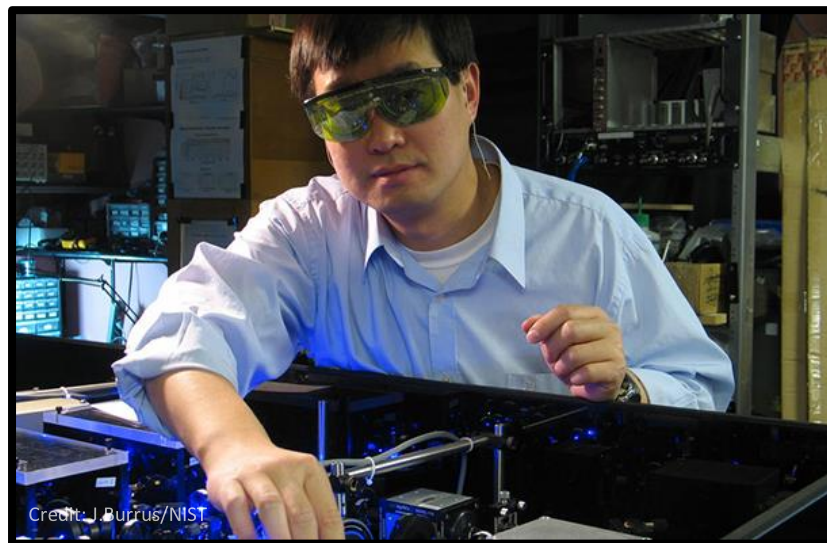
Senior Tech Policy Advisor & Lead, NIST CSF Program

**February 15, 2023**

# NIST's Mission



To promote U.S. innovation and industrial competitiveness by advancing **measurement science, standards,** and **technology** in ways that enhance economic security and improve our quality of life



# Celebrating 50 Years

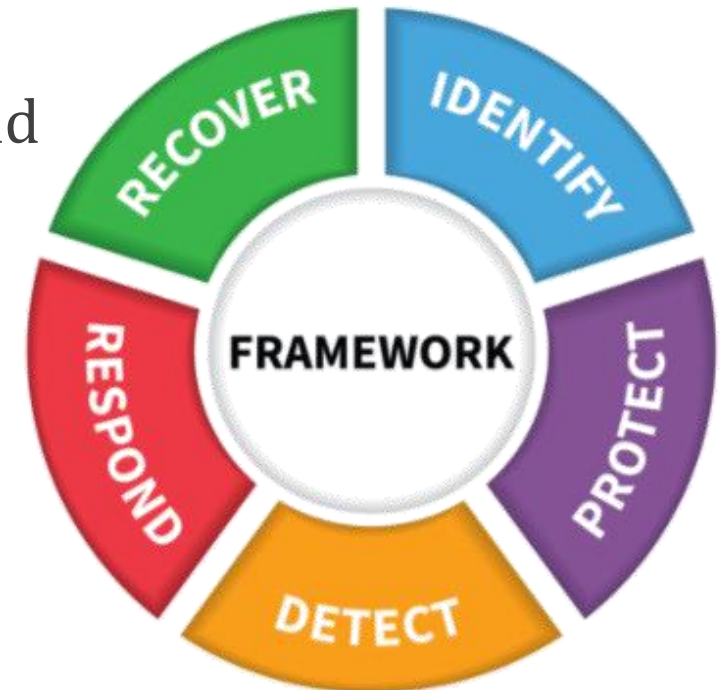


The year 2022 marked **50 years** of NIST's cybersecurity research and the development of cybersecurity and privacy guidance.

Our work has helped better secure the state of technology that exists today—while providing the platform for the secure technology development of tomorrow.

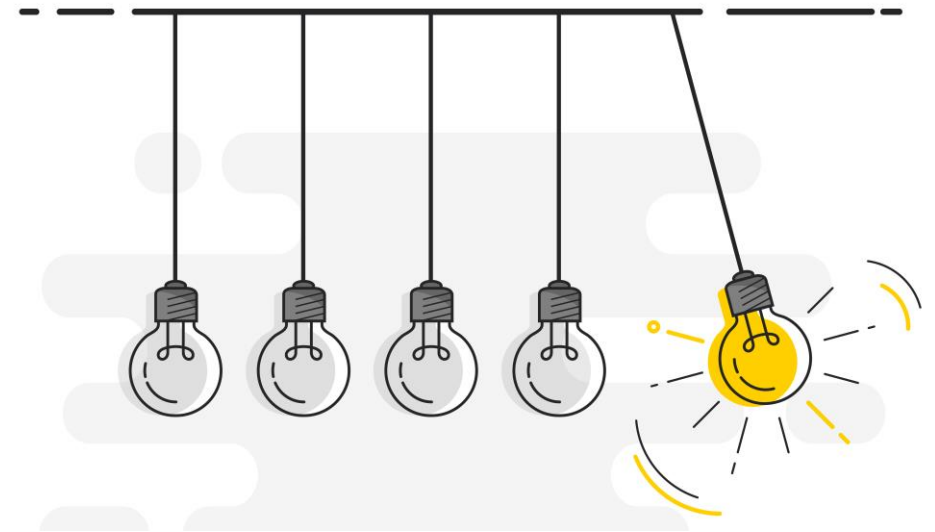
**The NIST Cybersecurity Framework (CSF) helps organizations reduce their cybersecurity risks and is widely recognized as foundational to securing organizations & technology.**

- 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



# CSF Indicators

- ~2 million total downloads
- 18,500+ attendees at workshops & webinars
- 800+ responses/comments from the public
- 14 sample CSF Profiles and dozens of resources, success stories
- 9 translations (Spanish, Japanese, Portuguese, Arabic, Bulgarian, Polish, Indonesian, French, Ukrainian)



Helping organizations to better understand and improve their management of cybersecurity risk since 2013.

# Innovative Uses of the CSF



Photo credit: Cheri Pascoe at ChiBrrCon



Photo credit: @\_davewm\_ via Twitter



Photo credit: @jamiemasello via Twitter

# 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](https://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](mailto:cyberframework@nist.gov).

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

## 1. CSF 2.0 will explicitly recognize the CSF's broad use to clarify its potential applications

- 1.1. Change the CSF's title and text to reflect its intended use by all organizations
- 1.2. Scope the CSF to ensure it benefits organizations regardless of sector, type, or size
- 1.3. Increase international collaboration and engagement



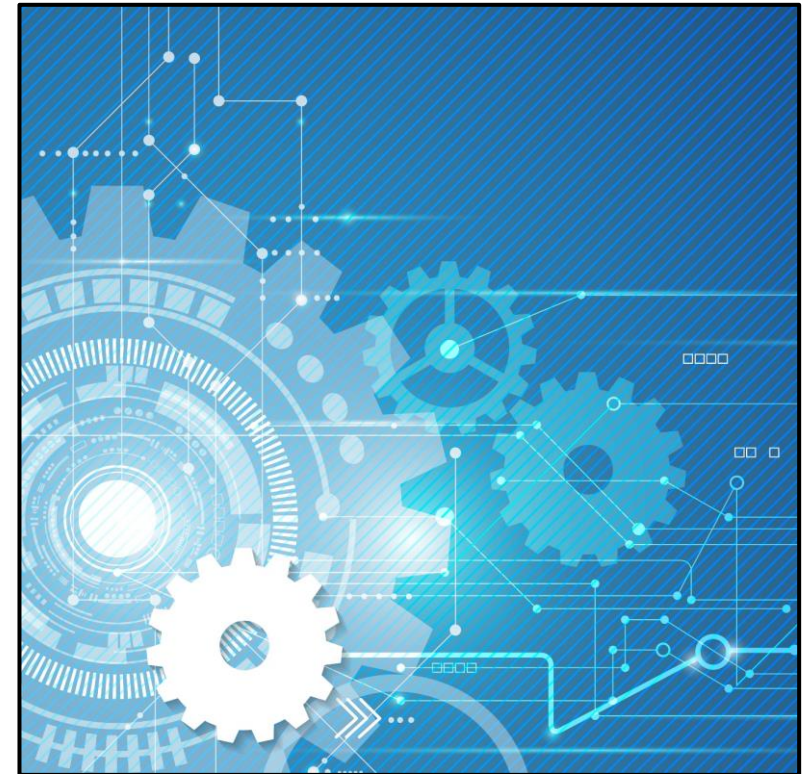
# Update on CSF International

- Downloaded to over 185 countries.
- 9 Translations: Spanish, Japanese, Portuguese, Arabic, Bulgarian, Polish, Indonesian, French, Ukrainian.
- Adapted into national cybersecurity policies, strategies, and requirements.
- Use cases identified in all regions.



## 2. CSF 2.0 will remain a framework, providing context and connections to existing standards and resources

- 2.1. Retain CSF's current level of detail
- 2.2. Relate the CSF clearly to other NIST frameworks
- 2.3. Leverage Cybersecurity and Privacy Reference Tool for online CSF 2.0 Core
- 2.4. Use updatable, online Informative References
- 2.5. Use Informative References to provide more guidance to implement the CSF
- 2.6. Remain technology- and vendor-neutral, but reflect changes in cybersecurity practices
















# CSF Mappings (OLIR & CPRT)



## PROTECT (PR)

Develop and implement appropriate safeguards to ensure delivery of critical services.

Category	Subcategory	Reference Items	OLIR Relationships 
<b>Data Security (PR.DS):</b> Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	<b>PR.DS-1:</b> Data-at-rest is protected	CISCSC: 13, 14 COBIT 5: APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 ISA 62443-3-3:2013: SR 3.4, SR 4.1 ISO/IEC 27001:2013: A.8.2.3 NIST SP 800-53 Rev. 4: <a href="#">MP-8</a> , <a href="#">SC-12</a> , <a href="#">SC-28</a>	<b>800-171 Rev 1 to PR.DS-1</b> <ul style="list-style-type: none"><li>• PR.DS-1  3.1.19</li><li>• PR.DS-1  3.13.10</li><li>• PR.DS-1  3.13.16</li><li>• PR.DS-1  3.8.1</li><li>• PR.DS-1  3.8.9</li></ul>
			<b>800-53 Rev 4 to PR.DS-1</b> <ul style="list-style-type: none"><li>• PR.DS-1  MP-8</li><li>• PR.DS-1  SC-12</li><li>• PR.DS-1  SC-28</li></ul>
			<b>800-53 Rev 5 to PR.DS-1</b> <ul style="list-style-type: none"><li>• PR.DS-1  MP-2</li><li>• PR.DS-1  MP-3</li><li>• PR.DS-1  SC-28</li><li>• PR.DS-1  MP-4</li></ul>

National Online Informative References Program (OLIR): <https://csrc.nist.gov/projects/olir>  
Cybersecurity & Privacy Reference Tool (CPRT): <https://csrc.nist.gov/projects/cprt>

## 3. CSF 2.0 (and companion resources) will include updated and expanded guidance on Framework implementation

- 3.1. Add implementation examples for CSF Subcategories
- 3.2. Develop a CSF Profile template
- 3.3. Improve the CSF website to highlight implementation resources



NIST Special Publication 1271

<https://doi.org/10.6028/NIST.SP.1271>

August 2021

## Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide

Amy Mahn<sup>1</sup>, Jeffrey Marron<sup>1</sup>, Stephen Quinn<sup>2</sup>, Daniel Topper<sup>3</sup>

<sup>1</sup> NIST Applied Cybersecurity Division, Information Technology Laboratory

<sup>2</sup> NIST Computer Security Division, Information Technology Laboratory

<sup>3</sup> Huntington Ingalls Industries



### What is the NIST Cybersecurity Framework, and how can my organization use it?

The [NIST Cybersecurity Framework](#)<sup>4</sup> can help an organization begin or improve their cybersecurity program. Built off of practices that are known to be effective, it can help organizations improve their cybersecurity posture. It fosters communication among both internal and external stakeholders about cybersecurity, and for larger organizations, helps to better integrate and align cybersecurity risk management with broader enterprise risk management processes as described in the [NISTIR 8286](#)<sup>5</sup> series.

The Framework is organized by five key Functions—Identify, Protect, Detect, Respond, Recover. These five widely understood terms, when considered together, provide a comprehensive view of the lifecycle for managing cybersecurity risk over time. The activities listed under each Function may offer a good starting point for your organization:



#### IDENTIFY

*Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities.*

- **Identify critical enterprise processes and assets** – What are your enterprise’s activities that absolutely must continue in order to be viable? For example, this could be maintaining a website to retrieve payments, protecting customer/patient information securely, or ensuring that the information your enterprise collects remains accessible and accurate.
- **Document information flows** – It’s important to not only understand what type of information your enterprise collects and uses, but also to understand where the data is located and how it is used, especially where contracts and external partners are engaged.
- **Maintain hardware and software inventory** – It’s important to have an understanding of the computers and software in your enterprise because these are frequently the entry points of malicious actors. This inventory could be as simple as a spreadsheet.
- **Establish policies for cybersecurity that include roles and responsibilities** – These policies and procedures should clearly describe your expectations for how cybersecurity activities will protect your information and systems, and how they support critical enterprise processes. Cybersecurity policies should be integrated with other enterprise risk considerations (e.g., financial, reputational).
- **Identify threats, vulnerabilities, and risk to assets** – Ensure risk management processes are established and managed to ensure internal and external threats are identified, assessed, and documented in risk registers. Ensure risk responses are identified and prioritized, executed, and results monitored.

<sup>4</sup> <https://www.nist.gov/cyberframework>

<sup>5</sup> <https://csrc.nist.gov/publications/detail/nistir/8286/final>



All resources on NIST CSF website:

[www.nist.gov/cyberframework](https://www.nist.gov/cyberframework)

CSF Quick Start Guide (NIST SP 1271):

[www.nist.gov/cyberframework/getting-started](https://www.nist.gov/cyberframework/getting-started)

## 4. CSF 2.0 will emphasize the importance of cybersecurity governance

- 4.1. Add a new Govern Function
- 4.2. Improve discussion of relationship to risk management





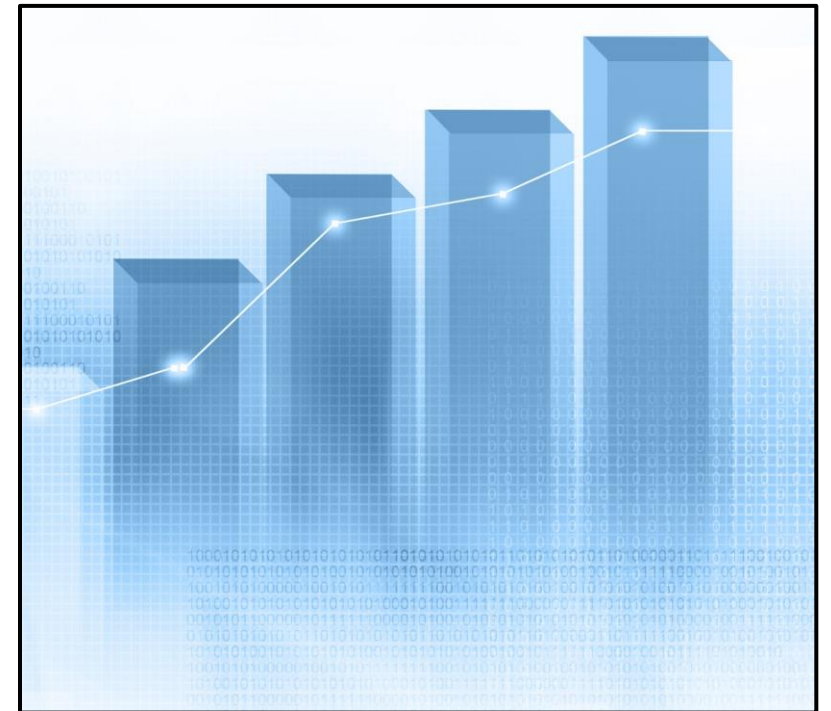
## 5. CSF 2.0 will emphasize the importance of cybersecurity supply chain risk management (C-SCRM)

### 5.1. Expand coverage of supply chain



## 6. CSF 2.0 will advance understanding of cybersecurity measurement and assessment

- 6.1. Clarify how leveraging the CSF can support the measurement and assessment of cybersecurity programs
- 6.2. Provide examples of measurement and assessment using the CSF
- 6.3. Update the NIST Performance Measurement Guide for Information Security
- 6.4. Provide additional guidance on Framework Implementation Tiers



## **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



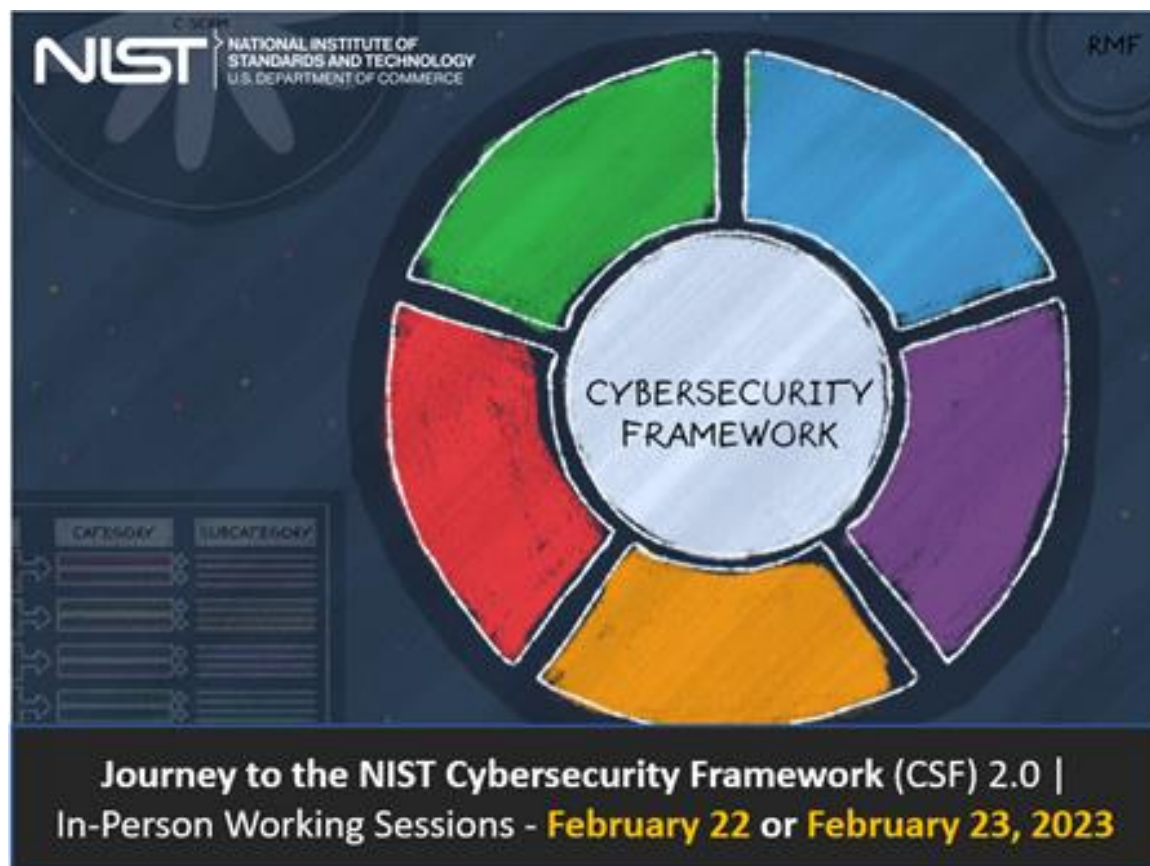
- Public workshops and events –
  - **Journey to CSF 2.0 Workshop #2** (*virtual*) today
  - **Journey to CSF 2.0 Working Sessions** (*in-person*) February 22-23, 2023, at NCCOE in Rockville, MD
  - Stay tuned for a workshop this Fall!
- Comment on drafts –
  - Comment on **CSF 2.0 Concept Paper** by 3/3/2023 via [cyberframework@nist.gov](mailto: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

Contact information: [cyberframework@nist.gov](mailto:cyberframework@nist.gov) | Ways to engage: [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)

# In-Person Working Sessions



Attendees should be familiar with the NIST Cybersecurity Framework (with hands-on implementation experience). Attendance at the [preceding virtual workshop](#) today is required to participate.



- Half day breakout sessions to discuss potential updates to the CSF at the NIST NCCoE in Rockville, MD
- Builds on today's *virtual* [CSF 2.0 Workshop #2](#), the [2022 NIST Request for Information \(RFI\)](#) and the [first CSF 2.0 workshop](#).

**Registration closes tonight:**

[www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-person-working-sessions](https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-person-working-sessions)

# STAY IN TOUCH

---

## CONTACT US



NIST.gov



@NISTcyber