# International Conference on the EU Cybersecurity Act

# Evaluating and Improving the NIST Cybersecurity Framework

**Cherilyn Pascoe**

Senior Tech Policy Advisor & Lead, NIST CSF Program

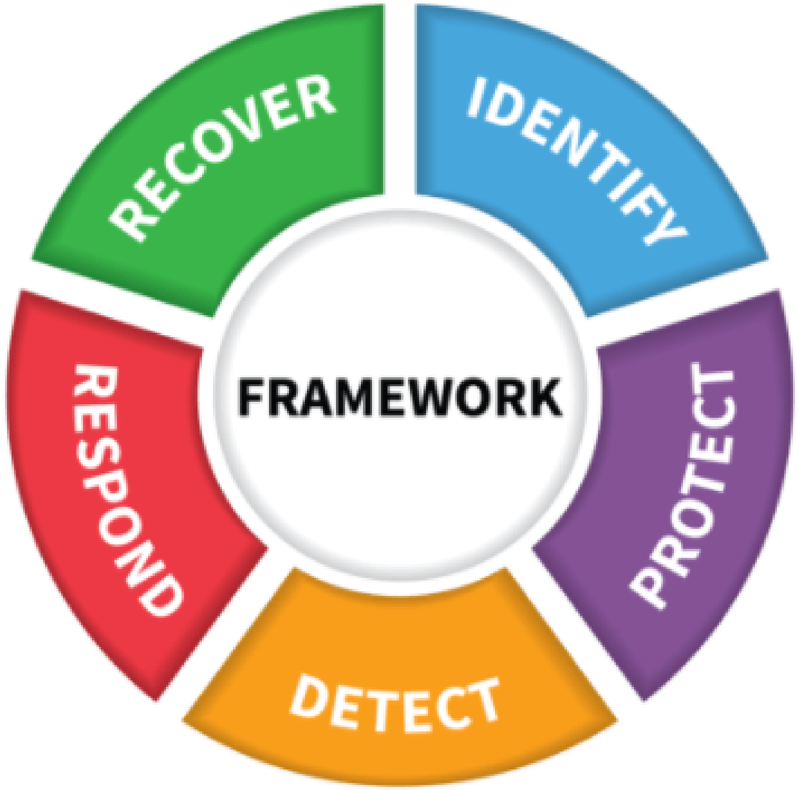
**March 29, 2023**

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

# Agenda

NIST

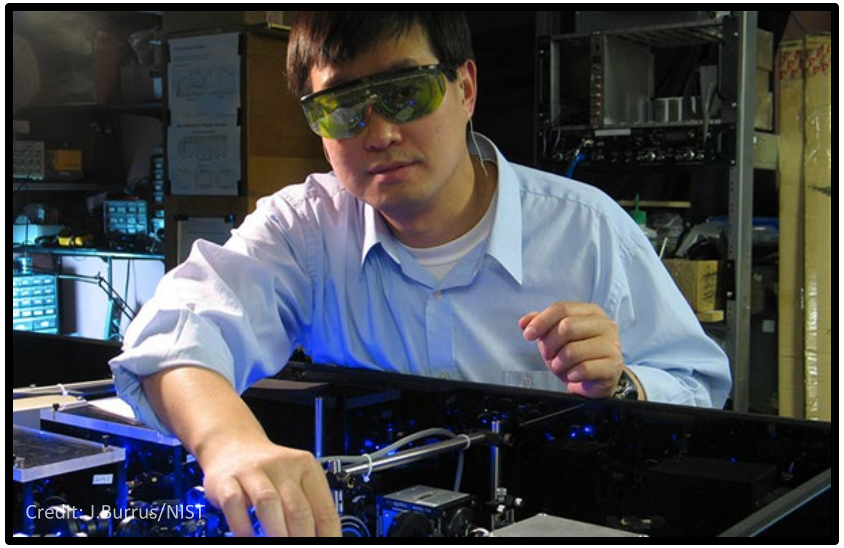
1. Cybersecurity Framework Overview
2. Cybersecurity Framework as Applied to Technology
3. CSF Update (Journey to 2.0)



# 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

©Robert Rathe

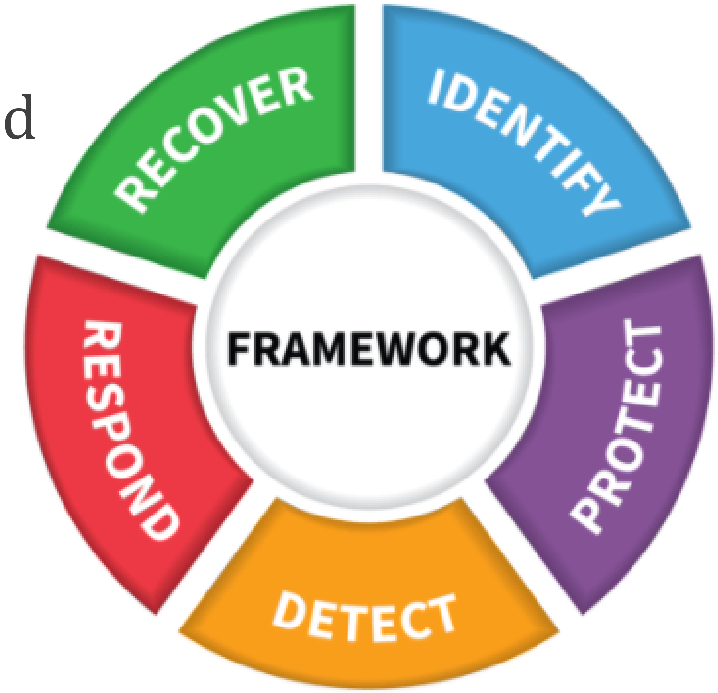

Credit: J.Burrus/NIST

©Nicholas McIntosh Photography

# Cybersecurity Framework

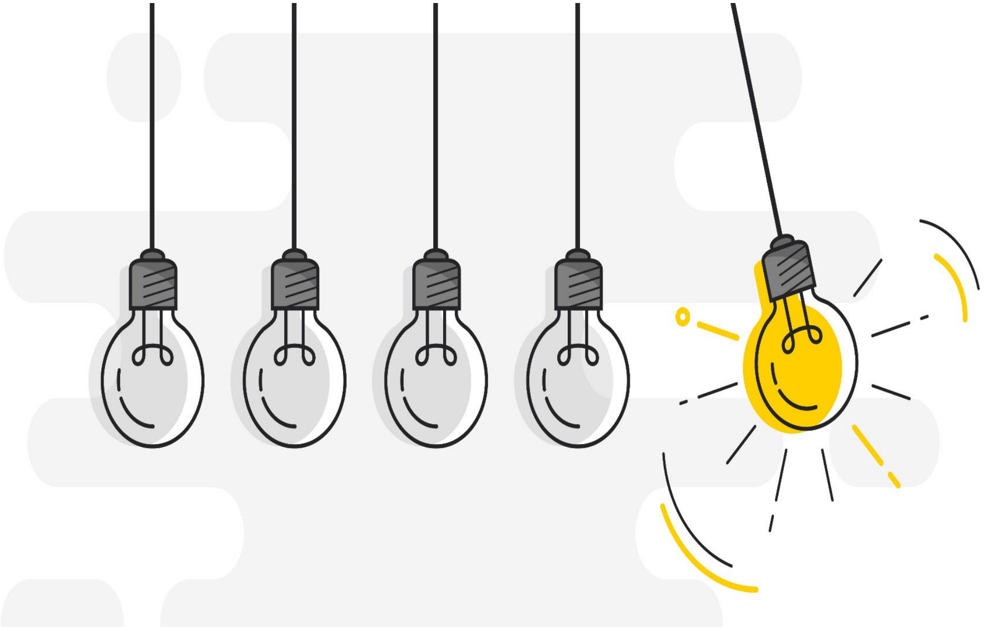
**The NIST Cybersecurity Framework (CSF) helps organizations reduce their cybersecurity risks and is widely recognized as foundational to securing organizations & technology.**

- 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 to over 185 countries.
- Built through community engagement:
  - 20,000+ attendees at workshops & webinars
  - 850+ responses/comments from the public
- 14 sample CSF Profiles and dozens of implementation resources
- 9 translations (Spanish, Japanese, Portuguese, Arabic, Bulgarian, Polish, Indonesian, French, Ukrainian)
- Adopted in organizational and government policies (at all levels) around the world.



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

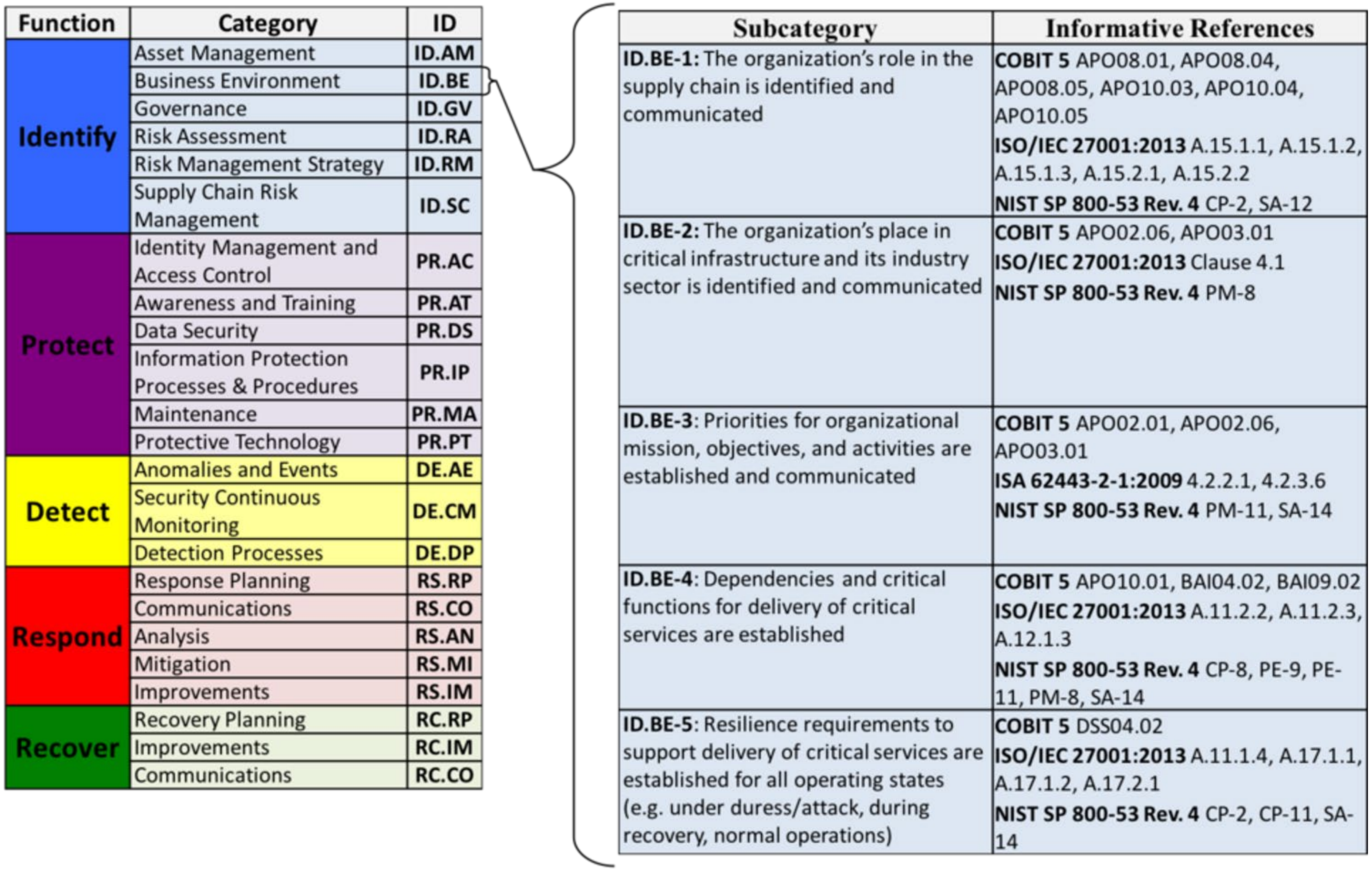
# Governmental Policies on CSF

## Adapted in several countries and regions

- United States (federal and state)
- Italy
- 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

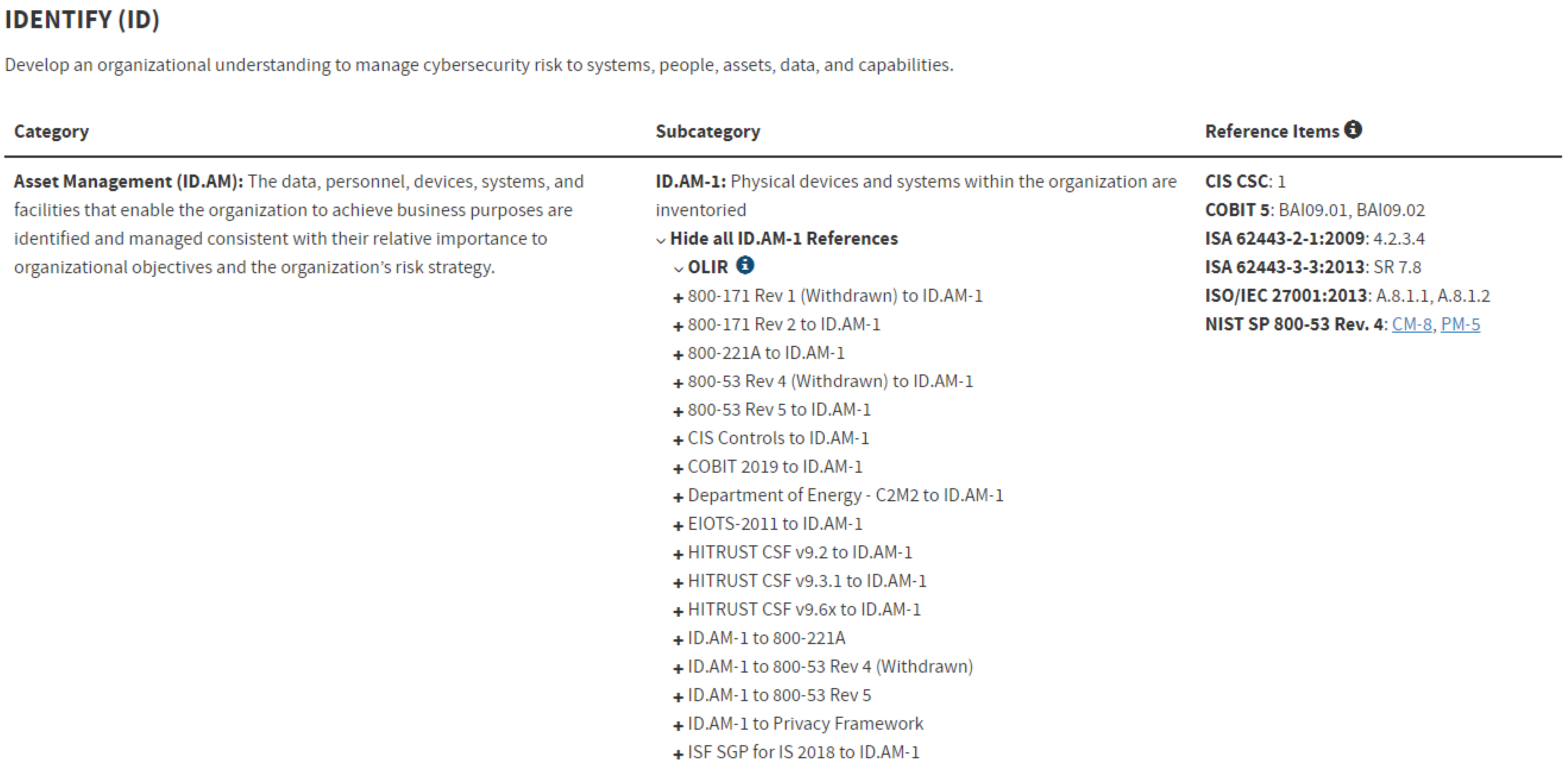
# CSF Core



| Function | Category | ID |
|---|---|---|
| Identify | Asset Management | ID.AM |
| | Business Environment | ID.BE |
| | Governance | ID.GV |
| | Risk Assessment | ID.RA |
| | Risk Management Strategy | ID.RM |
| | Supply Chain Risk Management | ID.SC |
| Protect | Identity Management and Access Control | PR.AC |
| | Awareness and Training | PR.AT |
| | Data Security | PR.DS |
| | Information Protection Processes & Procedures | PR.IP |
| | Maintenance | PR.MA |
| | Protective Technology | PR.PT |
| Detect | Anomalies and Events | DE.AE |
| | Security Continuous Monitoring | DE.CM |
| | Detection Processes | DE.DP |
| Respond | Response Planning | RS.RP |
| | Communications | RS.CO |
| | Analysis | RS.AN |
| | Mitigation | RS.MI |
| | Improvements | RS.IM |
| Recover | Recovery Planning | RC.RP |
| | Improvements | RC.IM |
| | Communications | RC.CO |

| Subcategory | Informative References |
|---|---|
| **ID.BE-1:** The organization's role in the supply chain is identified and communicated | **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05<br>**ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2<br>**NIST SP 800-53 Rev. 4** CP-2, SA-12 |
| **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated | **COBIT 5** APO02.06, APO03.01<br>**ISO/IEC 27001:2013** Clause 4.1<br>**NIST SP 800-53 Rev. 4** PM-8 |
| **ID.BE-3**: Priorities for organizational mission, objectives, and activities are established and communicated | **COBIT 5** APO02.01, APO02.06, APO03.01<br>**ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6<br>**NIST SP 800-53 Rev. 4** PM-11, SA-14 |
| **ID.BE-4**: Dependencies and critical functions for delivery of critical services are established | **COBIT 5** APO10.01, BAI04.02, BAI09.02<br>**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3<br>**NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14 |
| **ID.BE-5**: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) | **COBIT 5** DSS04.02<br>**ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1<br>**NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14 |

# CSF Mappings (OLIR & CPRT)



## IDENTIFY (ID)

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

| Category | Subcategory | Reference Items 🛈 |
|---|---|---|
| **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | **ID.AM-1:** Physical devices and systems within the organization are inventoried<br>⌄ **Hide all ID.AM-1 References**<br>⌄ **OLIR** 🛈<br>+ 800-171 Rev 1 (Withdrawn) to ID.AM-1<br>+ 800-171 Rev 2 to ID.AM-1<br>+ 800-221A to ID.AM-1<br>+ 800-53 Rev 4 (Withdrawn) to ID.AM-1<br>+ 800-53 Rev 5 to ID.AM-1<br>+ CIS Controls to ID.AM-1<br>+ COBIT 2019 to ID.AM-1<br>+ Department of Energy - C2M2 to ID.AM-1<br>+ EIOTS-2011 to ID.AM-1<br>+ HITRUST CSF v9.2 to ID.AM-1<br>+ HITRUST CSF v9.3.1 to ID.AM-1<br>+ HITRUST CSF v9.6x to ID.AM-1<br>+ ID.AM-1 to 800-221A<br>+ ID.AM-1 to 800-53 Rev 4 (Withdrawn)<br>+ ID.AM-1 to 800-53 Rev 5<br>+ ID.AM-1 to Privacy Framework<br>+ ISF SGP for IS 2018 to ID.AM-1 | **CIS CSC**: 1<br>**COBIT 5**: BAI09.01, BAI09.02<br>**ISA 62443-2-1:2009**: 4.2.3.4<br>**ISA 62443-3-3:2013**: SR 7.8<br>**ISO/IEC 27001:2013**: A.8.1.1, A.8.1.2<br>**NIST SP 800-53 Rev. 4**: CM-8, PM-5 |

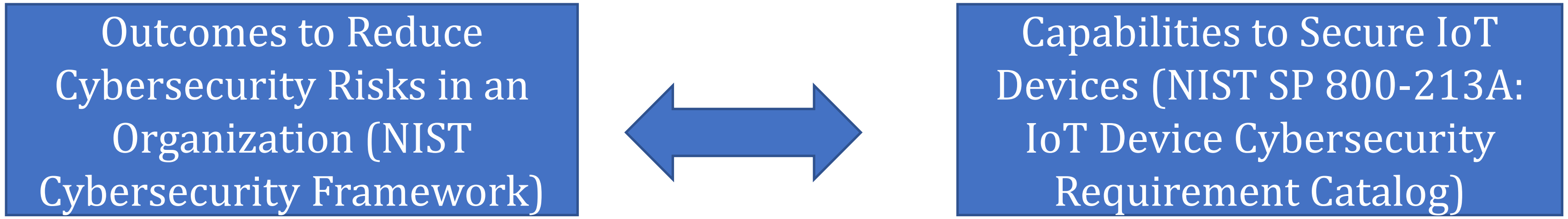
National Online Informative References Program (OLIR): https://csrc.nist.gov/projects/olir

Cybersecurity & Privacy Reference Tool (CPRT): https://csrc.nist.gov/projects/cprt

# Examples of Technology-Specific Mappings to the CSF

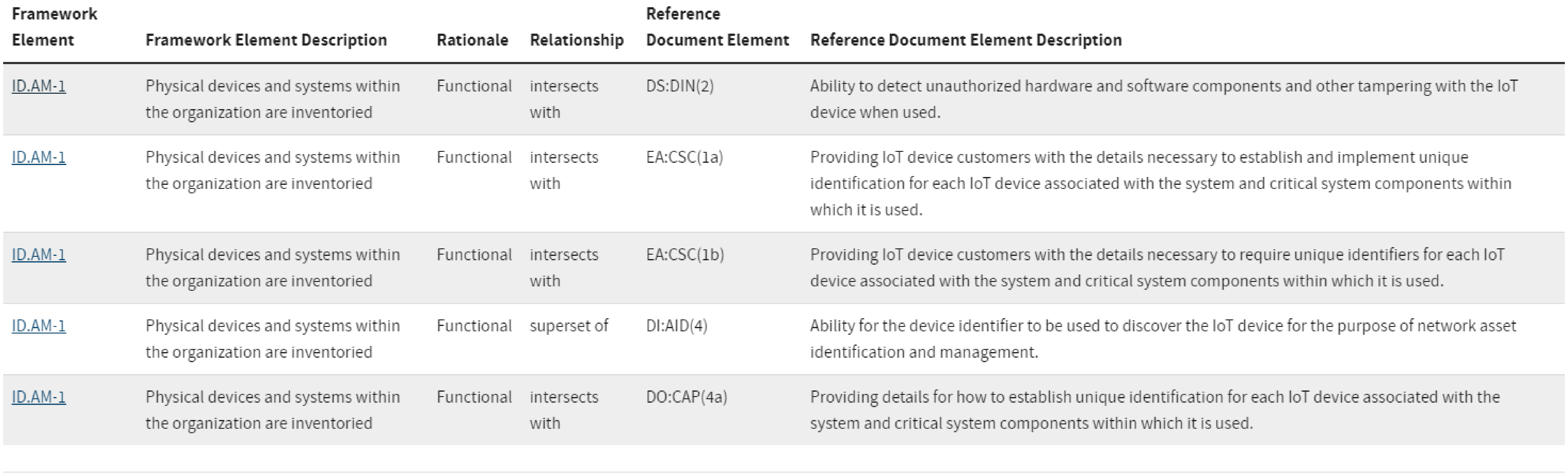
| Map security capabilities to the CSF outcomes | | | |
|---|---|---|---|
| **IoT Device Cybersecurity Requirement Catalog** | *Catalog of IoT device cybersecurity capabilities* | *NIST SP 800-213A* | Communicate how cybersecurity capabilities of an IoT product meet an organization's cybersecurity risk management effort |
| **Implementing a Zero Trust Architecture** | *End-to-end zero trust architecture implementations to help industry and government reduce the risk of cyber attack* | *SP 1800-35E: Risk and Compliance Management (preliminary draft)* | ZTA security functions can help support the outcome described in the CSF subcategories |
| **Supply Chain: Validating the Integrity of Computing Devices** | *Helping organizations verify that the internal components of the computing devices they acquire are genuine and have not been tampered with* | *SP 1800-34B: Section 3.5 Security Control Map (final)* | The security characteristics can assist organizations better manage supply chain risk as expressed in CSF subcategories |
| | | *SP 1800-34B: Section 3.6 Technologies (final)* | The specific products and services can help achieve the outcome described in the CSF subcategories |
| **Trusted IoT Device Network-Layer Onboarding and Lifecycle Management** | *Approaches to trusted network-layer onboarding of IoT devices and lifecycle management of the devices* | *Work in progress* | IoT on-boarding and security mechanisms security can help support the outcome described in the CSF subcategories |
| **5G Cybersecurity** | *Cybersecurity guidance to help consumers and operators of 5G networks securely adopt this technology as the development, deployment, and usage of 5G simultaneously evolves* | *Work in progress* | 5G protocols and underlying infrastructure security mechanisms can help support the outcome described in the CSF subcategories |
| **Migration to Post-Quantum Cryptography** | *Initiating the development of practices to ease migration from the current set of public-key cryptographic algorithms to replacement algorithms that are resistant to quantum computer-based attacks* | *Work in progress* | Practices followed in preparation and during the migration can help support the outcome described in the CSF subcategories |

# Examples of Secure Product Mappings to the CSF



Outcomes to Reduce Cybersecurity Risks in an Organization (NIST Cybersecurity Framework)

Capabilities to Secure IoT Devices (NIST SP 800-213A: IoT Device Cybersecurity Requirement Catalog)



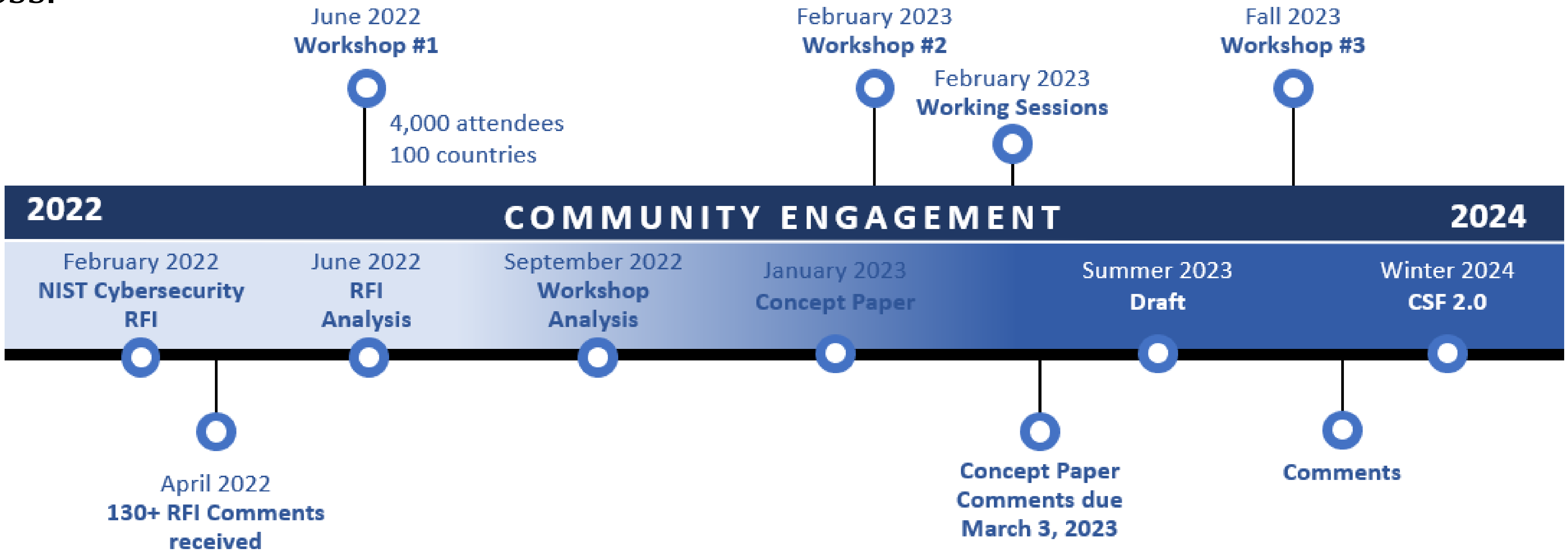
| Framework Element | Framework Element Description | Rationale | Relationship | Reference Document Element | Reference Document Element Description |
|---|---|---|---|---|---|
| ID.AM-1 | Physical devices and systems within the organization are inventoried | Functional | intersects with | DS:DIN(2) | Ability to detect unauthorized hardware and software components and other tampering with the IoT device when used. |
| ID.AM-1 | Physical devices and systems within the organization are inventoried | Functional | intersects with | EA:CSC(1a) | Providing IoT device customers with the details necessary to establish and implement unique identification for each IoT device associated with the system and critical system components within which it is used. |
| ID.AM-1 | Physical devices and systems within the organization are inventoried | Functional | intersects with | EA:CSC(1b) | Providing IoT device customers with the details necessary to require unique identifiers for each IoT device associated with the system and critical system components within which it is used. |
| ID.AM-1 | Physical devices and systems within the organization are inventoried | Functional | superset of | DI:AID(4) | Ability for the device identifier to be used to discover the IoT device for the purpose of network asset identification and management. |
| ID.AM-1 | Physical devices and systems within the organization are inventoried | Functional | intersects with | DO:CAP(4a) | Providing details for how to establish unique identification for each IoT device associated with the system and critical system components within which it is used. |

# 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 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

Written feedback on the Paper is posted on NIST CSF 2.0 Webpage.
The Concept Paper was also discussed at CSF 2.0 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

# How You Can Get Engaged in CSF 2.0

**NIST encourages you to engage and spread awareness of the CSF update**

- Help spread awareness of the CSF 2.0 effort
- Share policies that leverage or align with the CSF
- Share suggestions for potential changes

**Methods of engagement:**

- Direct 1-1 engagement– contact NIST at cyberframework@nist.gov
- Attend public workshops and events –
  - CSF 2.0 Workshop #1 (August 2022) and #2 (February 2023) recordings available
  - Stay tuned for a workshop this Fall!
- Comment on drafts –
  - Stay tuned for CSF 2.0 draft this summer

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

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

# STAY IN TOUCH

## CONTACT US

NIST.gov

@NISTcyber