Carnegie Mellon University
Software Engineering Institute

Overview of NIST CSF 2.0

JUNE 2, 2023

Brett Tucker

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM23-0559

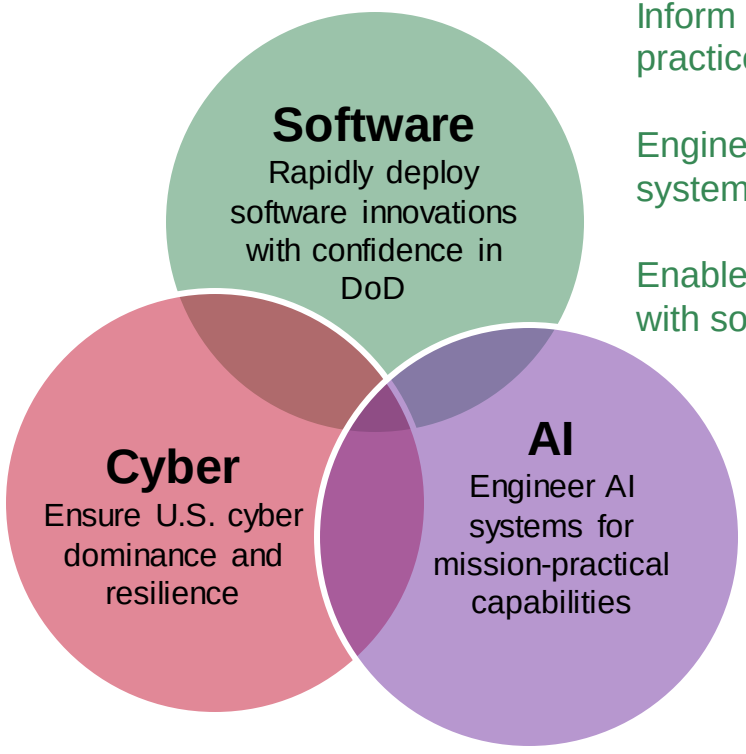
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

CMU Software Engineering Institute (SEI)

Bringing innovation to the U.S. Government

- Federally Funded Research and Development Center (FFRDC) chartered in 1984 and sponsored by the DoD
- Leader in researching complex software engineering, cyber security, and artificial intelligence (AI) engineering solutions
- Critical to the U.S. Government's ability to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

Our technical research connects software, AI, and cyber strategies for **maximum** impact



Inform DoD software policy and practice to accelerate acquisition

Engineer intelligent software systems

Enable DoD mission capability with software innovation

Advancing Cyber by Design

Enhancing Cyber Resilience

Moving the Market and Shaping the Future

AI for leap-ahead software engineering and cyber capabilities

Mature the discipline of AI Engineering

Apply and integrate AI technologies in DoD and related mission capabilities

CERT Division – Birthplace of Cyber Research

Carnegie Mellon University Software Engineering Institute

Our Legacy and Today's Role in Shaping the Future:

1988

Computer Emergency Response Team formed in response to the Morris Worm

2022

Cybersecurity Engineering and Resilience Team conducting collaborative and innovative evidence-based research to fortify the cyber ecosystem and protect national security and prosperity

Why CERT Matters:

Trusted

Conducting research for the U.S. Government in a non-profit, public-private partnership

Valued

Innovating solutions with a global collaboration of military, industry, and academia

Relevant

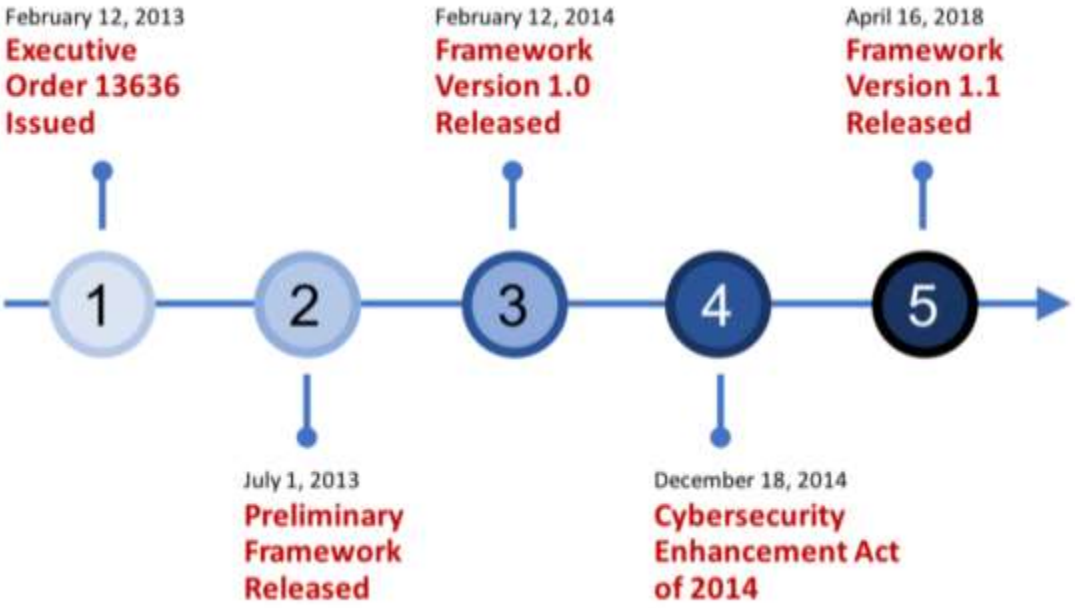
Achieving results for our mission partners

Discover more about our research at sei.cmu.edu

Download software and tools
Participate in education offerings
Attend an event
Search the digital library
Read the SEI Year in Review
Explore our research and capabilities
Collaborate with the SEI on a new project

Carnegie Mellon University
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213
888-201-4479
info@sei.cmu.edu

Cybersecurity Framework (CSF) Timeline



Community Engagement for a New Future

- August 17, 2022: Journey to the NIST Cybersecurity Framework (CSF) 2.0 Workshop #1
- January 2023: Concept Paper Published
- February 15, 2023: Virtual CSF 2.0 Workshop #2
- February 22 or 23, 2023: In-Person CSF 2.0 Working Sessions

Feedback Collected

- RFI
- Workshops
- Dedicated Slack channel
- Virtual and In-Person events
- Email comments

- Public, private, and academic institutions
- International participants from over 100 countries

CSF 2.0 Concept Paper Highlights

- Maintain the CSF as a framework
- Increase international engagement
- Expand adoption of the Online Informative References (OLIR) program with NIST
- Add a new Govern Function
- Expand coverage of cybersecurity supply chain risk management (C-SCRM)
- Further advance cybersecurity measurement and assessment

NIST CSF Concept Paper:
https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

CSF 2.0 Proposed Structure

Function
Identify
Protect
Detect
Respond
Recover
Govern

Function	Category	Subcategory
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

6 Functions

Total Categories and Subcategories to be Determined

Online Informative References

Govern Function – Most Profound Update

- May include:
  - Organizational Context - determination risk tolerances of the organization, customers, and society
  - Risk management strategy discussion
    - Assessment of cybersecurity risks and impacts
  - Establishment of cybersecurity policies and procedures
  - Understanding of cybersecurity roles and responsibilities

- Consistent with the Govern function in the Privacy Framework and the draft AI Risk Management Framework

Community Need: Mapping CSF 2.0

- Update or revise mappings to the new CSF 2.0
  - Cybersecurity Maturity Model Certification (CMMC)
  - Cybersecurity Capability Maturity Model (C2M2)
  - Cyber Resilience Review/External Dependency Management (CRR/EDM)

Call to Action – Provide Mappings: NIST welcomes submissions of mappings to the CSF. NIST encourages authors/owners of relevant cybersecurity resources to connect with NIST 1) to develop mappings to the CSF 1.1 if a mapping does not exist to ease the development of mappings to CSF 2.0, and 2) to coordinate releasing mappings to CSF 2.0.

Community Opportunity: Capabilities Mapping

Carnegie Mellon University Software Engineering Institute

"NIST is collaborating with the community to develop technology-specific mappings to describe the relationship between security capabilities that can be achieved by configuring or enabling security features within a technology stack and the desired outcomes described in the CSF."

- Opportunities include:
  - Zero trust architecture
  - 5G security
  - Artificial Intelligence (AI)
  - Trusted IoT

Other Opportunities for Community Collaboration

Carnegie Mellon University Software Engineering Institute

Call to Action – Share Example Profiles: NIST encourages private and public sector organizations to develop and share additional example Profiles for specific sectors, threats, and use cases, such as those identified on the NIST CSF website.

Call to Action – Submit CSF Resources: NIST encourages organizations to submit to NIST recently published resources pertaining to the CSF for inclusion in the resource repository on the CSF website. These can include approaches, implementation guides, mappings, case studies, tools, and others. Please review the criteria for inclusion on the CSF website.

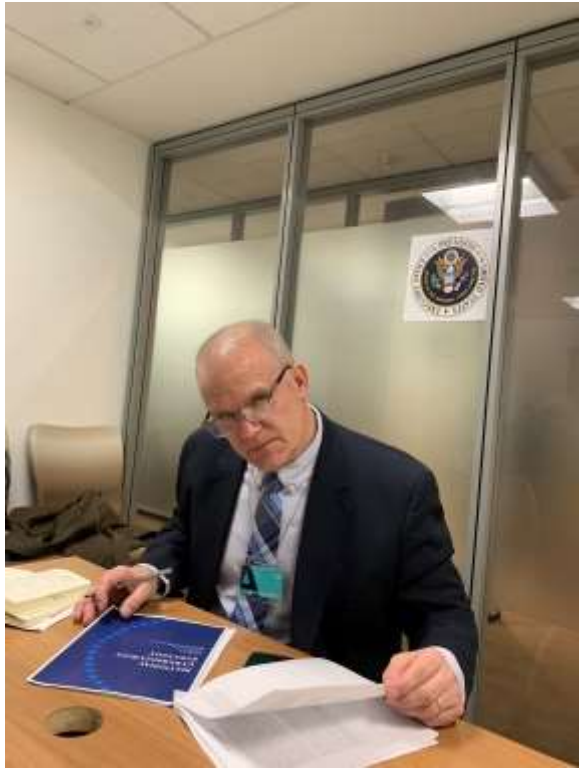
Call to Action – Share Use of the CSF in Measuring and Assessing Cybersecurity: NIST encourages organizations to share information with NIST about how they are using the CSF to measure and assess their cybersecurity. In addition, NIST encourages organizations to share information with NIST about the use of CSF Tiers. Relevant use cases could be incorporated into the CSF or provided as separate resources for additional implementation guidance.

Brief Thoughts on the New National Cyber Strategy

Carnegie Mellon University
Software Engineering Institute

Background

- National Cyber Strategy
- Developed by the Office of the National Cyber Director (ONCD)
  - Published in March 2023
  - Opportunities to contribute
    - Multiple visits to discuss and influence the path



[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

The Five Pillars

Seeks to build collaboration around these five pillars:

1. Defend Critical Infrastructure
2. Disrupt and Dismantle Threat Actors
3. Shape Market Forces to Drive Security and Resilience
4. Invest in a Resilient Future
5. Forge International Partnerships to Pursue Shared Goals

Items of Note

- Provides a glimpse into emerging trends
  - Complexity growing
  - Connectivity and communication critical
  - COVID-19 changed our perspective in terms of reliance and need

- Identifies traditional and non-traditional malicious threat actors
  - China, Russia, Iran, North Korea
  - Criminal syndicates as evidenced by Ransomware

- Counter these threats by
  - Rebalancing the digital ecosystem
  - Realigning incentives through new generational investments

Questions?