Community Profiles Workshop

Date: December 10, 2024

This webinar is being recorded

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

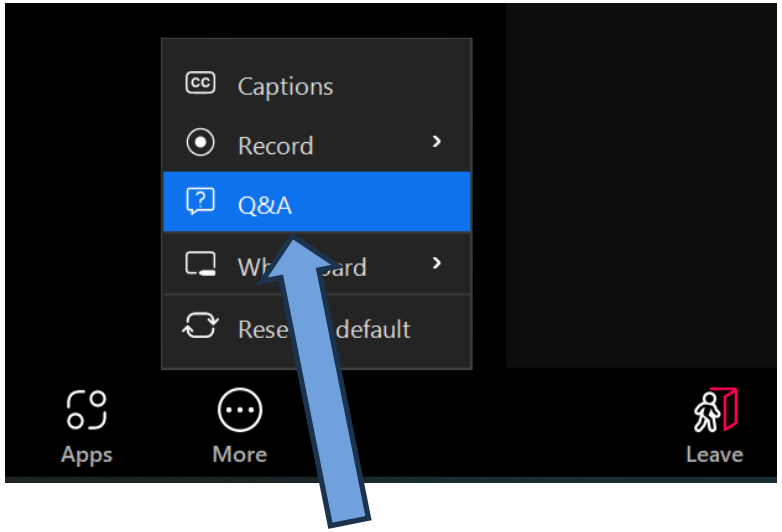
Agenda

Topics	Speaker
Welcome/Rules of Engagement	Tom Walters, MITRE
Introductions NIST Cybersecurity Framework (CSF) 2.0 Overview CSF Community Profiles Revealing of New Name for Resources Page	Nakia Grayson, NIST
Creating Community Profiles	Julie Snyder, MITRE
Break	All
Activity: Community Profiles Priorities	Julie Snyder, MITRE
Break	All
Interactive Discussion	Nakia Grayson, NIST Julie Snyder, MITRE
What's next….	Nakia Grayson, NIST
Q&A	All

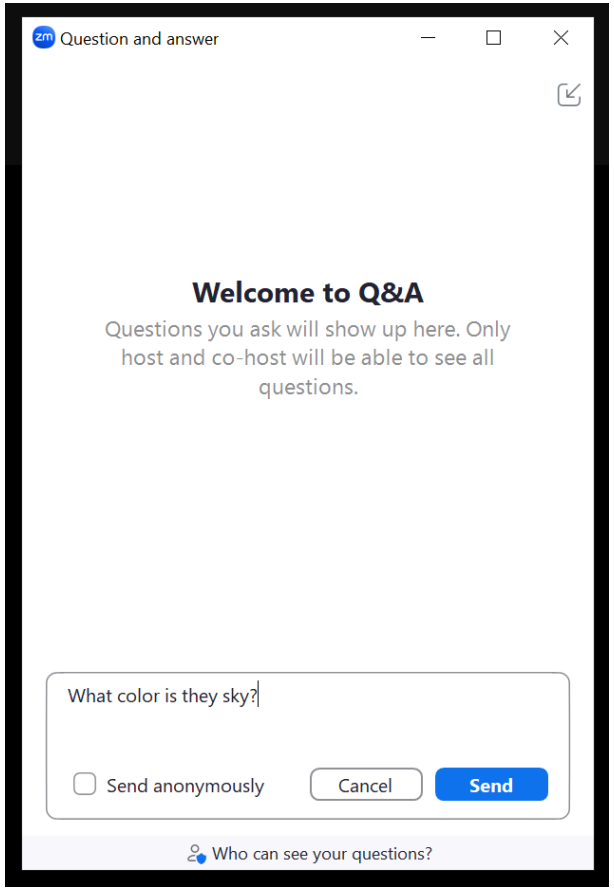
Submitting Questions

Please use the Q&A function to enter your questions.

We will do our best to answer all questions during the Q&A and will post responses to those we did not have time to cover.



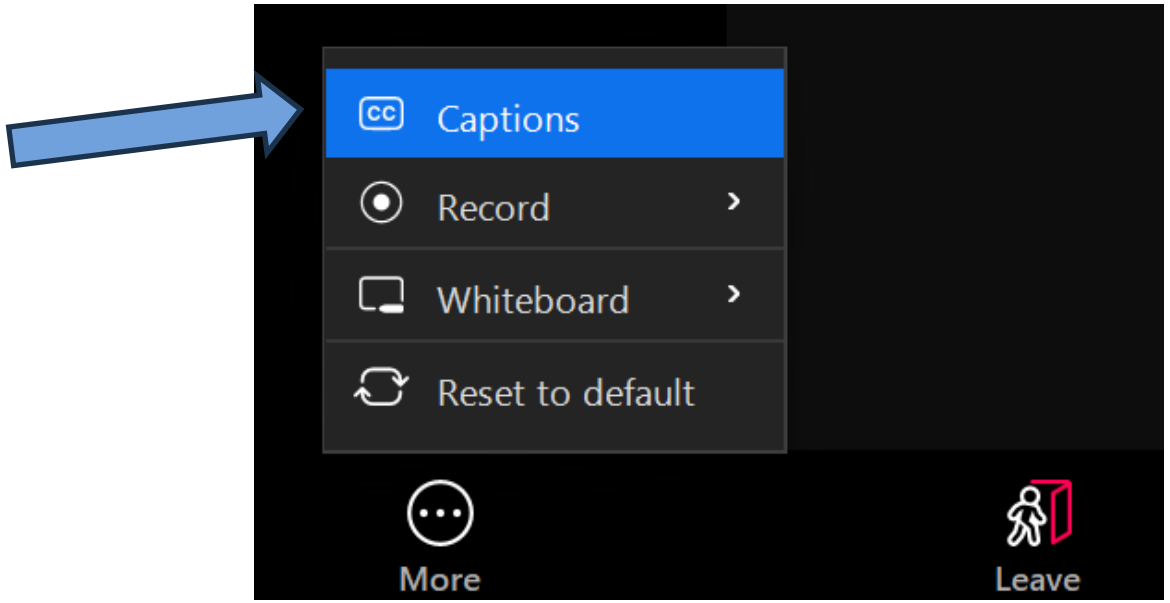
1. To open the Q&A function, click on “More” at the bottom of the screen and select the “Q&A” option.



2. Type your question in the text box and click Send

Captions

To open enable captioning during the event, click on “More” at the bottom of the screen and select the “Captions” option.



How to Participate in Menti Polls

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

We are observing Chatham House Rule to encourage open discussion

Join the Mentimeter (Menti) poll for this workshop in one of three ways:

Join at menti.com | use code 8554 7317

https://www.menti.com/al349u9ubxf6

If you would like to elaborate on any of your responses, feel free to provide additional information in the Zoom chat and/or raise your virtual hand through Zoom to be unmuted

Introductions

Introduction of Speakers

Nakia Grayson, NIST

Julie Snyder, MITRE

MENTI: Getting to Know You

- **What sector do you work in?**
- **Which NIST Frameworks does your organization use?**
- **Has your community developed any Community Profiles?**

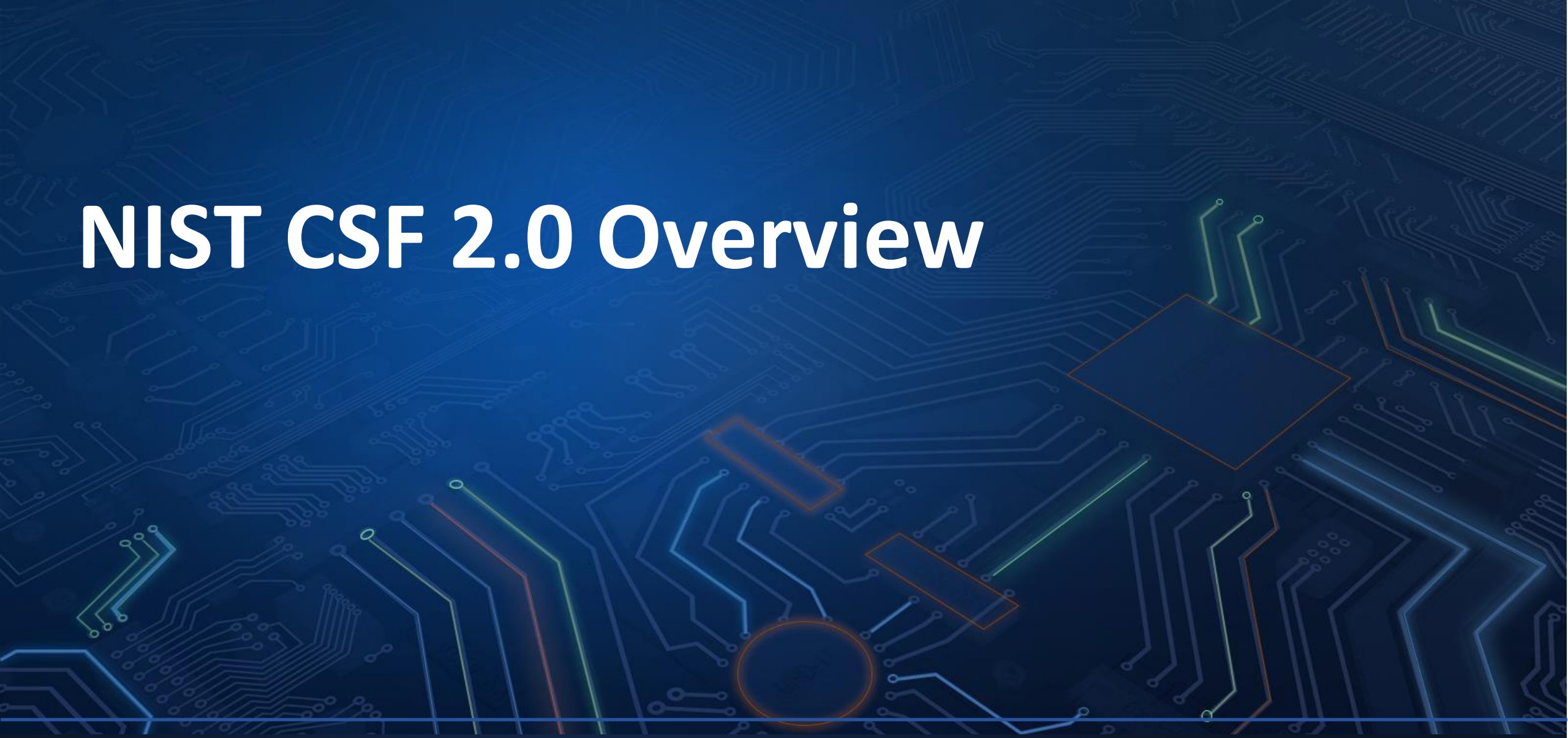
Join at menti.com | use code 8554 7317

Who We Are

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

An open, transparent and collaborative hub addressing complex cybersecurity problems

NIST CSF 2.0 Overview

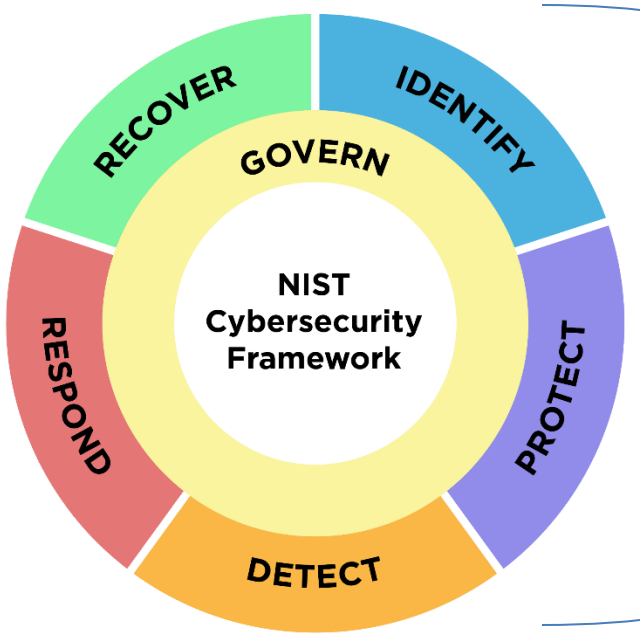


CSF 2.0 Overview

NIST has updated the widely used Cybersecurity Framework (CSF)—its landmark guidance document for reducing cybersecurity risk.

The Framework is comprised of:

- **CSF Core**
- **CSF Organizational Profiles**
- **CSF Tiers**



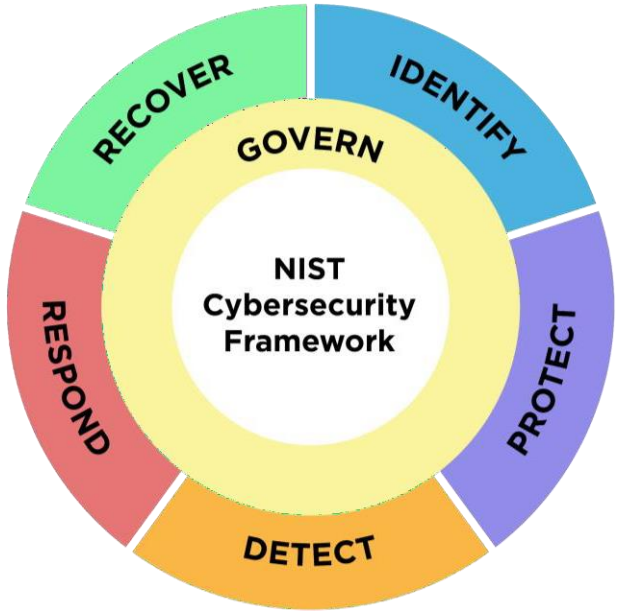
Together, these six Functions provide a comprehensive view for managing cybersecurity risk.

How Did We Get Here?

Visit our CSF 2.0 Website: www.nist.gov/cyberframework

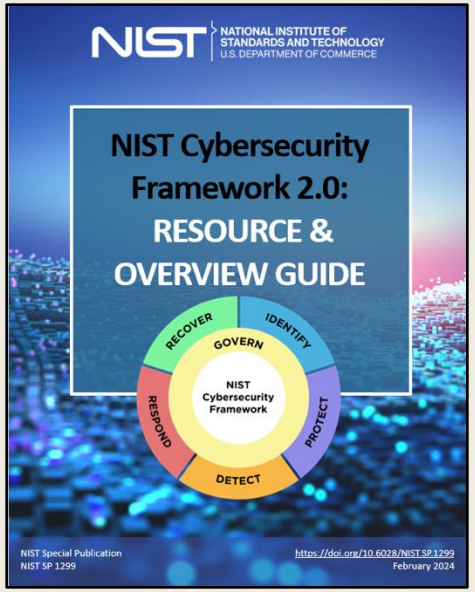
Evolution of Community Profiles in CSF 2.0

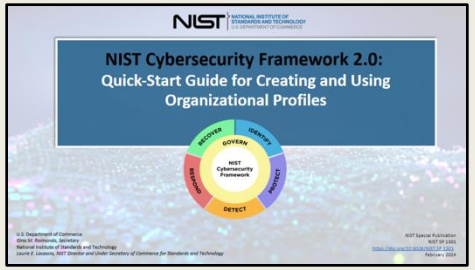
- Expanded scope beyond critical infrastructure
- Addition of a 6th Core Function “Govern”
- Increased emphasis on supply chain risk management
- Listened to feedback, made key updates, developed new resources and tools, and adjusted our guidance based on today’s cybersecurity environment.
- Formalized the term “Community Profiles”

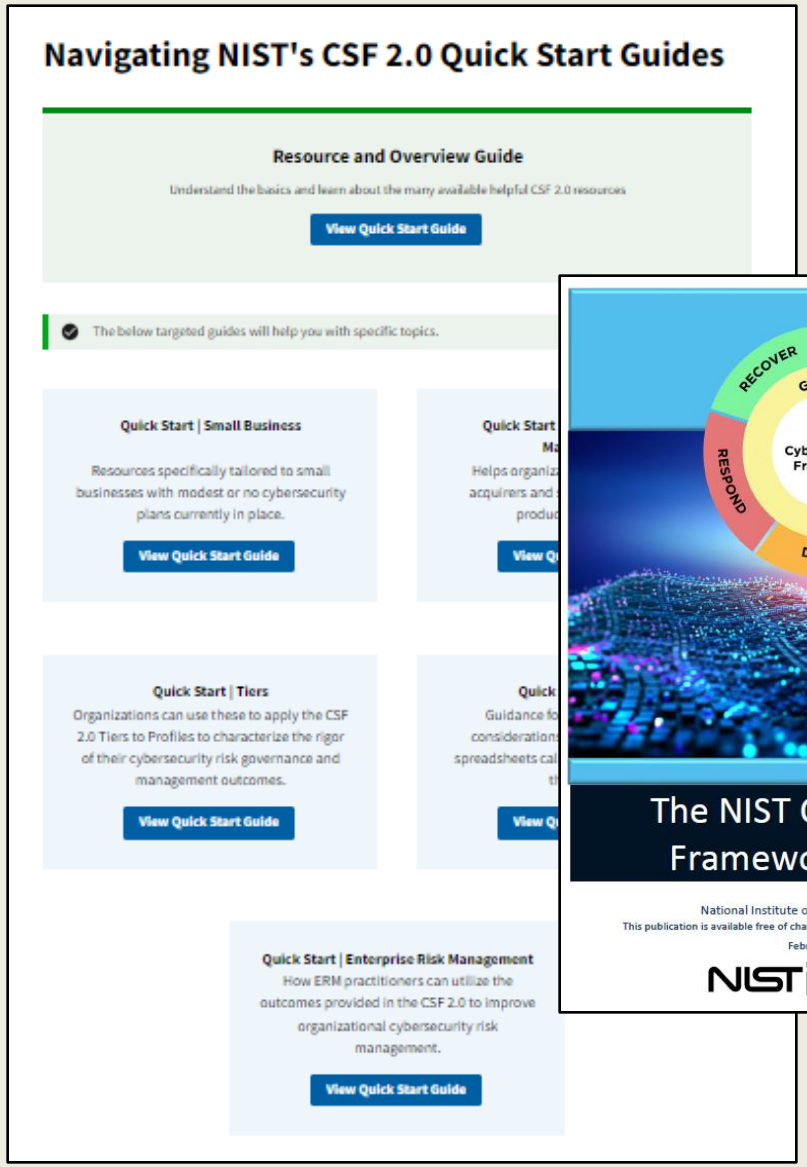


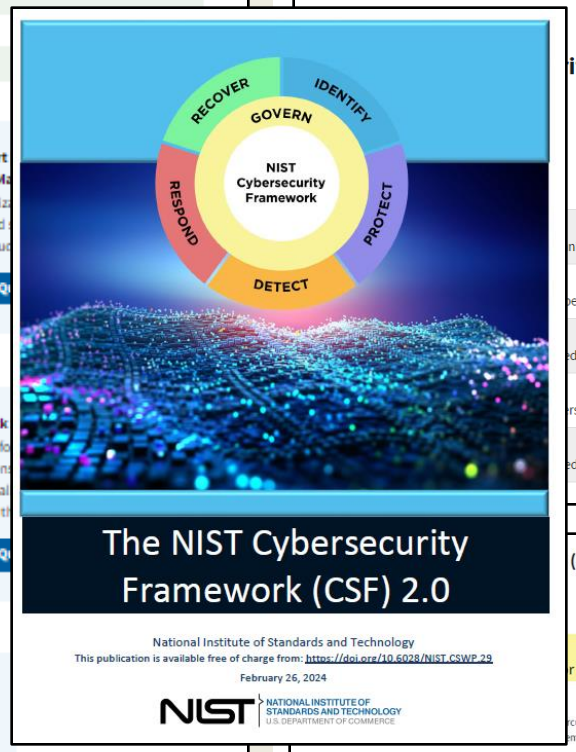
Suite of CSF 2.0 Resources Snapshot

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









Global Impact of CSF 2.0

- The CSF is used widely **internationally**.
- CSF versions 1.1 and 1.0 have been translated into 13 languages and CSF 2.0 have been translated into 6 languages.
- NIST's work with the International Organization for Standardization (ISO), in conjunction with the International Electrotechnical Commission (IEC), over the last 11 years has been expansive.
- The resources allow organizations to build cybersecurity frameworks and organize controls using the CSF Functions.

Learn About Our Global Impact: www.nist.gov/cyberframework

Profiles Overview: CSF 2.0 Terms

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Framework Profiles

Provide a way to understand, tailor, assess, prioritize, and communicate the Core's outcomes based on mission objectives, stakeholder expectations, threat landscape, and requirements.

Organizational Profiles

Describes an organization's current and/or target cybersecurity posture in terms of the Core's outcomes

Community Profiles

Describes CSF outcomes to address shared interests and goals among multiple organizations

The NCCoE Community Profiles work facilitates CSF implementation and helps each community address its specific cybersecurity challenges.

CSF Community Profiles

Communities

Organizations that share a common context and an interest in their cybersecurity posture:

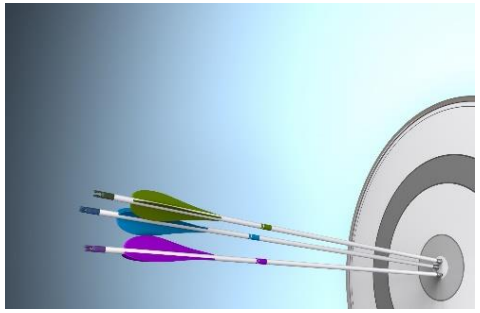
- **Sectors/subsectors (e.g., critical infrastructure sectors)**
- **Technologies (e.g., mobile, cloud)**
- **Other use cases**

Benefits of Community Profiles

Use **shared taxonomy** for cybersecurity and privacy in the context of the community

Align requirements from multiple sources

Leverage expertise across the community



Encourage **common target** outcomes

Minimize the burden by working together

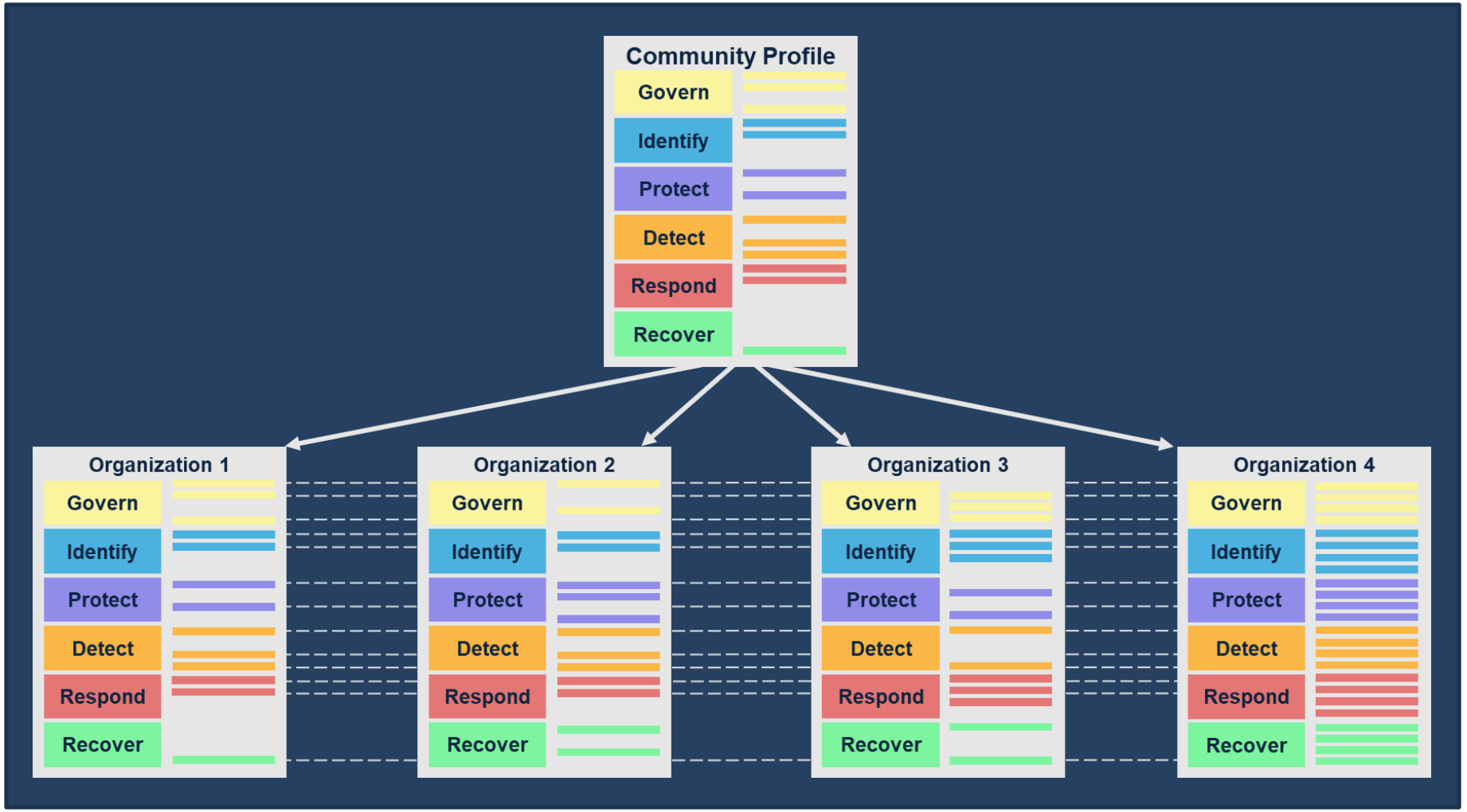
Communicate about cybersecurity and privacy risk

Source (adapted): *Pascoe C, Snyder JN, Scarfone KA (2024) NIST Cybersecurity Framework 2.0: A Guide to Creating Community Profiles. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 32 ipd. https://doi.org/10.6028/NIST.CSWP.32.ipd*

Community Profile Content

A Community Profile offers a common view.

Organizations can describe where and why they deviate from the Community Profile and each other and engage in risk discussions with a common starting point.



Community Profiles Inform Organizational Target Profiles

Notional Priority Levels*:

- ↑ Higher
- ● Same as Community Profile
- ↓ Lower

***Communities and organizations can choose any prioritization schema that works best for them**

Revealing of New Name for Resources Page

Community Profiles Resources

We have new name! The NCCoE Framework Resource Center web collection is now called:

Resources for Applying NIST Frameworks

https://www.nccoe.nist.gov/applying-frameworks-resources

Available Resources

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Check for updates

NIST Cybersecurity White Paper
NIST CSWP 32 ipd

NIST Cybersecurity Framework 2.0: A Guide to Creating Community Profiles

Initial Public Draft

Cherilyn Pascoe
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

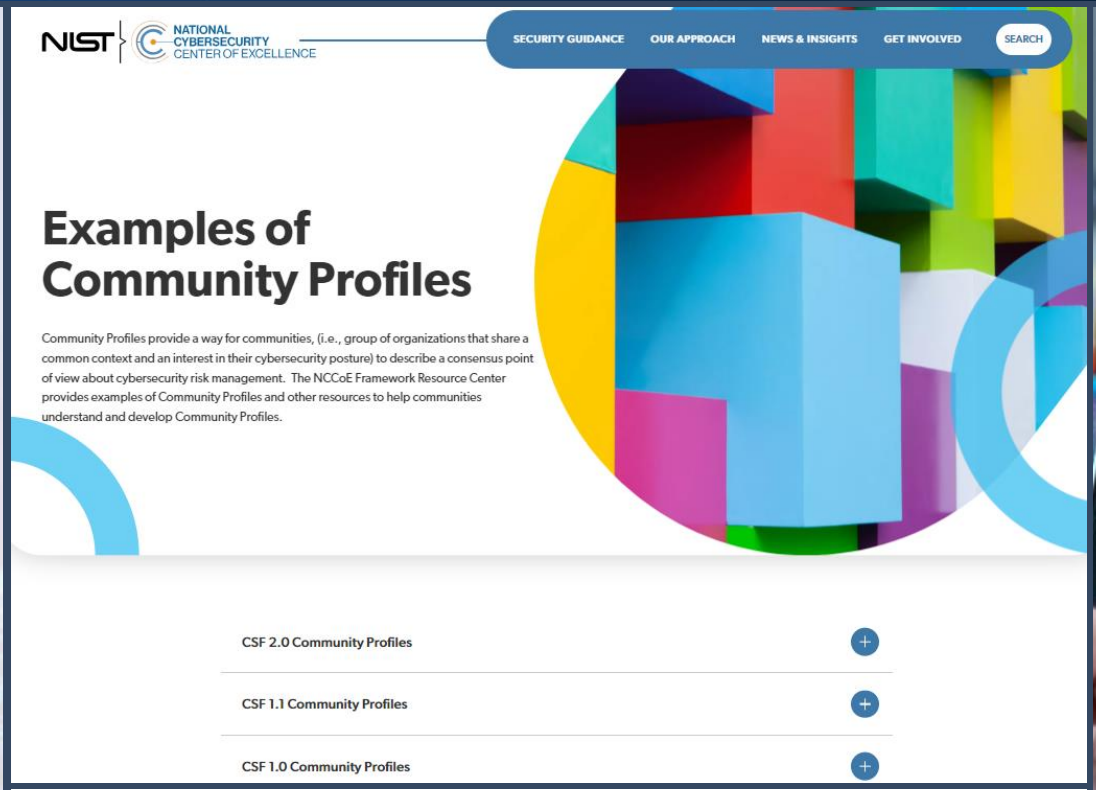
Julie Nethery Snyder
The MITRE Corporation

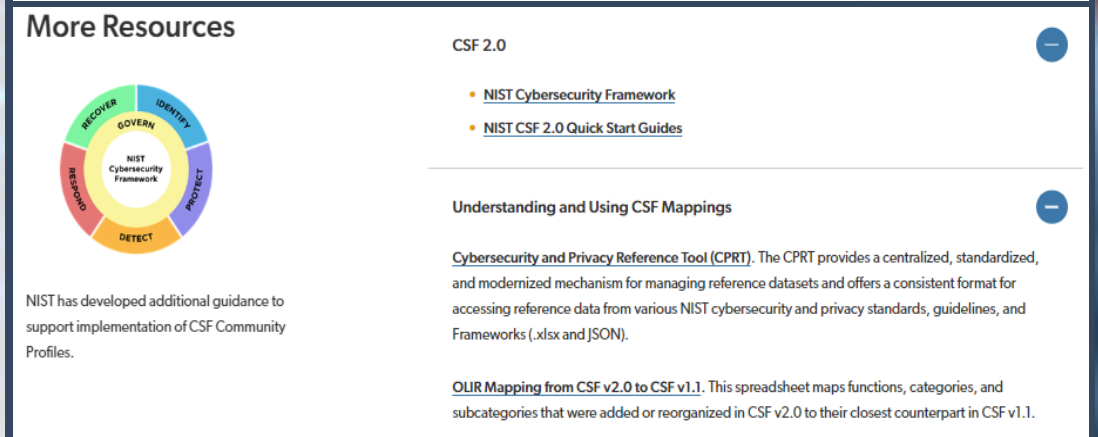
Karen Scarfone
Scarfone Cybersecurity

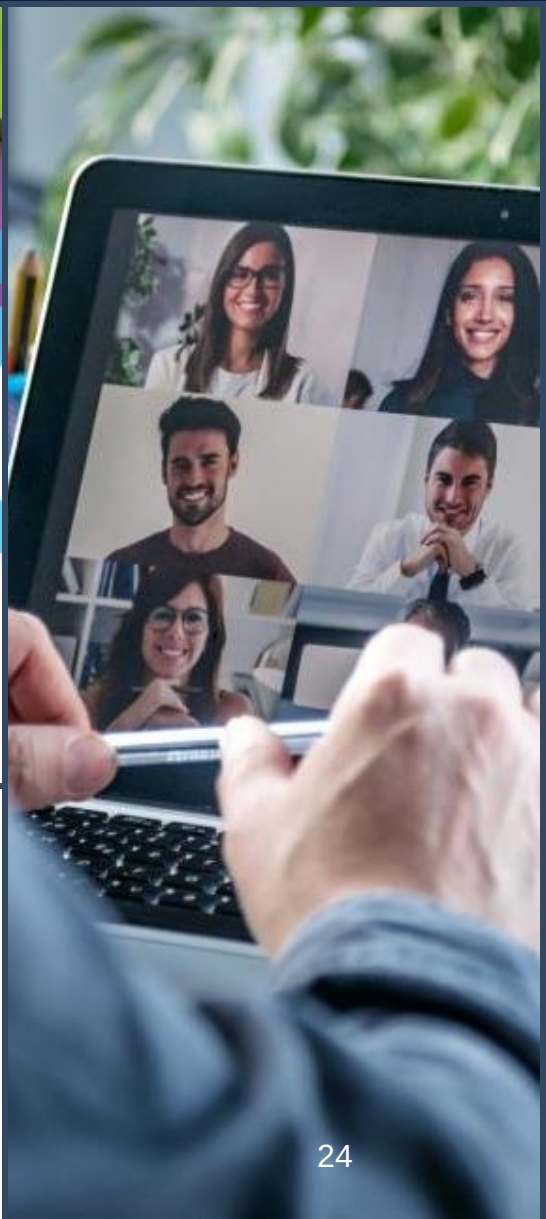
This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.32.ipd

February 26, 2024

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE







Creating Community Profiles

A Guide to Creating Community Profiles

NIST Cybersecurity White Paper (CSWP) 32

NIST Cybersecurity Framework 2.0: A Guide to Creating Community Profiles
Initial Public Draft

Cherilyn Pascoe
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Julie Nethery Snyder
The MITRE Corporation

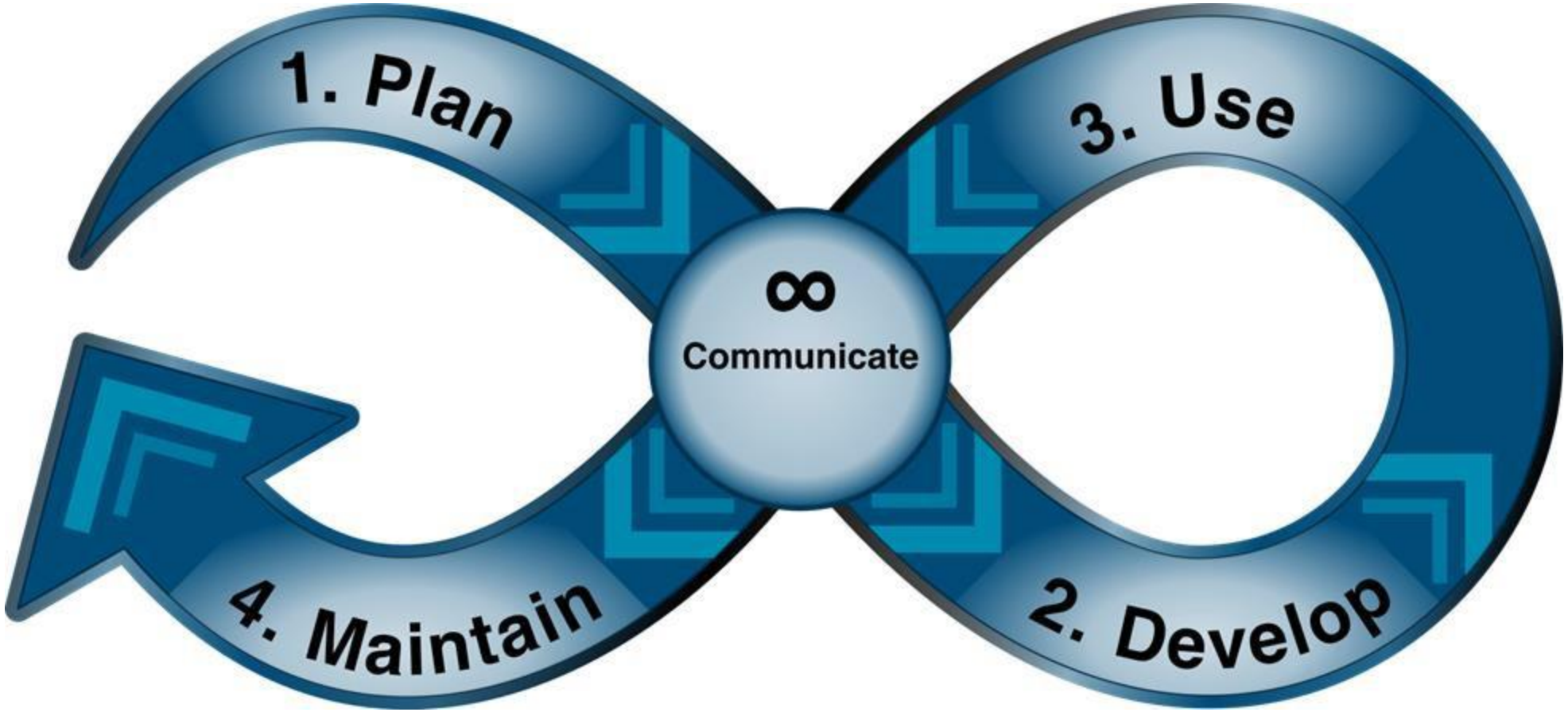
Karen Scarfone
Scarfone Cybersecurity

February 26, 2024

- Describes Community Profiles
- Provides a template and guidance for developing Community Profiles
- Offers a Community Profiles Lifecycle

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.32.ipd

Community Profile Lifecycle



The Community Profile Lifecycle offers a structured approach for developing and maintaining Community Profiles.

Community Life Cycle

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Plan

- Identify the intended audience
- Scope the Profile
- Identify participants
- Identify community-specific Informative References
- Determine long-term management approach

Develop

- Identify shared community priorities and objectives
- Align community priorities with CSF outcomes
- Decide what to include in the Profile
- Draft the Profile
- Engage the community to provide feedback
- Inform the community when the Profile is finalized

Use

- Inform leadership
- Align business and operational practices
- Benchmark against industry expectations
- Inform organization's Target Profile
- Assess Current State

Maintain

- Measure impact and determine whether additional resources are necessary
- Identify and monitor for changes and feedback
- Update when needed
- Retire Profile (when no longer needed)

Sample Template

CSF 2.0 Outcome		Priority	Rationale	Informative References / Mappings
ID.AM-01	Inventories of hardware managed by the organization are maintained			
ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained			

Available here: https://www.nccoe.nist.gov/projects/guide-creating-community-profiles

Community Profile Content

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Priorities
Fundamental purposes and operations of a community or organization that the processes and systems support

Informative References
References (e.g., standards, guidelines) the community are already using and can be mapped to CSF outcomes

Implementation Examples*
Examples of activities that could be implemented to achieve part or all of an outcome

Dependencies*
A requirement to meet a priority that lives outside of the community

Rationales
Applicability of the CSF outcome in the context of the community

Considerations*
Supplements rationale by providing additional details within the context of the Profile

Priorities' Relationships*
The relative importance of one item versus another

*** denotes optional Profile content**

Community Profile Tab

CSF 2.0 Core	CSF 2.0 Outcomes	Priority (recommended)	Rationale (recommended)	Informative References/ Mappings (recommended)	Recommendations and Considerations (optional)	Implementation Examples (optional)	Notes (optional)
GV	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored	High	Smart devices are vulnerable to various cyber threats such as malware, data breaches, and unauthorized access, which can have severe consequences for individuals and organizations using these devices. Help with addressing challenges such as ensuring that all smart devices have proper security measures in place, monitoring and updating polices, aligning with relevant industry regulations.	ISO/IEC 27001:2013 - Information security management systems, Center for Internet Security (CIS) Controls for IoT devices, IEC 62443 series on industrial automation and control systems security, NIST 800-125 on "Guide to Security for Full Virtualization Technologies	Regularly updates and patch all smart home devices to ensure smart home devices to ensure they are up-to-date with the latest security measures & use strong passwords for smart home device and change them regularly	Conduct regular vulnerability assessments on smart home devices to identify any security risks	N/A
GV.OC	The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood	High	Users vulnerable to cyber attacks on smart devices due to a lack of awareness or resources to properly secure these devices. The community can help to can help address these vulnerabilities and protect the community from potential cyber threats.	NIST 800-53: Security and Privacy Controls for Federal Information Systems and Organizations, CSA IoT Security Controls Framework, ISO/IEC 27001: Information Security Management Systems	N/A	Collaborate with stakeholders, such as smart home device manufacturers, service providers, and regulatory bodies, to ensure compliance with legal and regulatory requirements related to cybersecurity	Join groups that inform you about updates related to smart home devices

Example #1: Incident Response

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, and Notes Specific to Incident Response
GV.RR-02	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	Medium	**N1:** Roles and responsibilities that involve cybersecurity incident response typically exist throughout an organization and often include third parties (e.g., those under contract) to help perform incident response activities for the organization. **R1:** All roles and responsibilities involving cybersecurity incident response should be documented in an organization's policies. **R2:** All appropriate individuals or parties should be designated the authority necessary to fulfill their incident response-related responsibilities.

Example #2: Electric Vehicle Extreme Fast Charging Infrastructure

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

3.2. Mission Objective 2: Maintain Resilience of the XFC Infrastructure

All users in the EV/XFC ecosystem should have reliable access to services. A loss of cybersecurity may impact physical security; therefore, organizations must implement safeguards to ensure the cyber resilience of the EV/XFC ecosystem. All cybersecurity decisions should be balanced with business needs to maintain usability of the system while keeping the ecosystem secure and resilient.

The rationale for this mission objective includes:

- **EV**. EV owners want assurance that their vehicle is protected before they are willing to participate in the charging ecosystem. Batteries are a significant expense, and a compromised XFC ecosystem could potentially lead to physical damage to the battery, EV components, and other nearby equipment. Thus, implemented safeguards will ease the minds of users and encourage them to use the charging stations.
- **XFC/EVSE**. Due to the unique position of charging stations in the ecosystem, geographical dispersion, and general lack of physical security, charging stations have become an appealing target for threat actors. EVSE infrastructures should be protected, both cyber and physical, to prevent attacks like ransomware or damage to the charging infrastructure itself.
- **Cloud/Third-Party**. The cloud/third-party environment facilitates connectivity between domains of the infrastructure. It should be protected to maintain operations.
- **Utility/Building Management Systems**. Utilities and building management systems should have protection systems in place to prevent manipulation of utility components to maintain safe operations.

AM-4: External information systems are catalogued.	**Ecosystem:** Catalogue external partner connections and level of access to external information systems, establish processes and agreements with all external partners to ensure an understanding of information system usage, and establish a level of trust and security that is consistent with the policies of the organization.	**[NIST SP 800-53r5]** AC-20, PM-5, SA-9 **NERC CIP** 011-2-R1
AM-4 | EV	This may include cataloging EVSE connections to EV, processes used to verify EV identity and accounts, and charge profile information (current, capacity, battery health, etc.) communication. EV connections to cloud-based systems, including account, profile, and location information, should consider also being included.	**[NIST SP 800-53r5]** AC-20, PM-5, SA-9
AM-4 | XFC/EVSE	External information systems that EVSE interfaces with may include EV-specific systems as well as any communication to any cloud/third-party operators or utility/building management systems. EVSE functionality may be dependent upon external information systems to support EVSE connections to EV, to the utility (data flow for power metering, account billing, and demand forecasting) and connections to cloud (to support data flow for charge station search and reservation and billing information).	**ISA/IEC 62443-2-1:D4E1** ORG 1.1
AM-4 | Cloud/Third-Party	Cloud/Third-Party owners/operators may include interactions with external partners, systems, and entities, such as EVSE, utilities, building/facility management systems, and transaction management systems.	**[NIST SP 800-53r5]** AC-20, PM-5, SA-9
AM-4 | Utility/Building Management System	Some aspects of utility or building/facility management require external information systems for proper operation and support EVSE connections to utility and cloud-based systems for functions such as demand forecasting.	**ISA/IEC 62443-2-1:D4E1** ORG 1.1

Example #3: Electric Vehicle Extreme Fast Charging Infrastructure

Priority	Mission Objective (Keyword)
1	Manage provenance and data integrity throughout the genomic data lifecycle (**Data**)
2	Preserve privacy of relatives (**Relatives**)
3	Identify, model, and address security and privacy risks to genomic data (**Risks**)
4	Manage informed consent throughout the genomic data lifecycle (**Consent**)
5	Preserve privacy of donors (**Donors**)
6	Manage
7	Maintain
8	Facilitate
9	Maintain
10	Protect i
11	Enable a
12	Promote (**Platfor**
Note:	*This CSI Privacy Objectiv*

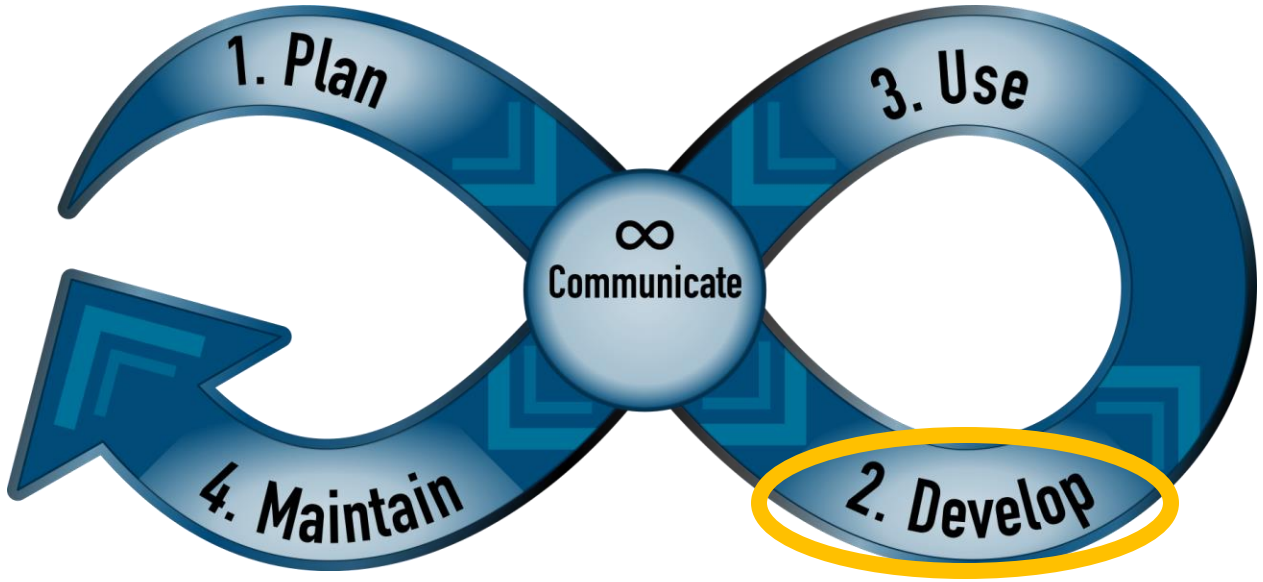
Mission Objective	1. Data	2. Relatives	3. Risks	4. Consent	5. Donors	6. Access	7. Trust	8. Research	9. Legal	10. IP	11. Diversity	12. Platforms	General Rationale	Mission Objective Specific Consideration
ID.AM-1: Physical devices and systems within the organization are inventoried	●●	●●	●●	●●	●●	●●●	●	●●	●●	●●●	●●	●●●	Manage physical assets to secure data stored, identify risks, and secure the analysis pipeline. Physical device asset management is rated a lower priority than managing virtual or software assets because it is generally considered a less likely attack vector.	6,10,12 - Physical access was considered higher priority for managing unauthorized access to data, protecting IP, and securing data analysis pipelines. 11 - Physical location may affect sample diversity; point of collection may vary from data processing location.
ID.AM-2: Software platforms and applications within the organization are inventoried	●●●	●●●	●●●	●●●	●●●	●●●	●	●●●	●●	●●●	●●	●●●	Software is considered a more likely attack vector and thus a higher priority than hardware to manage access, identify risks, and protect intellectual property. Software asset management helps identify potential risks to data integrity, provenance, IP protections, and platforms.	1 - Software inventory supports managing data integrity and provenance. 2,4,5 - Software Asset Management provides useful inputs for privacy risk management and requirements including managing consent. 10 - Software may be IP. 11 - Need to identify any software bias that impacts sample diversity.

Activity: Community Profile Priorities

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

The Case for Priorities

Helpful for understanding communities with a complex scope
Methodical way of thinking through community needs: operational, functional, business
Ties cybersecurity risk to enterprise risk for organizations in the community



Creating Community Profile Priorities

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

What is your community's strategic mission?

What does your community do?

What are the primary **operational activities** organizations in your community conduct?

What are the enabling business activities?

What does your community **hope to achieve** through deploying certain technologies?

How do you envision certain **capabilities** playing a role in your operations?

What is the "right" verb to describe those activities?

Build, Conduct, Coordinate, Deliver, Enable, Engage, Enhance, Facilitate, Improve, Maintain, Manage, Meet, Operate, Oversee, Perform, Prepare, Provide, Transfer, Use

Is the language concise, clear, and distinct?

Is the language clearly **distinguishable** to allow prioritization?

Is the language **concise** and enables a **common understanding**?

Are **domain-specific terms** needed?

Building a Community Priority Statement

Examples of Published Community Priorities

- Conduct and Oversee Voting Period Activities
- Coordinate Port Operations
- Protect Intellectual Property
- Maintain Logistics
- Maintain Operational Efficiency
- Maintain Operational Security
- Maintain Personnel Competencies
- Deliver Reliable Performance through Secure Communications
- Maintain Trust and Manage Reputational Risk
- Manage Crisis/Strategic Communications
- Ensure Secure and Timely Communications
- Obtain Timely Vessel Clearance
- Maintain Compliance with Laws and Regulations
- Minimize Driver Distraction and Workload

Welcome to the National Institute of Sweets & Taffies

Our sweets pull you in every time!

- Fictitious organization that supports the candy manufacturing community… but let's pretend it's real!
- About the organizations in our candy community:
  - Candy manufacturers that make their own candies
  - Suppliers in the global supply chain for sourcing ingredients
  - Sales and distribution entities
    - Organizations that own physical and online stores
    - Organizations that distribute to other retailers (e.g., big box stores)
  - Marketing partners

ACTIVITY: Creating Community Priorities

National Institute of Sweets & Taffies

About Our Community

- Candy manufacturers
- Suppliers for sourcing ingredients
- Sales and distribution entities
- Organizations that own stores
- Organizations that distribute to other retailers
- Marketing partners

What is the "right" verb to describe each activity?

Build, Conduct, Coordinate, Deliver, Enable, Engage, Enhance, Facilitate, Improve, Maintain, Manage, Meet, Operate, Oversee, Perform, Prepare, Provide, Transfer, Use

Community Priorities: Example Results

National Institute of Sweets & Taffies

ACTIVITY: In thinking about a community your organization is a part of, what are some Community Priorities you might recommend?

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Join at menti.com | use code 8554 7317

Interactive Discussion – Current and Planned Resources

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

MENTI: What additional information regarding assessments would be useful?

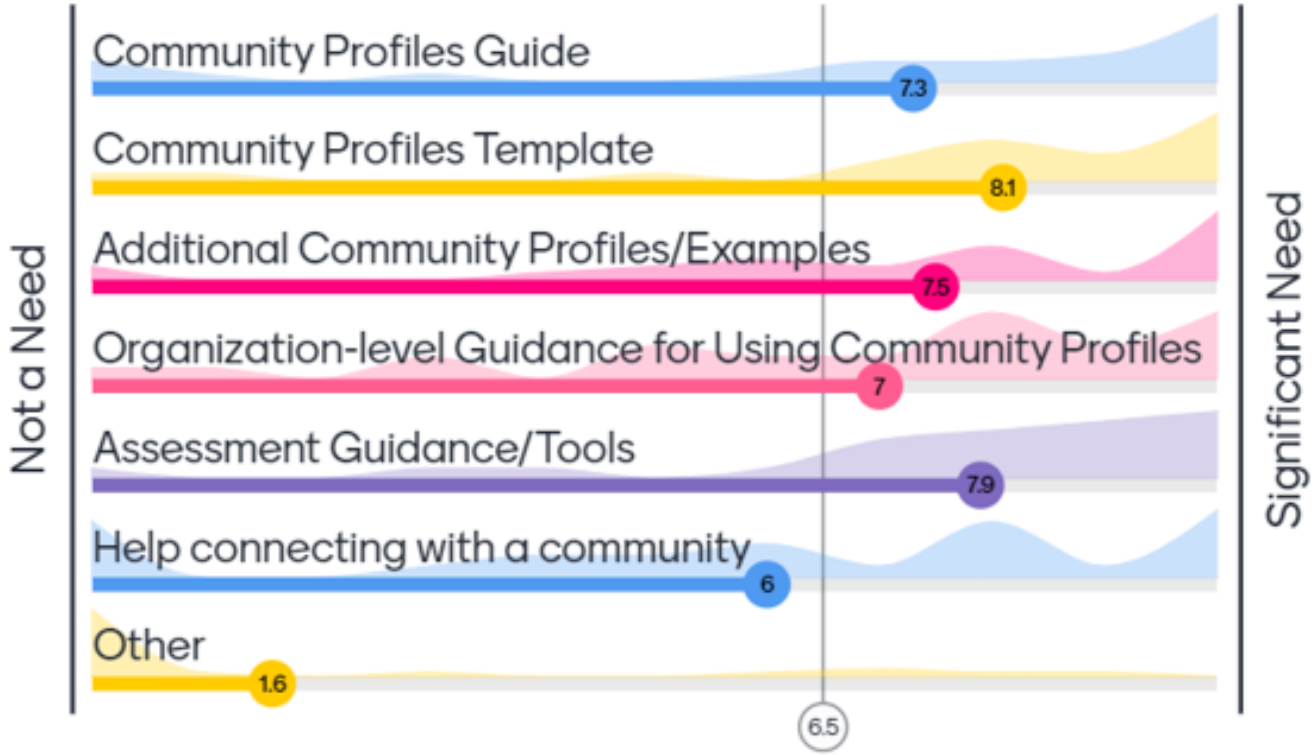
Assessing Current State

Community Profiles can serve as valuable tools for assessing both the community and organizations within the community. At the community level, Profiles can help a community determine where its ecosystem has systemic cybersecurity challenges or new challenges (e.g., impacts related to emerging trend and technology), and work in collaboration to address those challenges. Communities may also choose to create additional guidance to help organizations assess their progress.

In addition to using Community Profiles to create an Organizational Target Profile, organizations can use the information in Community Profiles to inform how they conduct internal assessments of their progress in relation to community expectations. Communities may choose to include assessment criteria and implementation examples to facilitate consistent evaluation by community members. These assessments will inform Organizational Profiles and strategic planning efforts for organizations in the community.

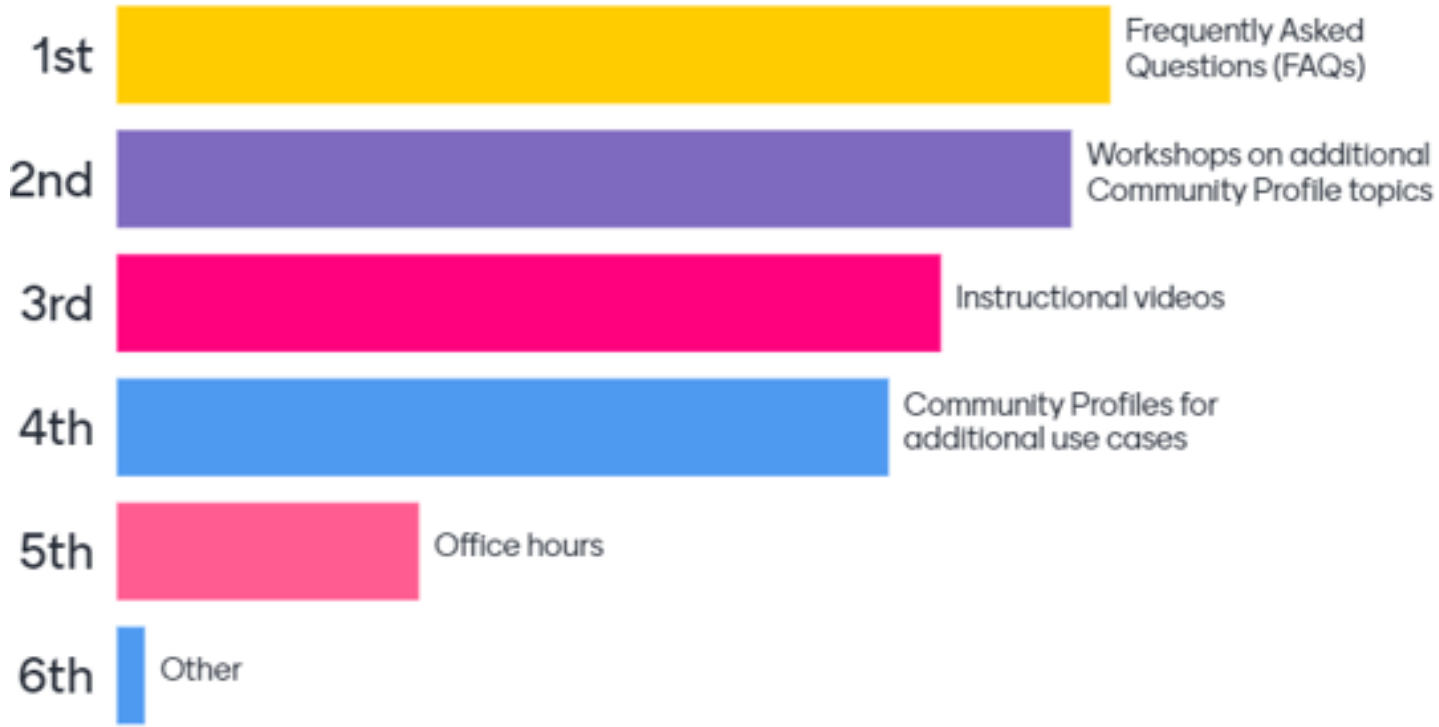
Join at menti.com | use code 8554 7317

MENTI: Are these still the right resources to help you create a Community Profile?



Join at menti.com | use code 8554 7317

Updates on Requested Resources



MENTI: What barriers or challenges are you experiencing when it comes to creating or using Community Profiles?

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Join at menti.com | use code 8554 7317

MENTI: What topics should we include during our next workshop?

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Join at menti.com | use code 8554 7317

What’s next….

Community Profiles in Progress @ NCCoE

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Cybersecurity Framework Profile for Semiconductor Manufacturing
https://www.nccoe.nist.gov/projects/cybersecurity-framework-profile-semiconductor-manufacturing

Cyber AI Profile
https://www.nccoe.nist.gov/projects/cyber-ai-profile

Cybersecurity and Privacy of Genomic Data
https://www.nccoe.nist.gov/projects/cybersecurity-and-privacy-genomic-data

Manufacturing
https://www.nccoe.nist.gov/manufacturing

Position, Navigation and Timing (PNT)
https://www.nccoe.nist.gov/projects/hybrid-satellite-networks-cybersecurity

Ransomware
https://www.nccoe.nist.gov/data-security

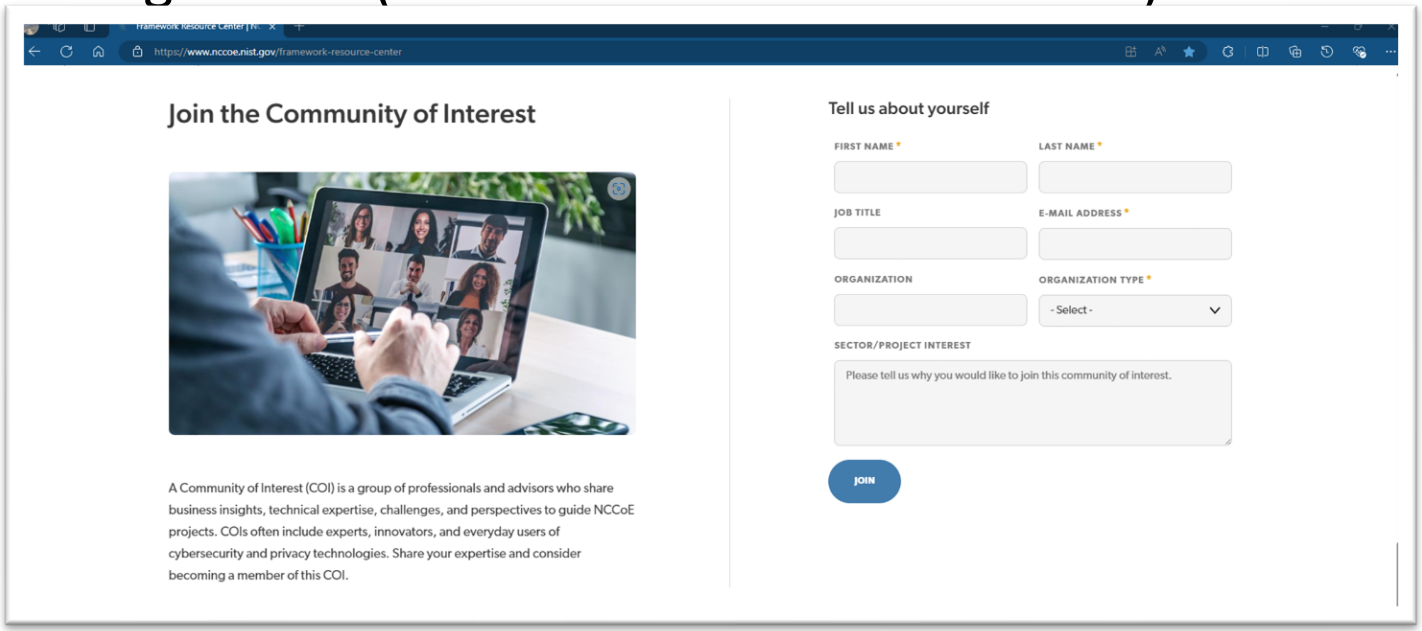
Upcoming Activities

- Continue developing additional Community Profiles
  - New communities/topics
  - Multi-framework Profiles
- Continue engagement
  - Existing & new communities
  - Understand additional resources needed
- Expand website content
  - Add FAQ's
  - Publish a final Guide for Creating Community Profiles
- Next workshop will be in the Spring (Date TBD)

How to Get Involved

How to Get Involved

- Join Community of Interest (COI)
- Provide feedback on Guide and Template
- Share your thoughts on additional resources that would be helpful
- Share your Community Profile adoption stories
- Participate in upcoming events (Will be shared on COI listserv)



Q&A

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

THANK YOU!

Your inputs help us create stronger work products!

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Resources for Applying NIST Frameworks

https://www.nccoe.nist.gov/applying-frameworks-resources

framework-profiles@nist.gov

nccoe.nist.gov

@NISTcyber