# Journey to the National Institute of Standards & Technology Cybersecurity Framework 2.0

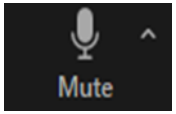
NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

APTA American Public Transportation Association

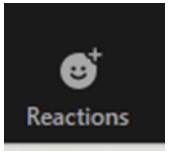
May 29, 2024

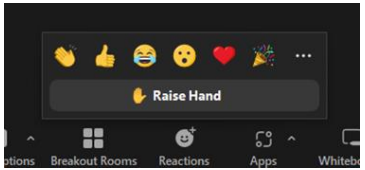
# Housekeeping

- **Mute** when not speaking.

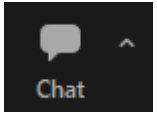



- If you do speak, share your name and agency.
- Raise your hand to speak.




- **Use the chat box to ask questions** or to share links and information.




American Public Transportation Association

# Business Members

The Business Members Cyber Committee educates and shares knowledge and experience about recognizing and better managing the opportunities and risks associated with new technology.

American Public Transportation Association

# Moderator

Scott Belcher
President and Chief Executive Officer
SFB Consulting, LLC
scottfbelcher@gmail.com

American Public Transportation Association

# Panelists

**Nakia Grayson**

IT Security Specialist

National Institute of Standards and Technology

Department of Commerce

**Jeff Marron**

IT Security Specialist

National Institute of Standards and Technology

Department of Commerce

**Amy Mahn**

International Policy Specialist

National Institute of Standards and Technology

Department of Commerce

**Daniel Eliot**

Lead for Small Business Engagement

National Institute of Standards and Technology

Department of Commerce

APTA American Public Transportation Association

# Securing the Road Ahead with the Cybersecurity Framework 2.0

**Amy Mahn, Nakia Grayson, Daniel Eliot, Jeff Marron**
Applied Cybersecurity Division
**May 2024**

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

# Agenda

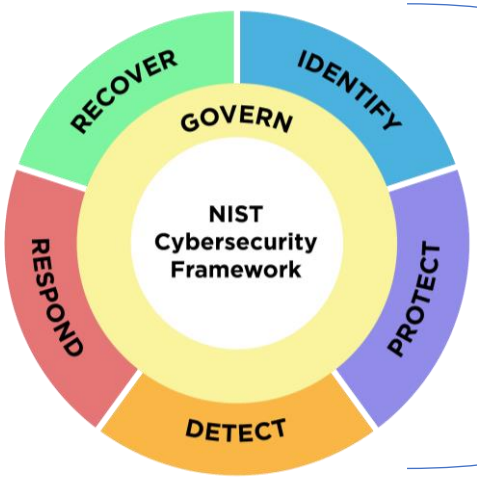
- Introduction
- Brief Overview of CSF 2.0
- CSF Community Profiles
- Overview of the CSF 2.0 Small Business Quick Start Guide
- Additional CSF 2.0 Resources
- How to Get Involved

# 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?

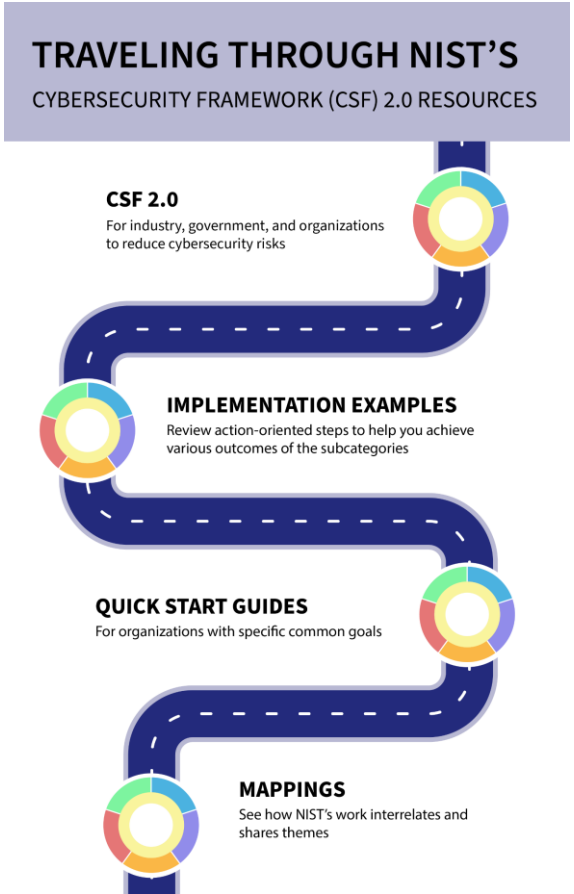
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE


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

# CSF 2.0 | What Makes it Different?

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

- Expanded scope beyond critical infrastructure. CSF 2.0 can help **all organizations** manage and reduce risks.
- Addition of a 6th Core Function “Govern.”
- Increased emphasis on supply chain risk management.
- Formalized the term “Community Profiles.”
- Improves on prior versions; we listened to your feedback, made key updates, **developed new resources and tools**, and adjusted our guidance based on today’s cybersecurity environment.



# Quote from the NIST Director

"The CSF has been a vital tool for many organizations, helping them anticipate and deal with cybersecurity threats. CSF 2.0, which builds on previous versions, is not just about one document. It is about a suite of resources that can be customized and used individually or in combination over time as an organization's cybersecurity needs change and capabilities evolve."

**~ Laurie E. Locascio**

Under Secretary of Commerce for Standards and Technology

& NIST Director

# 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 (*CSF 2.0 translations anticipated soon*).
- 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:** https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources


# Overview of Community Profiles

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

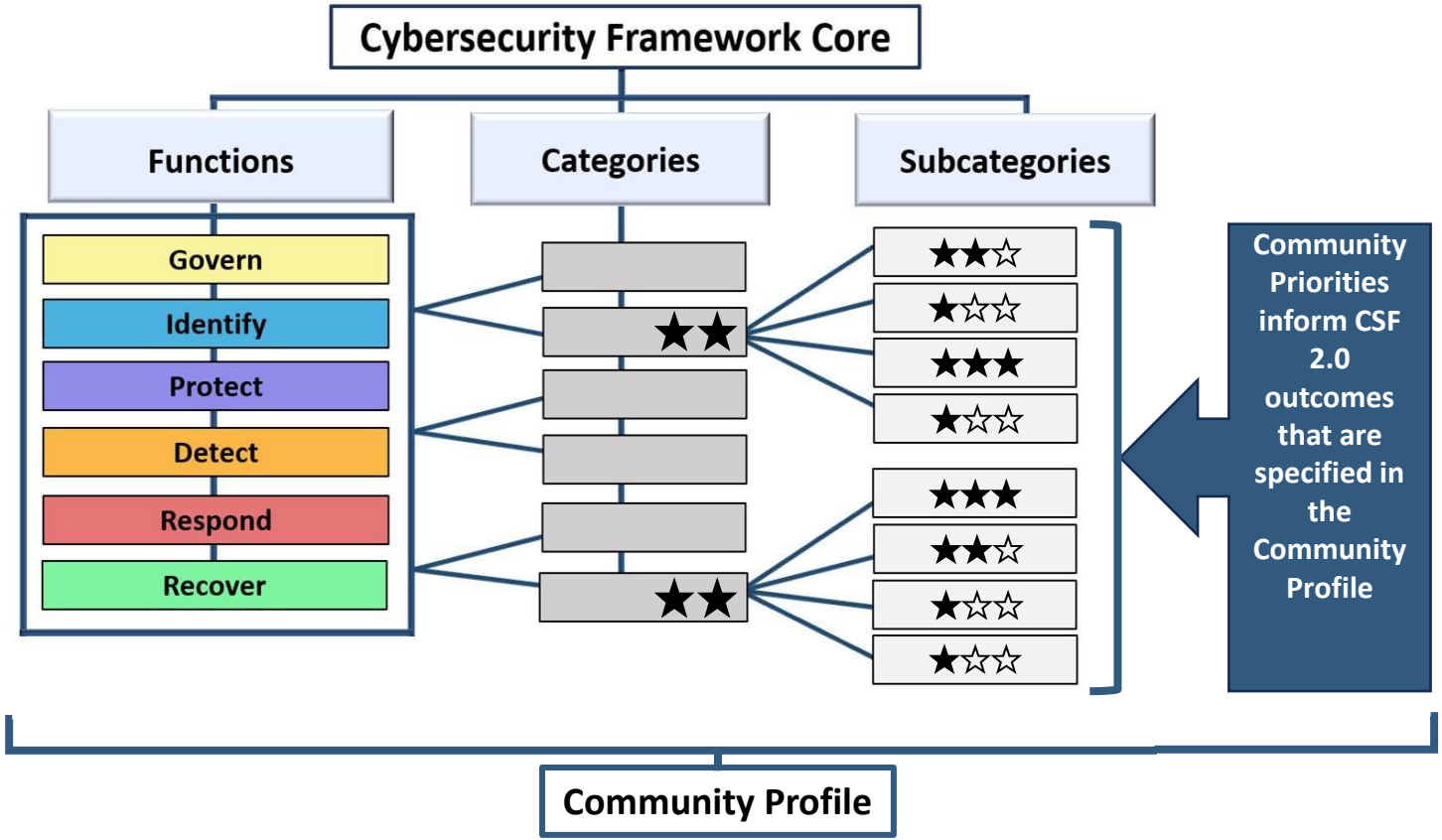
# CSF 2.0 Profiles



**Organizational Profiles:** describes an organization's current and/or target cybersecurity posture in terms of the Core's outcomes.

- Used to understand, tailor, assess, prioritize, and communicate the Core's outcomes by considering an organization's mission objectives, stakeholder expectations, threat landscape, and requirements
- **Current Profile:** specifies the Core outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved
- **Target Profile:** specifies the desired outcomes that an organization has selected and prioritized for achieving its cybersecurity risk management objectives
- **Community Profiles:** describes CSF outcomes to address shared interests and goals among multiple organizations

# Community Profiles

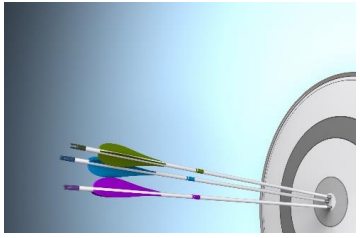


# Benefits of Community Profiles

Use **shared taxonomy** for cybersecurity 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 risk

# Examples of Community Profiles

**CSF 1.1 Profiles**

- eXtreme Fast Charging (XFC)
- Genomic Data (draft)
- Hybrid Satellite Networks (HSN)
- Ransomware

**CSF 2.0 Profiles**

- CRI Profile for the Financial Sector
- Incident Response

**https://www.nccoe.nist.gov/framework-resource-center**


# Resources for CSF 2.0

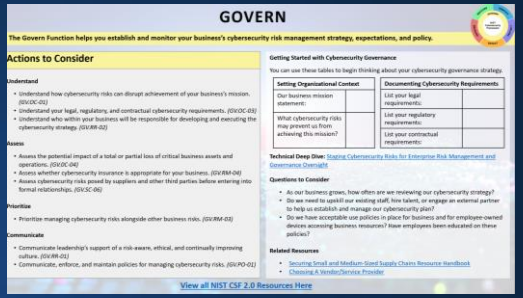
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

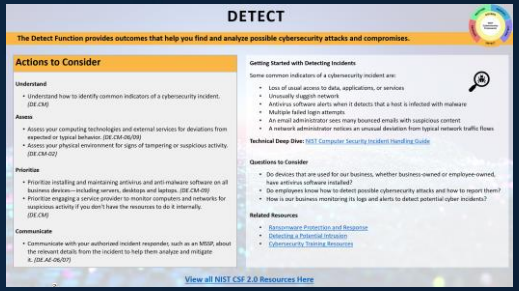
# NIST CSF 2.0 Small Business Quick Start Guide as an On-Ramp to the CSF 2.0 Journey

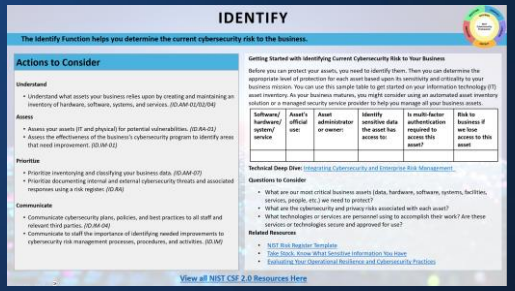

View full CSF 2.0 SMB Quick Start Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf

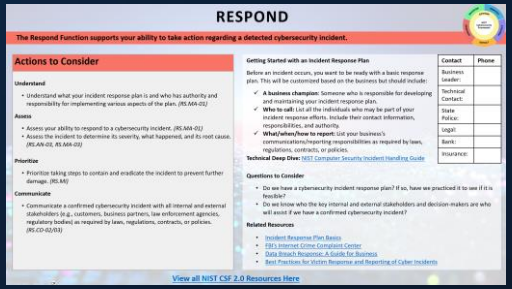
# Creation of CSF 2.0 SMB QSG

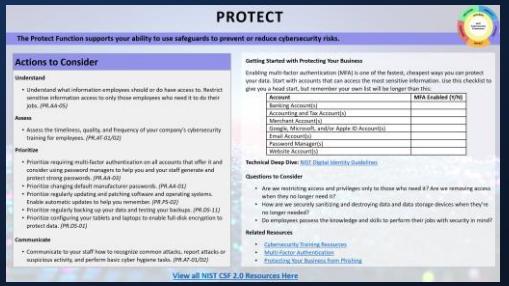
- There was a clear desire for an actionable, accessible CSF resource for smaller entities.
- Not limited to only small businesses.
- Leveraging Implementation Examples as content for “Actions to Consider.”
- Focus on usability and readability.
- Focus on  a limited number of high priority items that an under-resourced organization can implement.

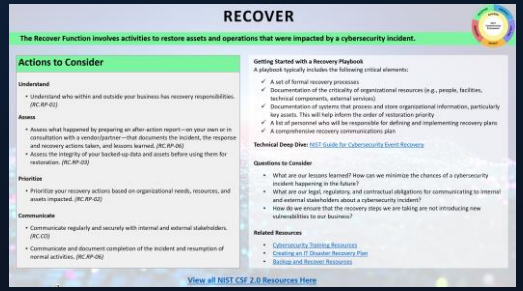



NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

# GOVERN


**The Govern Function helps you establish and monitor your business's cybersecurity risk management strategy, expectations, and policy.**

## Actions to Consider

**Understand**

- Understand how cybersecurity risks can disrupt achievement of your business's mission. *(GV.OC-01)*
- Understand your legal, regulatory, and contractual cybersecurity requirements. *(GV.OC-03)*
- Understand who within your business will be responsible for developing and executing the cybersecurity strategy. *(GV.RR-02)*

**Assess**

- Assess the potential impact of a total or partial loss of critical business assets and operations. *(GV.0C-04)*
- Assess whether cybersecurity insurance is appropriate for your business. *(GV.RM-04)*
- Assess cybersecurity risks posed by suppliers and other third parties before entering into formal relationships. *(GV.SC-06)*

**Prioritize**

- Prioritize managing cybersecurity risks alongside other business risks. *(GV.RM-03)*

**Communicate**

- Communicate leadership's support of a risk-aware, ethical, and continually improving culture. *(GV.RR-01)*
- Communicate, enforce, and maintain policies for managing cybersecurity risks. *(GV.PO-01)*

**Getting Started with Cybersecurity Governance**

You can use these tables to begin thinking about your cybersecurity governance strategy.

| Setting Organizational Context | |
|---|---|
| Our business mission statement: | |
| What cybersecurity risks may prevent us from achieving this mission? | |

| Documenting Cybersecurity Requirements | |
|---|---|
| List your legal requirements: | |
| List your regulatory requirements: | |
| List your contractual requirements: | |

**Technical Deep Dive:** Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight

**Questions to Consider**

- As our business grows, how often are we reviewing our cybersecurity strategy?
- Do we need to upskill our existing staff, hire talent, or engage an external partner to help us establish and manage our cybersecurity plan?
- Do we have acceptable use policies in place for business and for employee-owned devices accessing business resources? Have employees been educated on these policies?

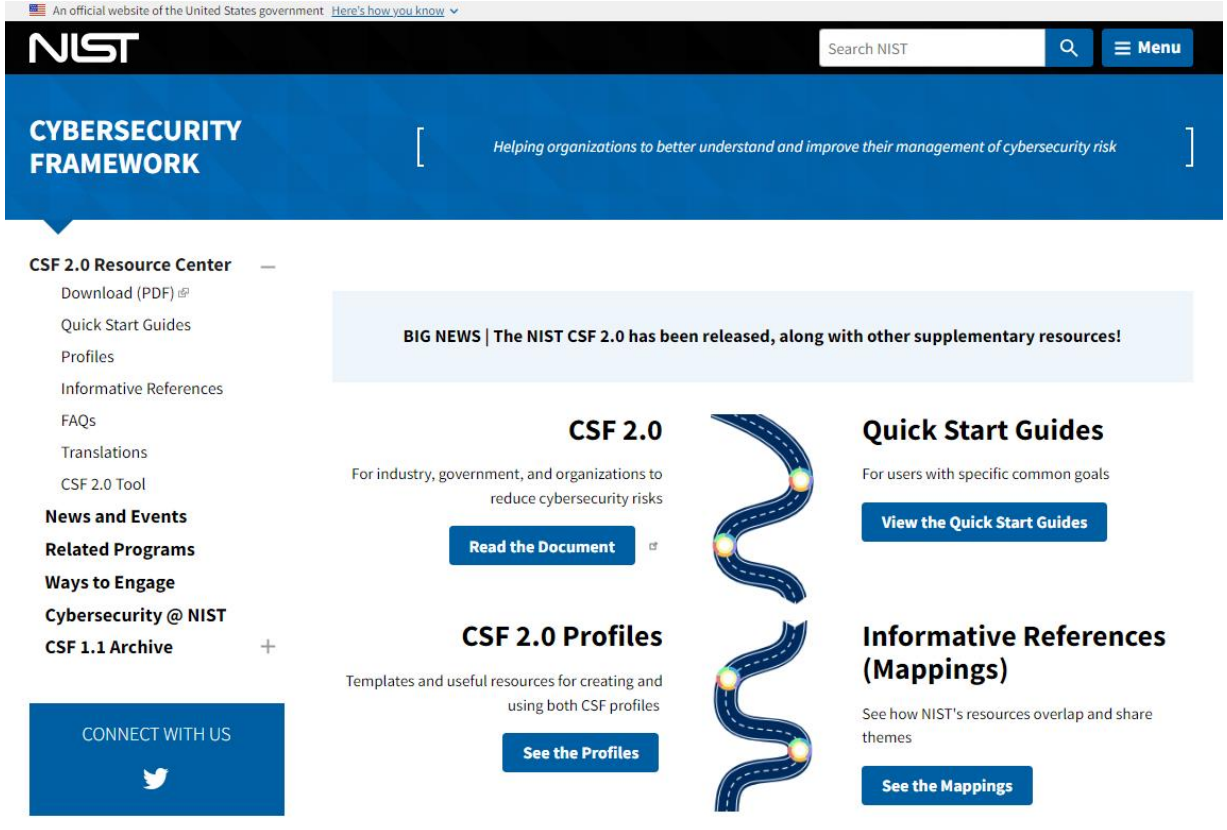
**Related Resources**

- Securing Small and Medium-Sized Supply Chains Resource Handbook
- Choosing A Vendor/Service Provider

View all NIST CSF 2.0 Resources Here

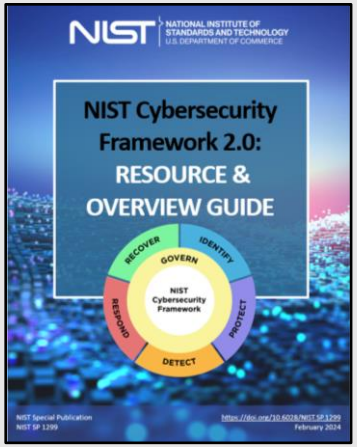

# Additional CSF 2.0 Resources

# CSF 2.0 Resource Library

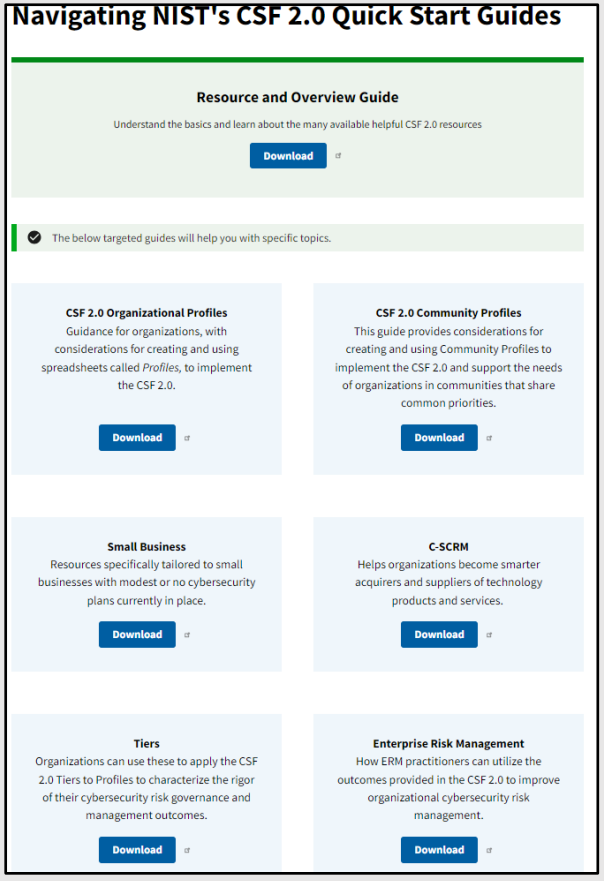


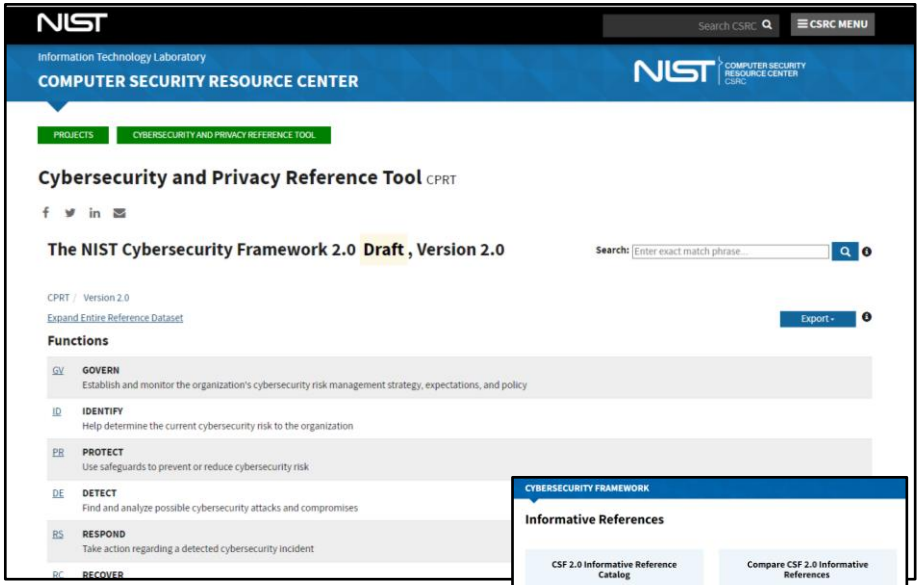

**View the CSF 2.0 Resource Library:** https://nist.gov/cyberframework

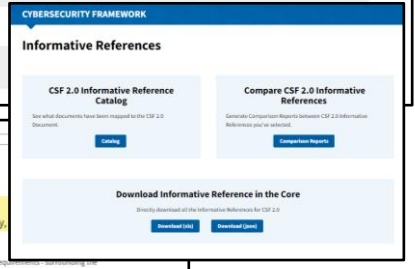
# Explore Other CSF 2.0 Resources

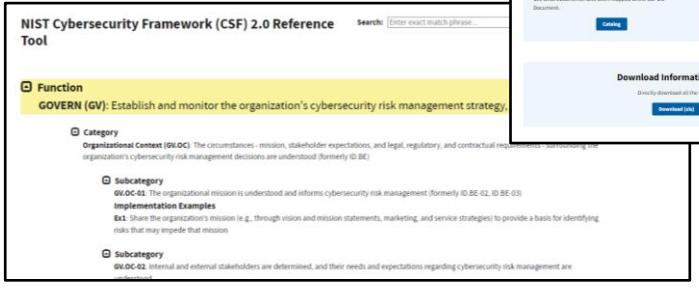





# Resources

| Quick Links | Contact Information |
|---|---|
| **CSF 2.0 Website:**<br>https://www.nist.gov/cyberframework<br><br>**CSF 2.0 FAQs:**<br>https://www.nist.gov/faqs | cyberframework@nist.gov |
| **Framework Resource Center-Community Profiles:**<br>https://www.nccoe.nist.gov/framework-resource-center<br><br>**Guide to Creating Community Profiles:**<br>https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.32.ipd.pdf | framework-profiles@nist.gov |
| **CSF 2.0 Small Business Quick Start Guide:**<br>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf | smallbizsecurity@nist.gov |
| **CSF 2.0 Cybersecurity Supply Chain Risk Management (C-SCRM) Quick Start Guide:**<br>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf | scrm-nist@nist.gov |
| **National Online Informative References Program (OLIR)-Mappings:**<br>https://csrc.nist.gov/projects/olir & https://csrc.nist.gov/Projects/olir/derived-relationship-mapping#/ | olir@nist.gov |
| **Cybersecurity and Privacy Reference Tool (CPRT):**<br>https://csrc.nist.gov/Projects/cprt - | cprt@nist.gov |
| **NIST International Cybersecurity and Privacy Resources:**<br>https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources | intl-cyber-privacy@nist.gov |

# How to Get Involved

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

# How to Get Involved

- **Join the NCCoE CSF 2.0 Community Profiles Community of Interest:** https://www.nccoe.nist.gov/framework-resource-center
- **Join a Small Business Cybersecurity Community of Interest:** https://www.nist.gov/itl/smallbusinesscyber/get-engaged
- **Submit resources.** These can include Profiles, Translations, Mappings, and more.
- **Sign up for CSF email alerts:** https://public.govdelivery.com/accounts/USNIST/subscriber/new
- **Send us a note:** cyberframework@nist.gov

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

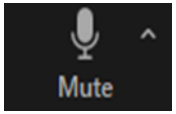
# Thank You for Joining Us Today!

**FOR FURTHER INFORMATION AND/OR QUESTIONS ABOUT THE CYBERSECURITY FRAMEWORK:**

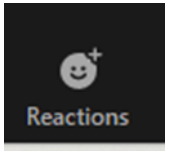
cyberframework@nist.gov

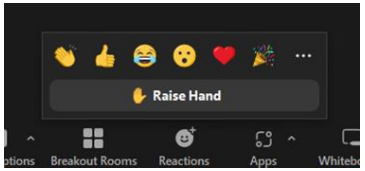
# Questions

- **Mute** when not speaking.

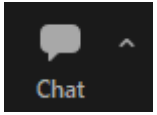



- If you do speak, share your name and agency.
- Raise your hand to speak.




- **Use the chat box to ask questions** or to share links and information.




American Public Transportation Association

# Resources

| Quick Links | Contact Information |
|---|---|
| **CSF 2.0 Website:**<br>https://www.nist.gov/cyberframework<br><br>**CSF 2.0 FAQs:**<br>https://www.nist.gov/faqs | cyberframework@nist.gov |
| **Framework Resource Center-Community Profiles:**<br>https://www.nccoe.nist.gov/framework-resource-center<br><br>**Guide to Creating Community Profiles:**<br>https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.32.ipd.pdf | framework-profiles@nist.gov |
| **CSF 2.0 Small Business Quick Start Guide:**<br>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf | smallbizsecurity@nist.gov |
| **CSF 2.0 Cybersecurity Supply Chain Risk Management (C-SCRM) Quick Start Guide:**<br>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf | scrm-nist@nist.gov |
| **National Online Informative References Program (OLIR)-Mappings:**<br>https://csrc.nist.gov/projects/olir & https://csrc.nist.gov/Projects/olir/derived-relationship-mapping#/ | olir@nist.gov |
| **Cybersecurity and Privacy Reference Tool (CPRT):**<br>https://csrc.nist.gov/Projects/cprt - | cprt@nist.gov |
| **NIST International Cybersecurity and Privacy Resources:**<br>https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources | intl-cyber-privacy@nist.gov |

# APTA Security Standards

https://www.apta.com/research-technical-resources/standards/security/


American Public Transportation Association

# PT ISAC

## Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION


American Public Transportation Association

# Thanks for attending


phanson@apta.com
703-505-2523

Polly Hanson
Senior Director Security, Risk and
Emergency Management
American Public Transportation Association


American Public Transportation Association