Cybersecurity Awareness for Transit Agencies Webinar

Federal Transit Administration

Office of Transit Safety and Oversight

10/28/2025

U.S. Department of Transportation
Federal Transit Administration

Toby Rao

Program Analyst

Office of Transit Safety and Oversight

U.S. Department of Transportation
Federal Transit Administration

Agenda

- CATT Tool Demo
- Cybersecurity Event Reporting
- Transit Cybersecurity Framework Community Profile
- Available Resources
- Q&A

CYBERSECURITY ASSESSMENT TOOL FOR TRANSIT AGENCIES

Sam Yimer

Office of Infrastructure and Asset Innovation

U.S. Department of Transportation
Federal Transit Administration

Cybersecurity Assessment Project

- From 2021-23, FTA worked with MetroLINK (Quad Cities area, Illinois) and its partners to assess cybersecurity risk and readiness for the transit industry
- The project used MetroLINK as a real-world setting in developing a cybersecurity assessment tool customized for transit (CATT)
- CATT is based on Dept. of Homeland Security's Cyber Resilience Review (CRR) and aligns with National Institute of Standards and Technology (NIST) Cybersecurity Framework

Tool Review and Launch

- **Cybersecurity Assessment Tool for Transit (CATT)** – Development and Demonstration 2021-2022
    - Tool reviewed by the industry - TSA, CISA, NRTAP, APTA, CTAA, N-CATT, AECOM, RTD Denver, Easterseals, SYSUSA, etc.
- **Tool launch on FTA Cybersecurity Page 2/10/2023** – https://www.transit.dot.gov/research-innovation/cybersecurity-assessment-tool-transit-catt
- **FTA hosted a Webinar for transit industry 3/1/2023** – Webinar Recording, Webinar Q&A

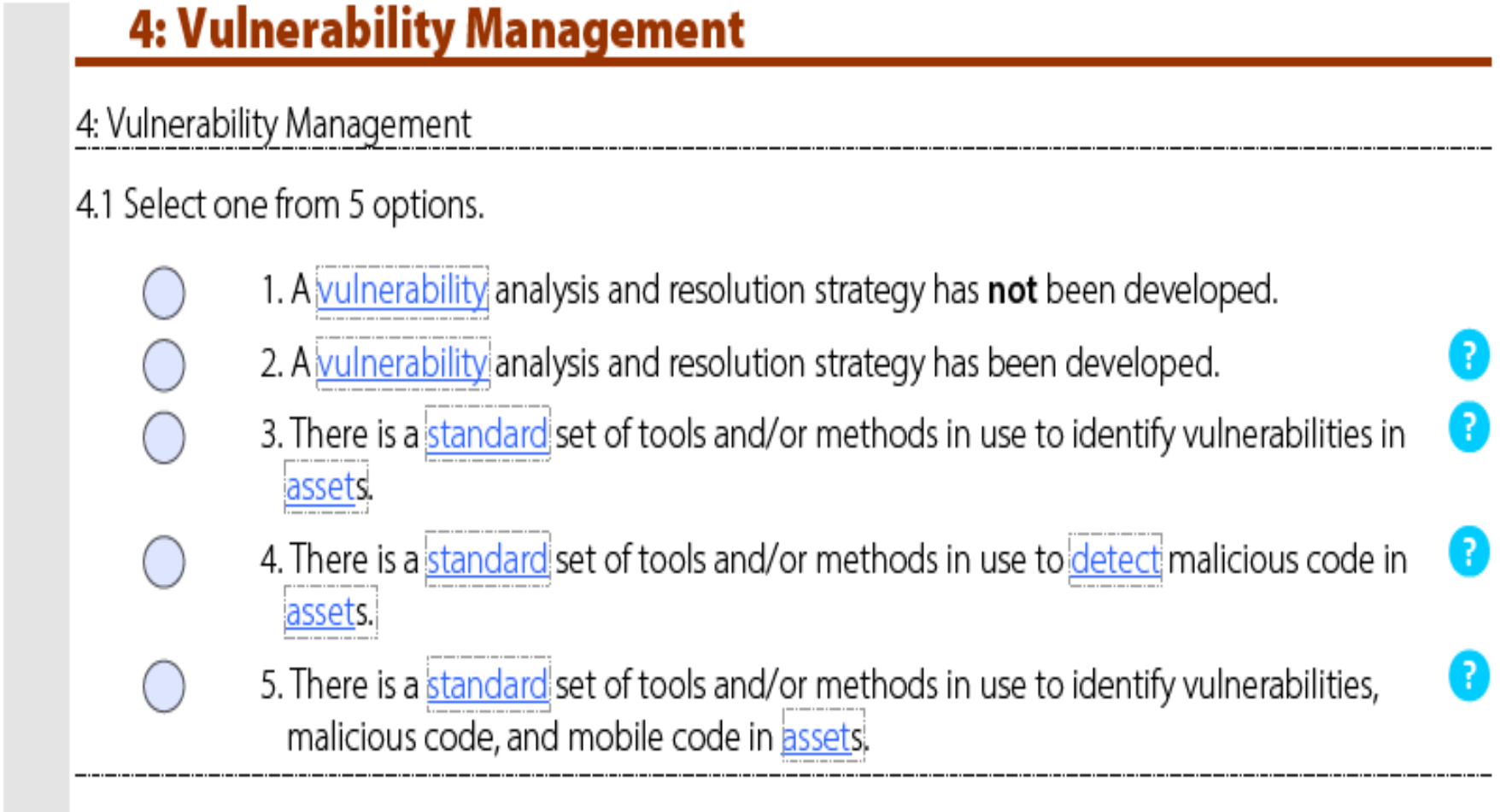
Assessment Process

Tool contains three primary components

- Data collection form
- Resulting report after data input by agency
- Resource guide on how to begin practices not yet started in each domain

Assessment Examples - next slide → → →

CATT Assessment (Input)



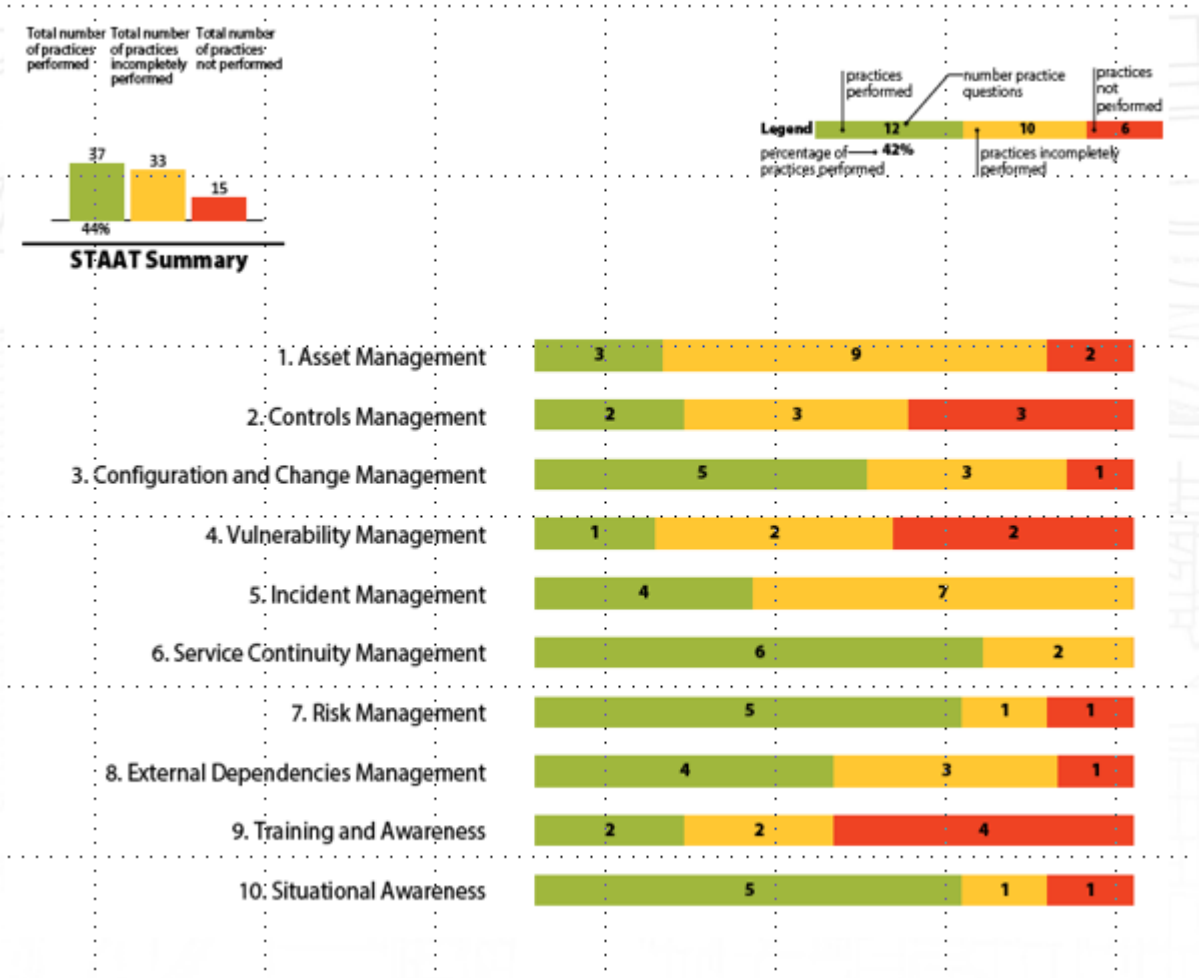
Select one of the bullets that best fits your organization

Key words can be clicked on for definitions

Provides info on how each relates to the NIST CSF

CATT Performance Summary (Output)

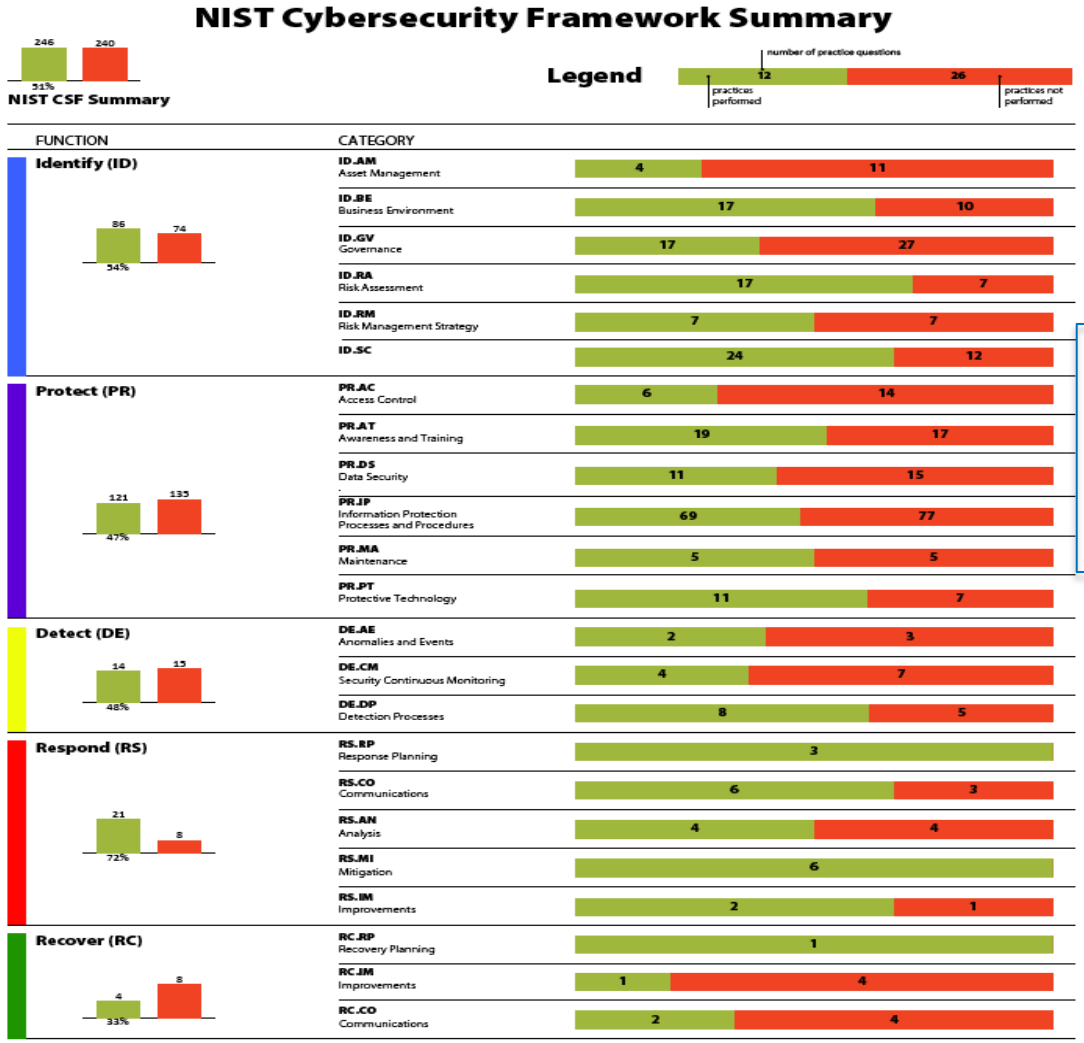
10 domains measured



Overview of practices performed under 1-10 domains

NIST CSF Overview (EXAMPLE)

5 NIST Cybersecurity Framework (NIST CSF 1.0).



Allows agencies to align results with other cybersecurity tools and resources available.

Concluding Remarks

CATT has been found to be useful by small and mid-size transit agencies

- Published by FTA for a free download (~ 3000 visits to date)
- Open-Source PDF File
- Stakeholders and users can modify the CATT tool, and repurpose it based on their need and applicability

Chelsea Champlin

Program Manager, National Transit Database

Office of Budget and Policy

U.S. Department of Transportation
Federal Transit Administration

FTA Cybersecurity Event Reporting

What's the National Transit Database?

FTA program that collects, validates, and publishes information about public transit in the U.S.

What's *cybersecurity* have to do with it?

A cybersecurity event is one system security event type reportable to the NTD.

What do I need to know?

Full reporters provide detailed data throughout the calendar year using the S&S-40, including reportable cybersecurity events.

Recent Reporting Clarifications

Infrastructure: it's not just physical!

- Transit related information, computer, and telecommunications systems that exist in transit facilities

Information Technology: it's not mode-limited!

- Cybersecurity events affect transit systems as a whole

Disrupting Operations: it may be substantial damage!

- Affects the normal operations of transit facilities, personnel, information, computer, or telecommunications systems associated with transit agencies

Additional Resources

For more information:

- 2025 NTD Safety and Security Reporting Policy Manual
- Federal Register Notice (10/31/2024) and Response to Comments (07/10/2025)
- Upcoming NTD courses and webinars offered with National Transit Institute

For technical assistance:

- Contact your NTD Safety Validation Analyst
- Contact the NTD Operations Center at NTDHelp@dot.gov
- Contact the FTA IT Help Desk at FTAITHelpDesk@dot.gov

Jeremy Furrer

Division Chief, Office of Safety Policy

Office of Transit Safety and Oversight

U.S. Department of Transportation
Federal Transit Administration

What We Will Cover

Development of a National Institute for Standards and Technology (NIST) Transit Cybersecurity Framework (CSF) 2.0 Community Profile:

- What are NIST CSF Community Profiles?
- Purpose and Value of the NIST Transit CSF 2.0 Community Profile.
- Key Elements of the Initial Public Draft.
- Current Status of the NIST Transit CSF 2.0 Community Profile.

What are NIST CSF Community Profiles?

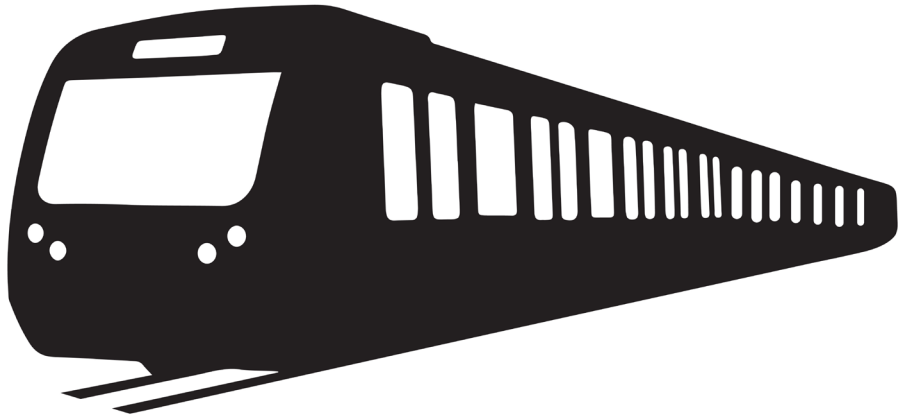
- NIST's CSF 2.0 provides organizations with guidance to manage cybersecurity risks.

- Communities are multiple organizations that share a common context and an interest in their cybersecurity posture—such as a sector or subsector (e.g., transit).

- NIST CSF Community Profiles describe CSF outcomes to address shared interests and goals among multiple organizations.

Purpose and Value of the NIST Transit CSF 2.0 Community Profile

- Community profiles, such as the Transit profile:
  - Inform development of cybersecurity strategies and planning for organizations in the community.
  - Enhance community reputation for strong, shared cybersecurity priorities and practices.
  - Foster collaboration and communication across the community.
- The Transit Community profile will provide a baseline set of minimal cybersecurity practices for mitigating described threats and vulnerabilities tailored to the specialized characteristics and needs of the transit community.



Key Elements of the Initial Public Draft

- Many of the critical systems that enable transportation services are becoming more digital and network-based, expanding the cyber-attack surface.
- Key transit challenges identified include:
  - Safety-critical control systems with regulatory constraints,
  - Long-lived legacy assets incompatible with modern controls,
  - Need to integrate cybersecurity into an existing safety-centric culture, and
  - Complex vendor/supply chain dependencies.
- Community priorities are outlined across four strategic focus areas:
  - Transit operations and ridership (reliability, safety),
  - Protection and management of transit assets (data, IT/OT protection),
  - Stakeholder coordination (collaboration, supply chain security), and
  - Organizational development (innovation, workforce/culture).

Status Update on NIST Transit Cyber Profile

- NIST released an initial public draft for public comment (August 20 - September 19, 2025) inviting stakeholder input to inform a full draft NIST Transit CSF 2.0 Community Profile.

- NIST requested input on the unique technical challenges of security in the transit sector; transit community priorities; and the set of standards, guidelines, and practices that address the needs of securing the transit ecosystem.

- **Current Status:** NIST is reviewing input received during recent comment period.

Questions

U.S. Department of Transportation
Federal Transit Administration

Thank You

Toby Rao

tobias.rao@dot.gov

Chelsea Champlin

chelsea.champlin@dot.gov

Sam Yimer

samuel.yimer@dot.gov

Jeremy Furrer

jeremy.furrer@dot.gov

U.S. Department of Transportation
Federal Transit Administration