CYBERSECURITY CONSIDERATIONS FOR TRANSIT INFRASTRUCTURE

VIRGINIA TRANSIT ASSOCIATION

2025 Annual Conference & Expo

May 28, 2025

Michael Baker INTERNATIONAL | *We Make a Difference*

VIRGINIA TRANSIT ASSOCIATION

The Voice of Public Transportation in Virginia

WHO AM I?

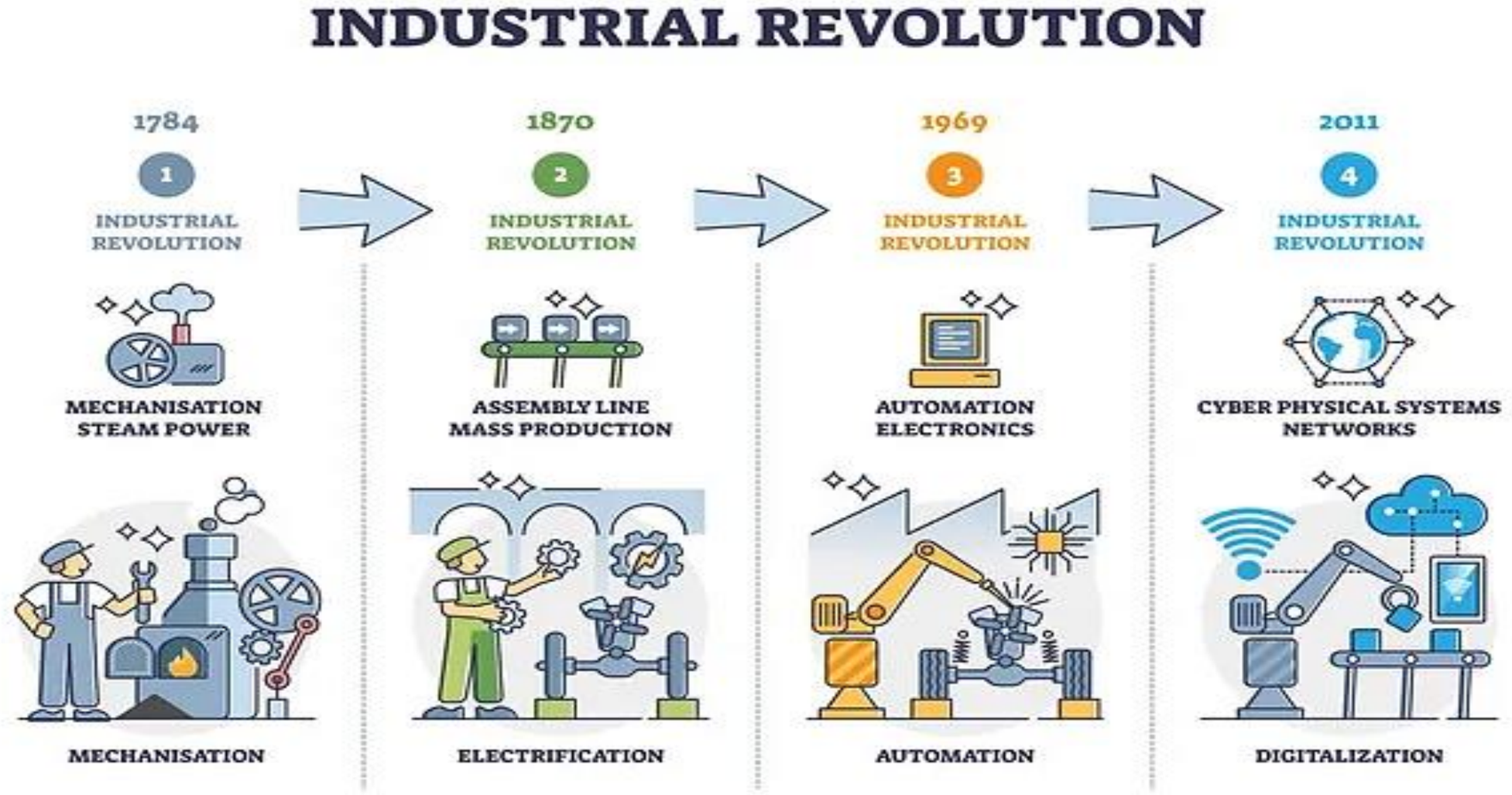
Susan Howard
VP ICS/OT Cybersecurity
Michael Baker International

- 10 years *Active-Duty United States Air Force* Telecomm and Cryptography
- 10 years University Network and Security Manager, *University of New Mexico main campus and hospital and healthcare center*
- **10 years Light Rail Systems Engineer (***Hatch (LTK) CH2M, Jacobs, Michael Baker International***)**
- 5 Years *Intel Corporation* Internet of Things (IoT) and Factory Automation
- 10 years ICS/OT Cybersecurity Consulting currently with **Michael Baker International Inc.**

CYBERSECURITY IN TRANSIT
WHAT DOES THIS MEAN?

"Technologies and Policies used to protect digital assets *(e.g., data, software, networks, hardware) from unauthorized access, exploitation, damage, or loss."*

CYBERSECURITY IN TRANSIT
PART OF THE 4TH INDUSTRIAL REVOLUTION

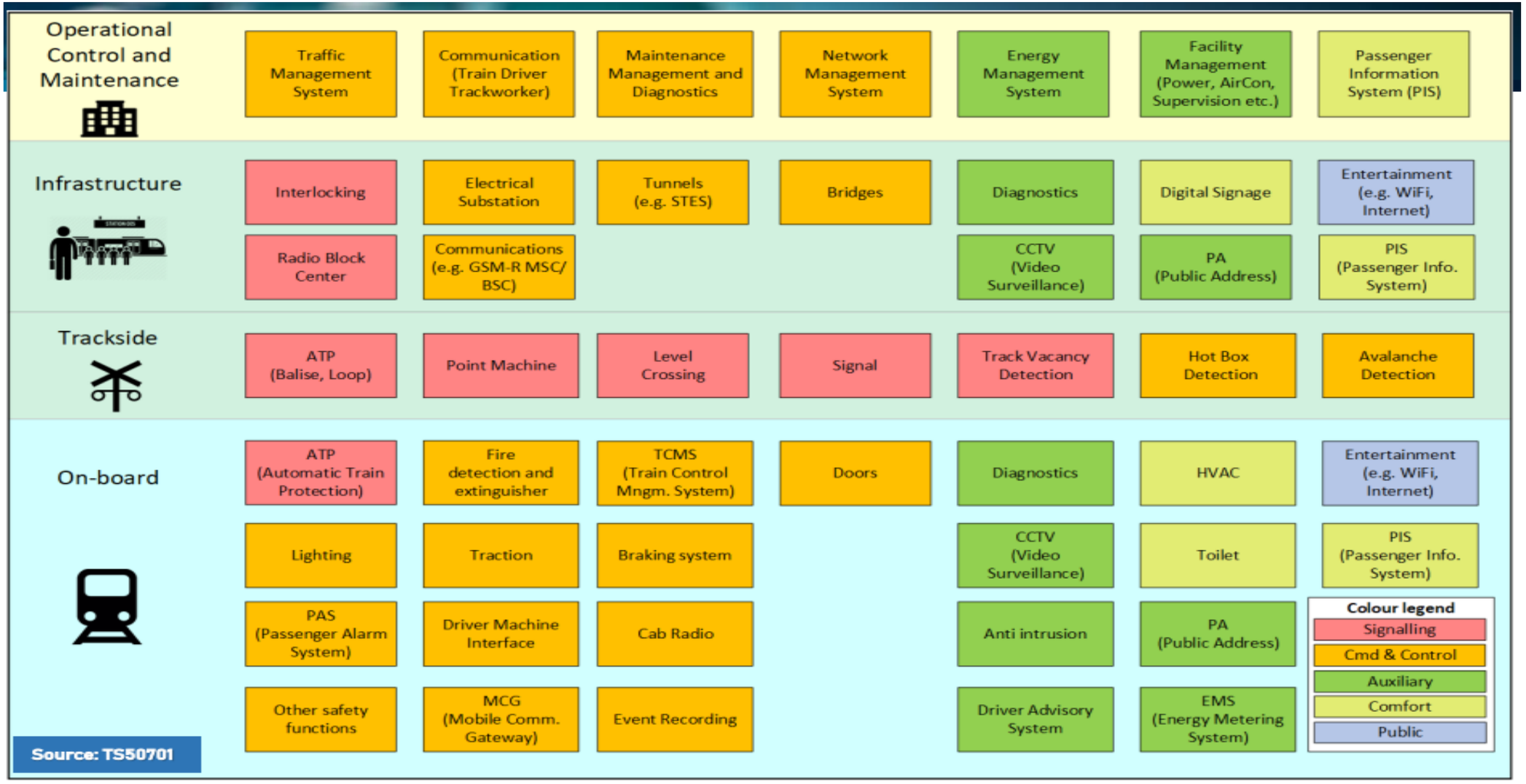


CYBERSECURITY IN TRANSIT
NOT JUST AN IT PROBLEM ANYMORE

- Open and Closed Loop Fare Systems
- Micro Transit (*Think GRTC LINK*)
- Light Rail Vehicles, Signals and Power
- Bus Dispatch
- Computer Aided Dispatch Automated Vehicle Location (CAD/AVL)
- Operations Control Centers
- Transportation Systems Management Operations (TSMO)
- Artificial Intelligence

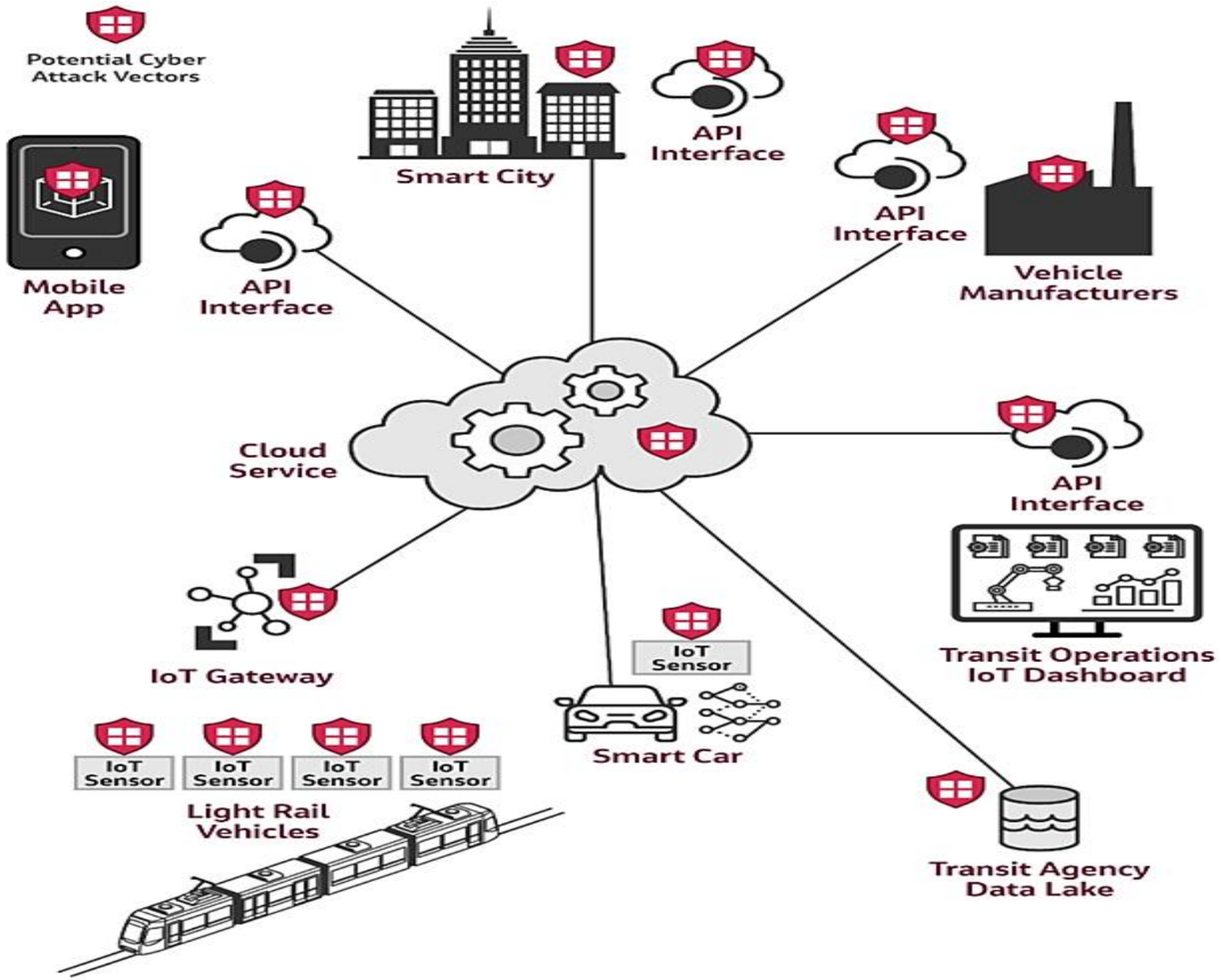
- CCTV Cameras
- Electric Bus (*Think Blacksburg Transit*)
- Advanced Traffic Management Systems (ATMS)
- Traffic Signal Controllers
- Intelligent Transportation Systems
- Passenger Information Systems
- Web Based Trip Planning
- Radio Systems
- Tunnel Systems

MANY TECHNOLOGIES MUST BE SECURED FOR A RAIL SYSTEM



CYBERSECURITY IN TRANSIT
NOT JUST AT IT PROBLEM ANYMORE

UBIQUITOUS CONNECTIVITY – EVERYTHING EVERYWHERE ALL AT ONCE



ACRONYM SOUP TERMS TO KNOW

- **API** – Application Program Interface
- **CVE** – Common Vulnerability and Exposure
- **CVSS** – Common Vulnerability Scoring System
- **IPS/IDS** – Intrusion Prevention System/Intrusion Detection System
- **ISAC** – Information Sharing and Analysis Center

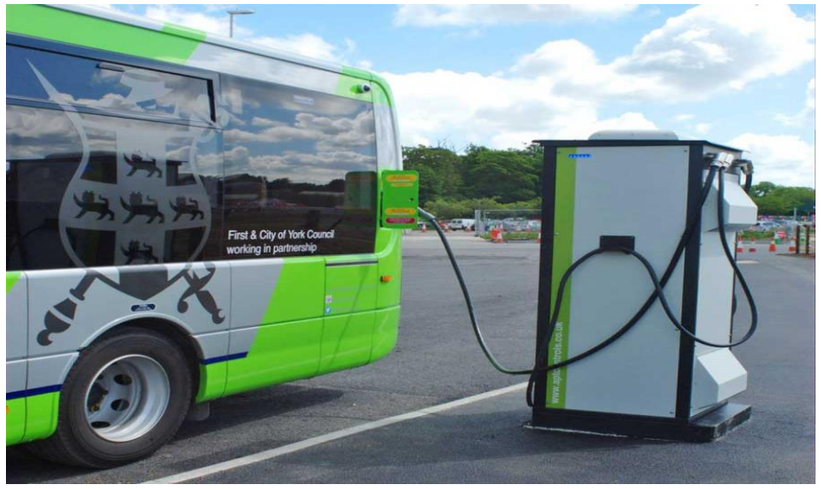
- **IoT –** Internet of Things
- **IT** – Information Technology
- **ITS** – Intelligent Transportation Systems
- **OT** – Operational Technology
- **SIEM** – Security Incident and Event Management
- **SOC** – Security Operations Center
- **TTX** – Tabletop Exercise

CYBERSECURITY IN TRANSIT IT, IoT, OT WHAT'S THE DIFFERENCE?

Laptops and Desktops

Fare Systems – Photo Courtesy Minneapolis Metro

Data Centers



Electric Bus Charging Systems – Photo Courtesy Siemens

CYBERSECURITY IN TRANSIT IT AND OT WHAT'S THE DIFFERENCE?

SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
ANTIVIRUS & MOBILE CODE COUNTER-MEASURES	Common & widely used	Can be difficult to deploy
SUPPORT TECHNOLOGY LIFETIME	3 to 5 years	Up to 40+ years
OUTSOURCING	Common/widely used	Rarely used (vendor only)
APPLICATION OF PATCHES	Regular/ scheduled	Slow (vendor specific, compliance testing required)
CHANGE MANAGEMENT	Regular/ scheduled	Legacy based – unsuitable for modern security

SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
TIME CRITICAL CONTENT	Delays are usually accepted	Critical due to safety
AVAILABILITY	Delays are usually accepted	24 x 7 x 365 x forever (Integrity also critical)
SECURITY AWARENESS	Good in both private and public sector	Generally poor inside the control zone
SECURITY TESTING/ AUDIT	Scheduled and mandated	Occasional testing for outages / audit for event recreation
PHYSICAL SECURITY	Secure	Traditionally good

Source: U.S. Department of Homeland Security

TRANSPORTATION IS CRITICAL INFRASTRUCTURE

Transportation Systems Sector

Moving millions of people and goods across the country every day, CISA protects the transportation systems sector from a limitless number of threats and risks to ensure a continuity of operations.

CISA CYBER+INFRASTRUCTURE

CYBERSECURITY IN TRANSIT
SAMPLING OF CYBER ATTACKS IN 2024

Metro Transit Cyber Attack **2023 freezes systems In St Louis, MO**

Oahu Transit TheBus attack shuts down service and compromises rider data **2024**

Kansas City Area Transportation Authority
2024 Ransomware Attack

Pittsburgh transit agency victim of ransomware attack **Pittsburgh Regional Transit 2024**

CYBERSECURITY IN TRANSIT

INFORMATION SHARING ANALYSIS CENTERS(ISACs)

ISACs came about in the late 1990s as result of PDD-63 to collect and disseminate threat, risk, and vulnerability information for critical infrastructure sectors. ISACs are non-profits, typically 24/7/365 providing sector specific information with demonstrated success in incident response, threat mitigation, and risk reduction in each sector. https://www.nationalisacs.org/about-isacs

ST-ISAC – Surface Transportation ISAC; **PT-ISAC** – Passenger Transportation ISAC;

OTRB-ISAC – Over The Road Bus ISAC https://surfacetransportationisac.org/

MS-ISAC – Multi-State ISAC is open free of charge to all U.S., State, Local, Tribal, and Territorial governments for assistance with cybersecurity threat prevention, mitigation, incident response, and information dissemination. https://www.cisecurity.org/ms-isac

Auto-ISAC – Automotive ISAC developed to collectively enhance vehicle cybersecurity. Requires application for full membership. Guest memberships open, full memberships limited to automobile industry at this time. https://automotiveisac.com/

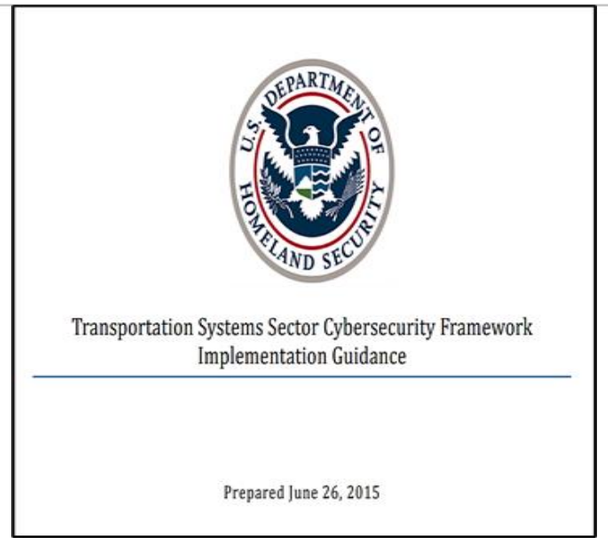
CYBERSECURITY PLANNING, POLICY, AND RESOURCES

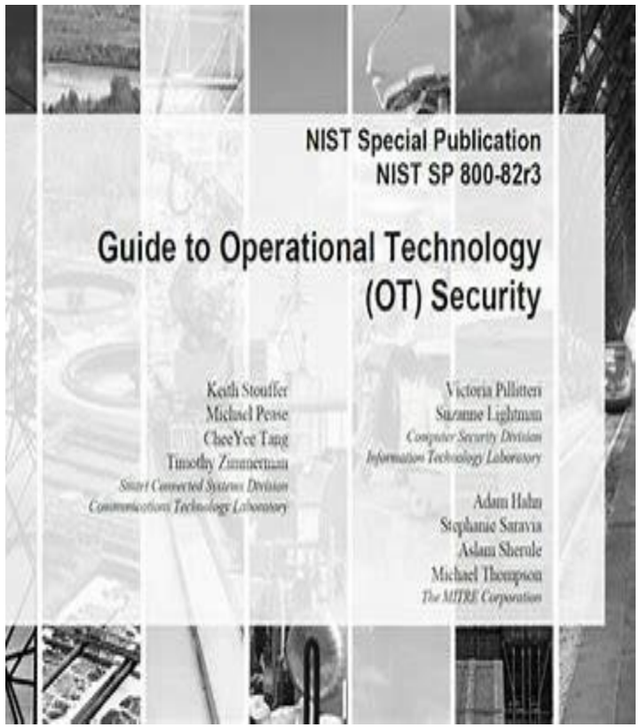
INCLUDE CYBERSECURITY AS PART OF STRATEGIC PLANNING

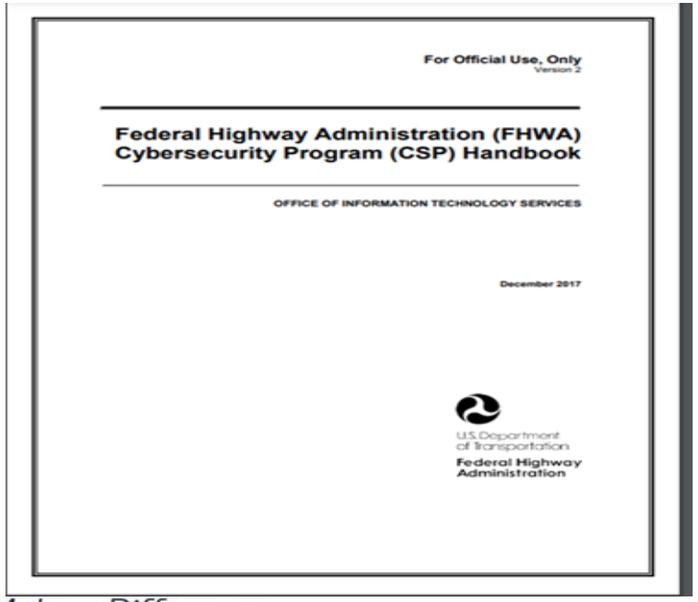
To add cybersecurity into transit planning, consider the following:

- **Self Audit** - Use the **Cybersecurity Assessment Tool (CATT)** published by FTA to identify risks and develop a Risk Register for your planning purposes.
- **Risk Register** - Address physical and cybersecurity risks relevant to the transportation mode and project type and scale. **Include the Risk Register in your Transit Development Plan or Strategic 10 Year Plan.**
- **APTA** - Develop cybersecurity strategies for your organization based on the **American Public Transportation Association's (APTA) guidelines.**
- **CSET** - Utilize the **Cyber Security Evaluation Tool (CSET®)** from the Department of Homeland Security to identify risks for key cyber assets.
- **3rd Party Audit** - Ensure quick recovery after a cyber incident by **commissioning an independent cyber audit.**

CYBERSECURITY IN TRANSIT
RESOURCES







FTA CATT TOOL IS FREE

Online Here: CATT-Self-Assessment-Package.zip

Cybersecurity Assessment Tool for Transit (CATT)

FTA published an open-source CATT tool on February 10, 2023, which assists small and mid-sized transit agencies in self-assessing their cybersecurity preparedness

CATT has three primary components:

- Data collection form
- Resulting report produced given data input from transit agency
- Resource guide on how to begin practices

CATT provides an on-ramp for agencies to identify key practices of a modern cybersecurity program with a self-assessment that uses Department of Homeland Security's Cyber Resilience Review as a basis and aligns with National Institute of Standards and Technology framework

Cybersecurity Resources for Transit Agencies

Courtesy WWW.FTA.ORG

FTA DATA AND CYBERSECURITY REPORT - 2024

Online Here Cyber and Data Security (TRACS Final Report) | FTA

Transit Advisory Committee for Safety (TRACS) Cyber and Data Security Recommendations

- In February 2024, the TRACS Cyber and Data Security sub-committee released a Cyber and Data Security Report to aid FTA and USDOT leadership in improving cyber and data security.
- The report details seven recommendations, including implementation suggestions, to improve the cybersecurity hygiene for transit agencies.

Courtesy www.fta.gov

DHS CISA PROVIDES FREE CYBER SERVICES FOR ALL CRITICAL INFRASTRUCTURE

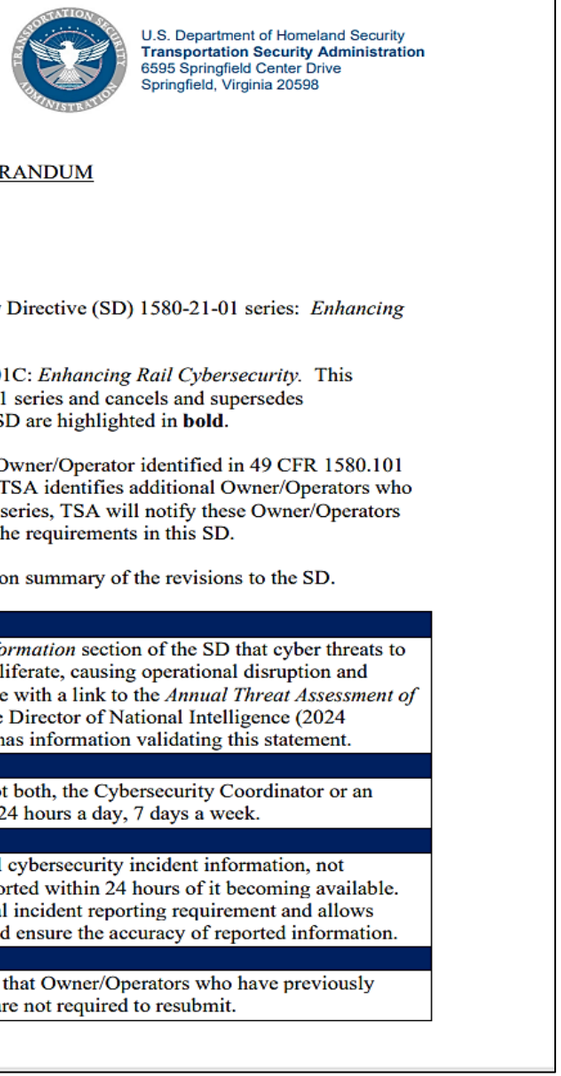
Regional office: CISARegion3@cisa.dhs.gov
Media inquiries: CISAMedia@cisa.dhs.gov
After hours: Central@cisa.gov
Organizations can also report anomalous cyber activity and/or cyber incidents 24/7 to SayCISA@cisa.dhs.gov or by calling 1-844-Say-CISA (1-844-729-2472).
https://www.cisa.gov/about/regions/region-3

Region 3 Director William J. Ryan

Regional Director William J. Ryan leads a cadre of security professionals located throughout the region.

LEARN MORE →

TSA CYBERSECURITY MEMORANDUM CURRENTLY IN EFFECT FOR CLASS 1 FREIGHT AND LARGE PASSENGER AGENCIES



U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

MEMORANDUM

To: Covered Railroad Owner/Operators

Date: October 22, 2024

Subject: Renewal with revisions to the Security Directive (SD) 1580-21-01 series: *Enhancing Rail Cybersecurity*

Attached to this memorandum is SD 1580-21-01C: *Enhancing Rail Cybersecurity*. This directive is a continuation of the SD 1580-21-01 series and cancels and supersedes SD 1580-21-01B. Revisions to the text of the SD are highlighted in **bold**.

The SD applies to each freight railroad carrier Owner/Operator identified in 49 CFR 1580.101 and other TSA-designated freight railroads. If TSA identifies additional Owner/Operators who were not already subject to the SD 1580-21-01 series, TSA will notify these Owner/Operators and provide specific compliance deadlines for the requirements in this SD.

The following table provides a section-by-section summary of the revisions to the SD.

Section I.
TSA is noting in the *Purpose and General Information* section of the SD that cyber threats to surface transportation systems continue to proliferate, causing operational disruption and economic harm. TSA is also adding a footnote with a link to the *Annual Threat Assessment of the U.S. Intelligence Community*, Office of the Director of National Intelligence (2024 Intelligence Community Assessment), which has information validating this statement.
Sections I.A. and II.B.3.c.
TSA is adding clarifications that either, but not both, the Cybersecurity Coordinator or an alternate must be available to TSA and CISA 24 hours a day, 7 days a week.
Section II.C.4.f.
TSA is adding clarifications that supplemental cybersecurity incident information, not available at the time of reporting, must be reported within 24 hours of it becoming available. This time duration is in keeping with the initial incident reporting requirement and allows Owner/Operators adequate time to compile and ensure the accuracy of reported information.
Section II.E.3.
This section includes new language clarifying that Owner/Operators who have previously submitted a vulnerability assessment to TSA are not required to resubmit.

CYBERSECURITY IN TRANSIT
TSA POLICY UPDATE PENDING RESOLUTION

- TSA Notice of Proposed Rule Making was issued in November 2024 with comments closed February 2025. Currently still in review between DHS and TSA

Enhancing Surface Cyber Risk Management

A Proposed Rule by the Transportation Security Administration on 11/07/2024

This document has a comment period that ends in 80 days. (02/05/2025)

19 comments received. View posted comments

PUBLISHED CONTENT - DOCUMENT DETAILS

Agencies: Department of Homeland Security
Transportation Security Administration
Agency/Docket Number: Docket No. TSA-2022-0001
CFR: 49 CFR 150049 CFR 150349 CFR 152049 CFR 157049 CFR 1580
49 CFR 158249 CFR 158449 CFR 1586
Document Citation: 89 FR 88488
Document Number: 2024-24704
Document Type: Proposed Rule
Pages: 88488-88592 (105 pages)
Publication Date: 11/07/2024
RIN: 1652-AA74

- **TSA increasing cyber and physical requirements and regulatory harmonization for Pipeline; Passenger Rail; Freight Rail; and Bus Operators**

- **Department of Homeland Security Transportation Security Administration 49 CFR Parts 1500, 1503, 1520, 1570, 1580, 1582, 1584, and 1586[Docket No. TSA-2022-0001]RIN 1652-AA74**

Source : Enhancing Surface Cyber Risk Management

TSA POLICY UPDATE PENDING RESOLUTION

What will agencies have to do?

- Hire Independent Assessors to perform cybersecurity assessments
- Develop a TSA-Approved Cybersecurity Operational Implementation Plan
- Develop and maintain an Incident Response Plan
- Train cybersecurity coordinators
- Continuous Monitoring Platforms
- Patch Management, Supply Chain Management, Plan of Action & Milestone (POA&M)
- Network Segmentation, Secure by Design; Zero Trust etc.

22

FEDERAL CYBERSECURITY GRANTS CHECK FOR CURRENT AVAILABILITY

- **Federal Grants**: https://www.fema.gov/grants/preparedness/transit-security FEMA Transit Security Grant Program was developed in FY2024

1. DHS/FEMA Transit Security Grant Program
2. NIST Cybersecurity Framework
3. FTA Urbanized Area Formula Program
4. FTA Formula Grants for Rural Areas Program
5. **FTA State of Good Repair Program (*Cybersecurity can be included*)**
6. Government and federal funding opportunities for Cybersecurity Services
7. Grants to protect critical transportation infrastructure and increase resilience.

23

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP)

- A total of 4 years of funding were appropriated for the SLCGP. The funding began in federal fiscal year (FFY) 2022 and goes through FFY2025. Each funding year has a period of performance of 48 months. Info online below. **Funding Window NOW Closed**

https://www.vita.virginia.gov/information-security/grant-programs/faqs/

- In Virginia, local governments worked with the Virginia Cybersecurity Planning Committee to receive subawards.

- **Cyber threat indicator information sharing – Funding was established to create a Virginia Information Sharing and Analysis Center (VA-ISAC).**

5 THINGS AGENCIES CAN DO FOR FREE
KEY TAKE-AWAYS

1. Develop an **Incident Response Plan** for BOTH IT and OT and PRACTICE execution via a Tabletop Exercise (TTX) with all stakeholders, internal and external

2. IT and OT must **design a defensible network using segmentation** between the IT and OT pieces of the network

3. Increase **awareness and training** with phishing exercises and annual cybersecurity training for all employees

4. Ask DHS for a **FREE cybersecurity assessment,** as part of critical infrastructure, all transit agencies are eligible.

5. **Sign up for FREE cybersecurity scanning** service from DHS CISA Region 3

CYBERSECURITY IN TRANSIT RESOURCES

Susan Howard
VP ICS/OT Cybersecurity
Susan.Howard@mbakerintl.com

VIRGINIA TRANSIT ASSOCIATION

The Voice of Public Transportation in Virginia

THANK YOU

Michael Baker INTERNATIONAL | *We Make a Difference*