

Why is Cybersecurity Important?

Ralph Volpe

Federal Highway Administration

2023 Arkansas Transportation Research Conference

May 2023



U.S. Department of Transportation
Federal Highway Administration



U.S. Department of Transportation
Federal Highway Administration

Disclaimer

Except for any statutes or regulations cited, the contents of this presentation do not have the force and effect of law and are not meant to bind the public in any way. This presentation is intended only to provide information regarding existing requirements under the law or agency policies.



Operational Benefits from Technology Deployment

- Improve health monitoring of infrastructure
- Improve operational efficiency
 - Improved mobility information
 - Quicker control ability
 - Better automation
- Improve user experiences
 - Transit arrival time
 - Travel time estimates



U.S. Department of Transportation
Federal Highway Administration

Risks from Technology Deployment

- Shorter device and system life cycle
- Increased exposure to maintenance challenges
- Cybersecurity vulnerability

HPA approved
6/7/2022



History of Attacks and Vulnerabilities

Back in the 20 th Century...	<ul style="list-style-type: none">• Homemade signal preemption kit• Hijacked Ethernet switches on broadband cable modem
Early 2000's	<ul style="list-style-type: none">• West Coast Toll tag vulnerability discovered• Portable Dynamic Message Signs hack instruction online
2010's	<ul style="list-style-type: none">• Digital parking meters vulnerabilities discovered• Transit payment system and transit vehicles vulnerabilities discovered• Public safety radio spectrum (4.9GHz) vulnerabilities discovered• Center to field network attacked• Sensors and controllers attacked, and vulnerabilities discovered• Ransomware attacks on agency enterprise systems
Early 2020's	<ul style="list-style-type: none">• Monitoring interrupted on State highway due to ransomware attack



Why is this my problem?

- **Information Technology** – IT or Technology Department
 - Email systems
 - General Internet services
- **Operation Technology** – Transportation agency's responsibility
 - Traffic signal control
 - Optimization and management software
 - Advance traveler information systems



Cybersecurity vs. Cyber Resilience

Cyber Resilience	The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources
Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks. Prevention of damage to, protection of, and restoration of <ul style="list-style-type: none">• computers,• electronic communications systems and services,• wire and electronic communication,• including information contained therein, to ensure its confidentiality, availability, integrity, authentication, and nonrepudiation.

NIST Special Publication 800-160, Volume 2, Revision 1, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach"



Classification and Motivations

- Use the right name
 - Don't call them "hackers"
 - Cyber Threat Actors present a threat
 - Security Researchers discover vulnerabilities
- Motivations Vary
 - Curiosity, bragging rights
 - Greed
 - Political causes
 - Warfare



U.S. Department of Transportation
Federal Highway Administration

All cyber attacks follow a similar cycle:



Scanning and Breaching the Perimeter



Mapping the Interior



Exploitation and Egress

HPA approved
6/7/2022



U.S. Department of Transportation
Federal Highway Administration

What Must Be Protected?

- What is your agency's mission?
- Common mission:
 - Safe operation
 - Efficient mobility
 - Trusted information

HPA approved
6/7/2022



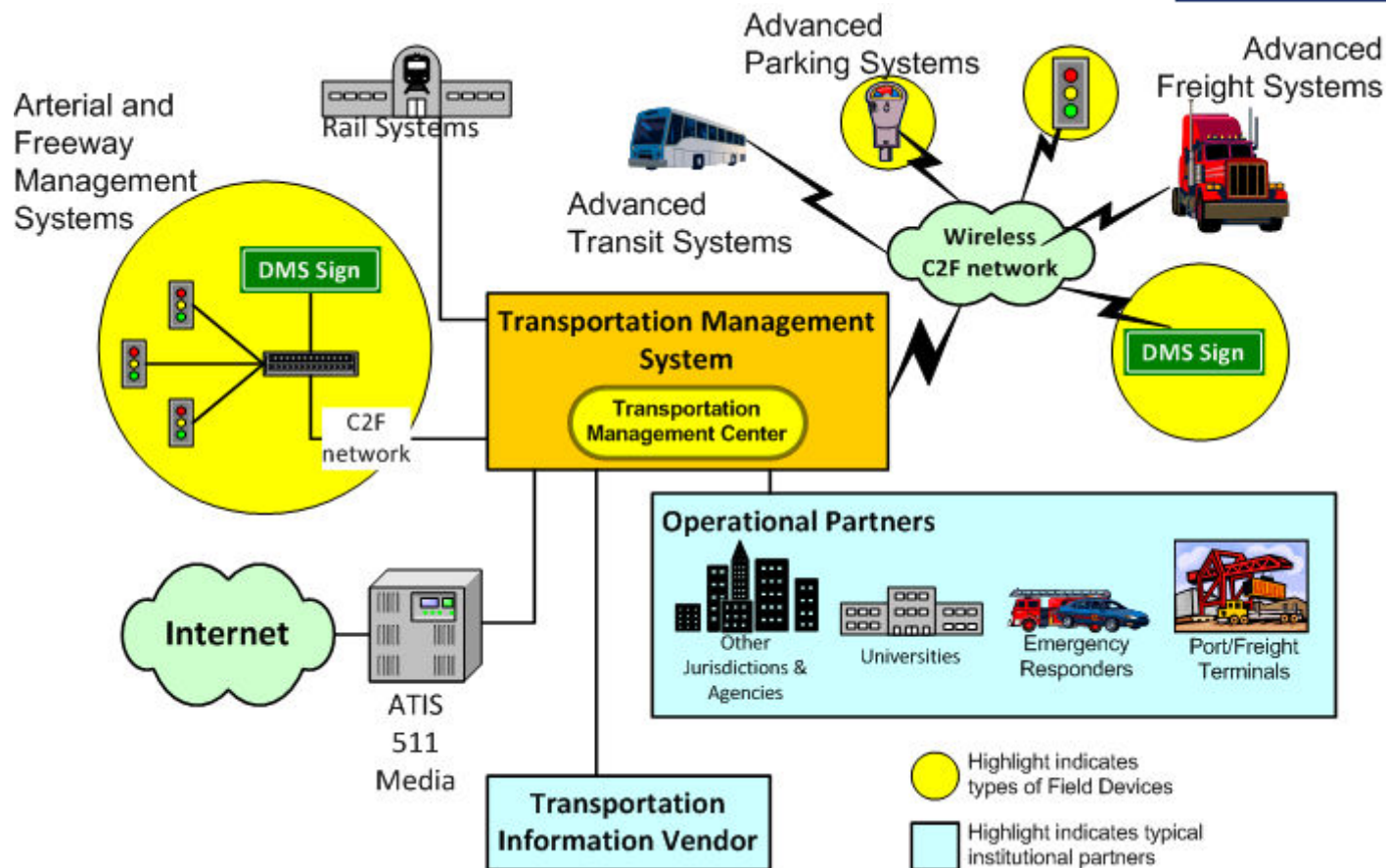
Surmountable Challenge

- Focus on delivering agency objectives
- Apply known defense concept to
 - Disrupt the “kill chain”
 - Minimize exposure of agency objectives
- Identify a sustainable level of engagement

So where are we vulnerable?



U.S. Department of Transportation
Federal Highway Administration



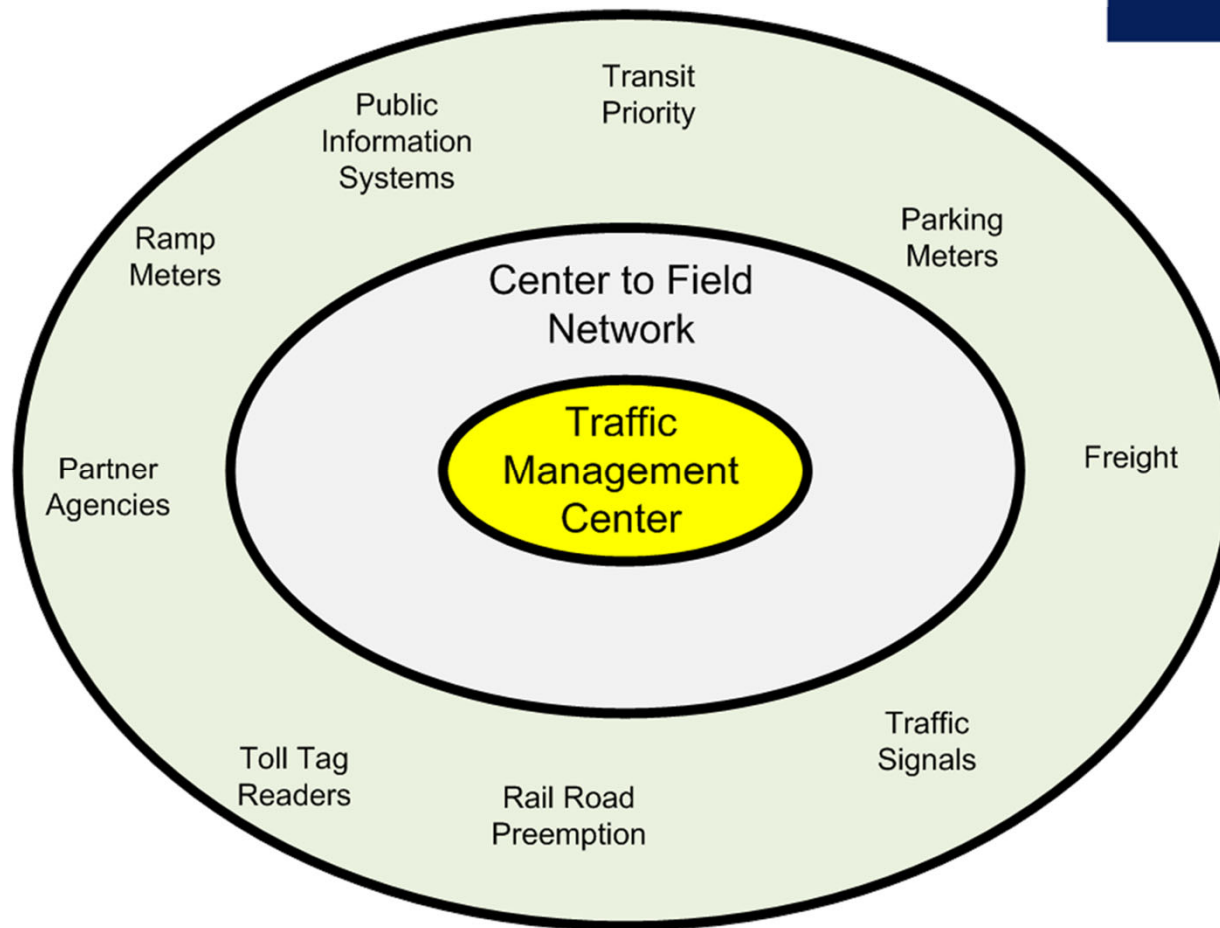
Source: USDOT

HPA approved
6/7/2022

So where are we vulnerable?



U.S. Department of Transportation
Federal Highway Administration



Source: USDOT

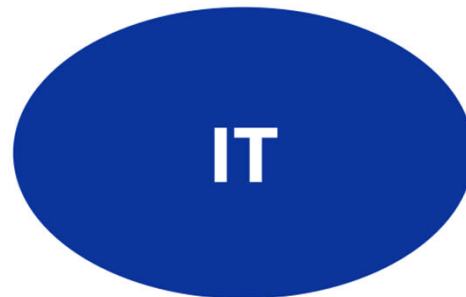
HPA approved
6/7/2022



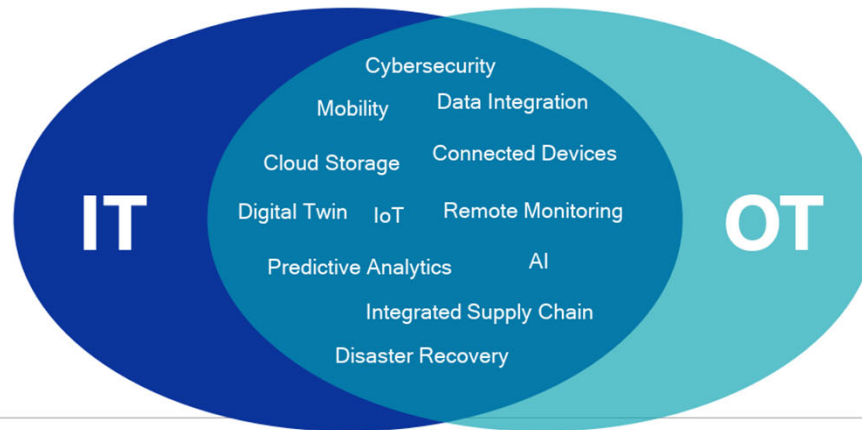
U.S. Department of Transportation
Federal Highway Administration

Information Technology (IT) vs. Operational Technology (OT)

The
Past



The
Future



(Source: M. Rao, Virginia Department of Transportation. National Operations Center of Excellence (NoCoE) Webinar Series, October 6, 2020, webinar-series-part-2-how-leverage-it-resources-improve-tsmo)

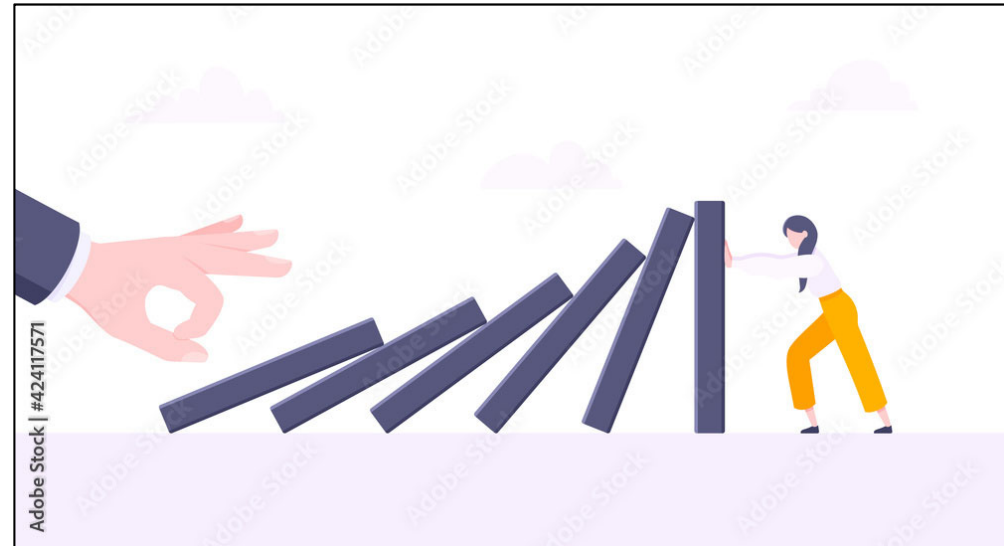
HPA approved
6/7/2022

Balancing Security and Resilience



U.S. Department of Transportation
Federal Highway Administration

- Resilience
 - The capacity to recover quickly from a fault and maintain service
 - Transportation agencies are very good at resilience
- Security – freedom from danger



HPA approved
6/7/2022



Principles of Protection

- Cyber Security Framework offers a structured approach
- Developed by National Institute of Standards and Technology

The Core Functions of the Framework:

- Identify
- Protect
- Detect
- Respond
- Recover



U.S. Department of Transportation
Federal Highway Administration

Context of an Attack

- Not all attacks are battle worthy
- Not all nuisance attacks can be ignored



Approved
322



Staff is the line between disaster and hero

- **Example** San Francisco Metropolitan Transit Authority (2016)
 - Turn a ransomware attack into “Black Friday Miracle”
 - Search Term: “San Francisco MTA ransomware 2016”
- **Example** Hawaii Emergency Operation Center (2017)
 - Turn a press opportunity into a password breach incident.
 - Search Term: “Hawaii EOC password photo”

All Protection can be Circumvented by Staff

- **Unintended Risks**
 - Poor security habits
 - Vulnerability from balancing customer service and security
- **Insider Risk**
 - Human Resources and organizational policies will be critical for insider attack



U.S. Department of Transportation
Federal Highway Administration



HPA approved
6/7/2022



Teams should be functionally cross-cutting

- **Cross-Cutting Technical Team**
 - Operational technology team
 - Information technology team
- **Internal and external communication team**
 - Keep manager informed and ready to make decisions when required
 - Allow the technical team to stay focused on technical restoration
 - Keep stakeholder and public informed and coordinated
- **Management and Human Resources**
 - Sustainable staff training and management



Presidential Executive Orders

- **Executive Order 13636** (EO 13636) Improving Critical Infrastructure Cybersecurity
- **Executive Order 13800** (EO 13800) Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- **Presidential Policy Directive 21** (PPD-21) Critical Infrastructure Security and Resilience
- **Presidential Policy Director 41** (PPD-41) U.S. Cyber Incident Coordination

Federal Regulations US Department of Transportation vs. Department of Homeland Security



U.S. Department of Transportation
Federal Highway Administration

- **USDOT does not have regulations** on transportation cybersecurity at State, Local, Tribal, and Territorial (SLTT) agencies
- Any **Federal Regulation will come from Department of Homeland Security**
 - Transportation Security Agency (TSA)
 - Cybersecurity and Infrastructure Security Agency (CISA)



U.S. Department of Transportation
Federal Highway Administration

State Laws on incident disclosure

- Each State can have its own regulation around cybersecurity
 - Privacy
 - Incident or breach disclosure
 - Consider impacts from local regulations

HPA approved
6/7/2022

23



Possible Next Steps for your Organization

- Short Term
 - Identify what's important and the regulatory landscape
- Medium Term
 - Develop physical and human assets needs
 - Create the security process based on established model such as National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Long Term
 - Keep security process current as threat changes
 - Maintain workforce competency

Improve Cybersecurity Communication

- Identify and address existing gaps in vulnerability and exploit information sharing
- A framework for communication and information sharing for vulnerabilities and incident response
- Develop of glossary of common terms
- “Transportation Cybersecurity Incident Response and Management Framework” (available from ROSA-P)



U.S. Department of Transportation
Federal Highway Administration

Transportation Cybersecurity Incident Response and Management Framework

Cybersecurity Incident Exercise
Summary Report

May 2021



Transportation Cybersecurity Incident Response and Management Framework

Final Report

July 2021



Source: USDOT

HPA approved
6/7/2022

Intelligent Transportation Systems Penetration Testing Guide

- Methodology of scoping a test: type, management, and test readiness
- Template test plan for your own penetration testing
- “Cybersecurity and Intelligent Transportation Systems – A Best Practice Guide” (source: ROSA-P)



U.S. Department of Transportation
Federal Highway Administration

Cybersecurity and Intelligent Transportation Systems

A Best Practice Guide

www.its.dot.gov/index.htm
Best Practice Guide – September 17, 2019
Publication Number: FHWA-JPO-19-763



U.S. Department of Transportation

Source: USDOT

HPA approved
6/7/2022

Updated National ITS Architecture



U.S. Department of Transportation
Federal Highway Administration

ARC-IT Version 9.0
The National ITS Reference Architecture

Architecture > Security > Device Classes

Device Classes

A device class, or more precisely, a device security class, is a statement of the security requirements for a device in terms of its requirements for Confidentiality, Integrity, and Availability, expressed as LOW, MODERATE, or HIGH ratings for each of the three. Within the ITS Architecture, devices are the building blocks for physical objects. So if the devices that implement a physical object collectively meet a given device class, that physical object does as well.

Device security classes are intended to be of use to a supplier of devices and systems for use in C-ITS deployments. A device can only be used to play a role in a particular application if it meets the security requirements of that role; however, higher security requirements will in general translate to more expensive devices. The concept behind the device security class is to develop collections of security requirements which suppliers can develop to, allowing them to provide the most cost-effective solutions that meet the security requirements.

Since there are three security views, there are potentially 27 (3³) different device security classes. In principle, suppliers could develop devices in each of these classes. In practice, there will likely be economies of scale in reducing the number of classes. As such, various analyses have led to the establishment of five device classes:

- Every physical object is covered by a device class that matches or exceeds its security requirements
- Every physical object is covered by a device class that exceeds its security requirements under no more than two headings

The first property ensures that physical objects meet the security requirements; the second ensures that implementations are not significantly more expensive than necessary, relative to security requirements. Device security classes are intended to be of use to suppliers of devices and systems for use in C-ITS deployments. A device can only be used to play a role in a particular application if it meets the security requirements of that role; however, higher security requirements will in general translate to more expensive devices. The concept behind the device security class is to develop collections of security requirements which suppliers can develop to, allowing them to provide the most cost-effective solutions that meet the security requirements.

There are currently five physical object device security classes defined:

Class	Confidentiality	Integrity	Availability
Class 1	LOW	MODERATE	MODERATE
Class 2	MODERATE	MODERATE	MODERATE
Class 3	MODERATE	HIGH	MODERATE
Class 4	HIGH	HIGH	MODERATE
Class 5	HIGH	HIGH	HIGH

These device security classes were derived by analyzing the requirements associated with application-combined information flows, and then combining those flows at physical object boundaries to determine matching device requirements. While this resulted in roughly one dozen device classes, a more moderate number is desirable to realize economies of scale. While additional classes may be added in the future, these five provide a baseline.

A more detailed analysis was conducted on the V2I environment that led to selection of specific security controls that should be applied to Connected Vehicle Roadside Equipment (CVRSE), ITS Roadway Equipment (ITRE), and Vehicle OBEs. These controls can be seen from the following:

Class 1 controls for CVRSE, ITRE, Vehicle OBE
 Class 2 controls for CVRSE, ITRE, Vehicle OBE
 Class 3 controls for CVRSE, ITRE, Vehicle OBE
 Class 4 controls for CVRSE, ITRE, Vehicle OBE

Control documentation is largely sourced from NIST 800-53r4 (revision 5 was not available at the time of the analysis), with the notable exception of privacy focused content which is based on ISO 15406-2. For the NIST sourced material, the control definition and supplemental guidance are largely consistent with the NIST source (i.e., limited customization relevant to the V2I environment); all of the content in the Approved Mechanisms and Protocol Implementation Performance Statements (PIPS) sections were created as a result of the analysis and specifically for the V2I environment. For the ISO-

ARC-IT Version 9.0
The National ITS Reference Architecture

Architecture > Security > Device Class 1 Controls

Device Class 1 Controls

Device Class 1 Security Requirements:

- Confidentiality: LOW
- Integrity: MODERATE
- Availability: MODERATE

Devices of class 1 must meet controls from NIST 800-53 and ISO/IEC 15408 in the following areas:

- Access Control**
 - AC-3 Access Enforcement (Class 1)
 - AC-4 Information Flow Enforcement (Class 1)
 - AC-6 Least Privilege (Class 1)
 - AC-7 Unsuccessful Authentication Attempts (Class 1)
 - AC-8 System Use Notification (Class 1)
 - AC-11 Session Locks (Class 1)
 - AC-12 Session Termination (Class 1)
 - AC-17 Remote Access (Class 1)
 - AC-18 Wireless Access (Class 1)
- Audit and Accountability**
 - AU-2 Audit Events (Class 1)
 - AU-3 Content of Audit Records (Class 1)
 - AU-4 Audit Storage Capacity (Class 1)
 - AU-5 Response To Audit Processing Failure (Class 1)
 - AU-7 Audit Remediation And Report Generation (Class 1)
 - AU-8 Time Stamps (Class 1)
 - AU-9 Protection Of Audit Information (Class 1)
 - AU-12 Audit Generation (Class 1)
- Configuration Management**
 - CM-3 Asset Enumeration (Class 1)
 - CM-11 User-Installed Software (Class 1)
- Contingency Planning**
 - CP-12 Safe Mode (Class 1)
- Identification and Authentication**
 - IA-2 Identification And Authentication (Organizational Users) (Class 1)
 - IA-3 Authenticator Management (Class 1)
 - IA-5 Authenticator Feedback (Class 1)
 - IA-7 Cryptographic Module Authentication (Class 1)
 - IA-11 Re-authentication (Class 1)
- Incident Response**
 - IR-5 Incident Monitoring (Class 1)
 - IR-6 Incident Reporting (Class 1)
- Media Protection**
 - MP-6 Media Sanitization (Class 1)
- Privacy**
 - ISO PPR_PSE-1 Pseudonymity (Class 1)
 - ISO PPR_PSE-2 Reversible Pseudonymity (Class 1)
 - ISO PPR_UNL-1 Unlinkability (Class 1)
- Risk Assessment**
 - RSA- Vulnerability Scanning (Class 1)
- Routin and Communications Protection

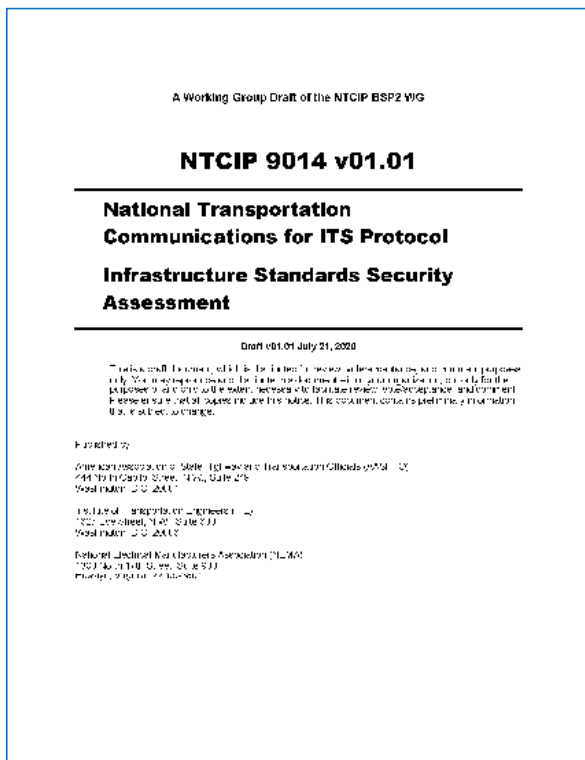
Source: USDOT

HPA approved
6/7/2022

Updated National Transportation Communications for ITS Protocol (NTCIP) Standards



U.S. Department of Transportation
Federal Highway Administration



Source: USDOT

- Provides direction to other NTCIP Standards working group
- Focuses on
 - Simple Network Management Protocol (SNMP)
 - Replace SNMPv1 protocol with SNMPv3+ protocol
 - Mitigate SNMPv1 use cases that have technical barrier to upgrades
- Balances between Interoperability and security

HPA approved
6/7/2022

ITS Profile for NIST Cybersecurity Framework



U.S. Department of Transportation
Federal Highway Administration

- In development during mid-2022
- Cybersecurity profile and candidate guidelines for State and Local DOTs' decision-making and activities to address cybersecurity issues for the ITS ecosystem
- Includes a reference implementation that describes how to implement cybersecurity controls for several service packages from the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT)

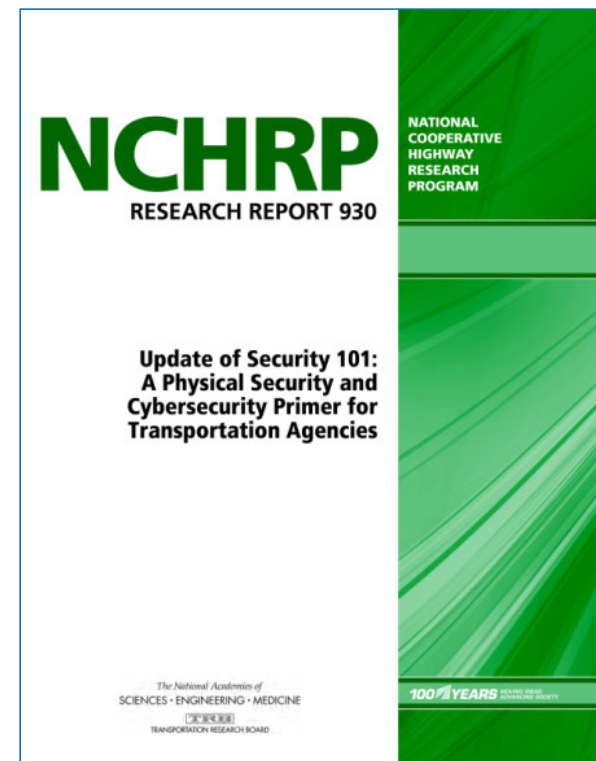
HPA approved
6/7/2022

NCHRP Cybersecurity Projects



U.S. Department of Transportation
Federal Highway Administration

- TRB Snap Search - Cyber
- Cybersecurity of Traffic Management Systems (NCHRP 3-127)
- Security 101: A Physical Security and Cybersecurity Primer for Transportation Agencies (NCHRP Research Report 930)
- Guidelines for State Transportation Agency Chief Executive Officers on Cybersecurity Issues and Protection Strategies (NCHRP 23-03, In Development)



Source: TRB

HPA approved
6/7/2022

30



U.S. Department of Transportation
Federal Highway Administration

Additional Resources

- MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) searchable terms
- Transportation Management Center Information Technology Security (available from ROSA-P)
- ITS Joint Program Office Professional Capacity Building Program for additional training

ATT&CK® for Industrial Control Systems

ATT&CK for ICS is a knowledge base useful for describing the actions an adversary may take while operating within an ICS network. The knowledge base can be used to better characterize and describe post-compromise adversary behavior. Please see the overview page for more information about ATT&CK for ICS.

You may start with the following links to become more familiar with ATT&CK for ICS:

- [ATT&CK for ICS - Philosophy Paper](#)
- [Full list of ATT&CK for ICS techniques](#)
- [Software used by ICS threats](#)
- [Adversary groups from ICS related incidents](#)
- [Assets present in ICS](#)
- [Contribute or contact us](#)

The MITRE ATT&CK for ICS Matrix is an overview of the tactics and techniques described in the ATT&CK for ICS knowledge base. It visually aligns individual techniques under the tactics in which they can be applied. Some techniques span more than one tactic because they can be used for different purposes.

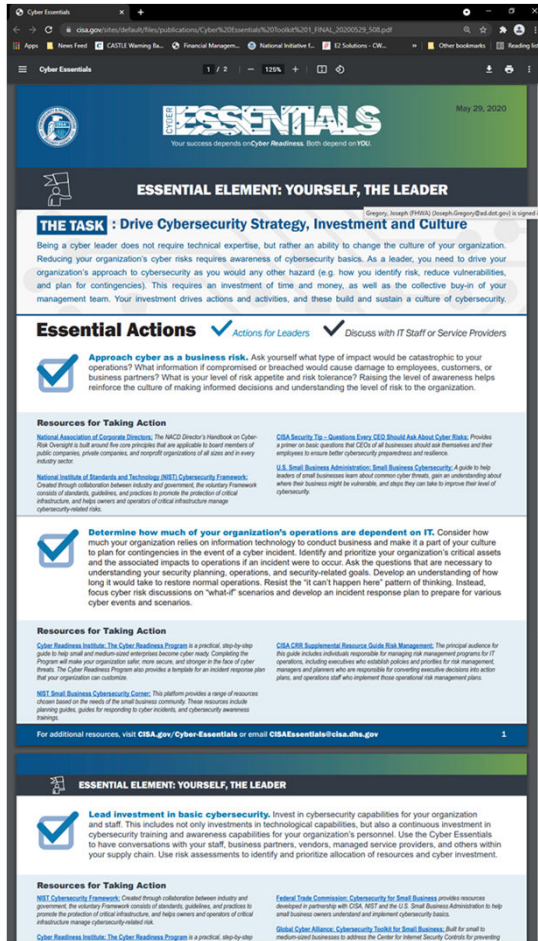
Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impact Process Control	Impact
Data Historical Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command Line Interface	Module Persistence	Hooping	Exploitation for Function	Network Sniffing	Exploitation of Remote Services	Data from Information Replication	Connective Proxy	Alarm Suppression	Modify Parameter	Denial of Control

Source: MITRE

HPA approved
6/7/2022



Additional Resources (continued)



- Follow Cybersecurity & Infrastructure Security Agency (CISA)
- Monitor and issues cybersecurity threat and vulnerability warning
- Search term “Industrial Control Systems (ICS) cybersecurity training ICS-CERT” for training
- Source: CISA

ITS JPO Cybersecurity Research Program



U.S. Department of Transportation
Federal Highway Administration

Intelligent Transportation Systems Joint Program Office (ITS JPO)
ITS CYBERSECURITY RESEARCH PROGRAM

Home About ITS Cybersecurity ITS Cybersecurity Implementation Tools and Resources ITS Cybersecurity Research ITS Cybersecurity Workforce Development **Cyber Incident Reporting**

ITS CYBERSECURITY RESEARCH PROGRAM

Cybersecurity is a serious and ongoing challenge for the transportation sector. Cyber threats to transportation systems can impact national security, public safety, and the national economy. The ITS Cybersecurity Research Program was developed in response to the urgent need to protect Intelligent Transportation Systems (ITS) from cyber-attacks.

- About ITS Cybersecurity
- ITS Cybersecurity Implementation
- Tools and Resources
- ITS Cybersecurity Research
- ITS Cybersecurity Workforce Development
- Cyber Incident Reporting

This site describes the ITS Cybersecurity Research Program. If you are experiencing a cybersecurity attack, click [Report a Cyber Incident](#) to view a list of resources.

Contact
Contact the ITS Cybersecurity Research Program with your questions or for more information: ITS_CybersecurityResearch@usdot.onmicrosoft.com

Links
[Cybersecurity Across USDOT](#) [Report a Cyber Incident](#)

HPA approved
6/7/2022

Questions?

Ed Fok

FHWA Operations Technical Services Team

Edward.Fok@dot.gov



U.S. Department of Transportation
Federal Highway Administration

MI