Why is Cybersecurity Important?

Edward Fok

Federal Highway Administration

Intelligent Transportation Society of New York (ITS NY) Annual Meeting

June 16 – 17, 2022

U.S. Department of Transportation
Federal Highway Administration

Disclaimer

U.S. Department of Transportation
Federal Highway Administration

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

U.S. Department of Transportation
Federal Highway Administration

- 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

Risks from Technology Deployment

U.S. Department of Transportation
Federal Highway Administration

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

History of Attacks and Vulnerabilities

U.S. Department of Transportation
Federal Highway Administration

Back in the 20th Century…	• Homemade signal preemption kit • Hijacked Ethernet switches on broadband cable modem
Early 2000's	• West Coast Toll tag vulnerability discovered • Portable Dynamic Message Signs hack instruction online
2010's	• 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	• Monitoring interrupted on State highway due to ransomware attack

Why is this my problem?

U.S. Department of Transportation
Federal Highway Administration

- **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

U.S. Department of Transportation
Federal Highway Administration

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 • 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”

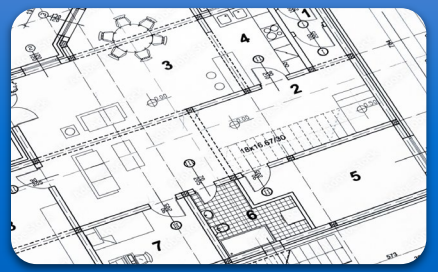
Classification and Motivations

- 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

All cyber attacks follow a similar cycle:

U.S. Department of Transportation
Federal Highway Administration

Scanning and Breaching the Perimeter



Mapping the Interior

Exploitation and Egress

What Must Be Protected?

U.S. Department of Transportation
Federal Highway Administration

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

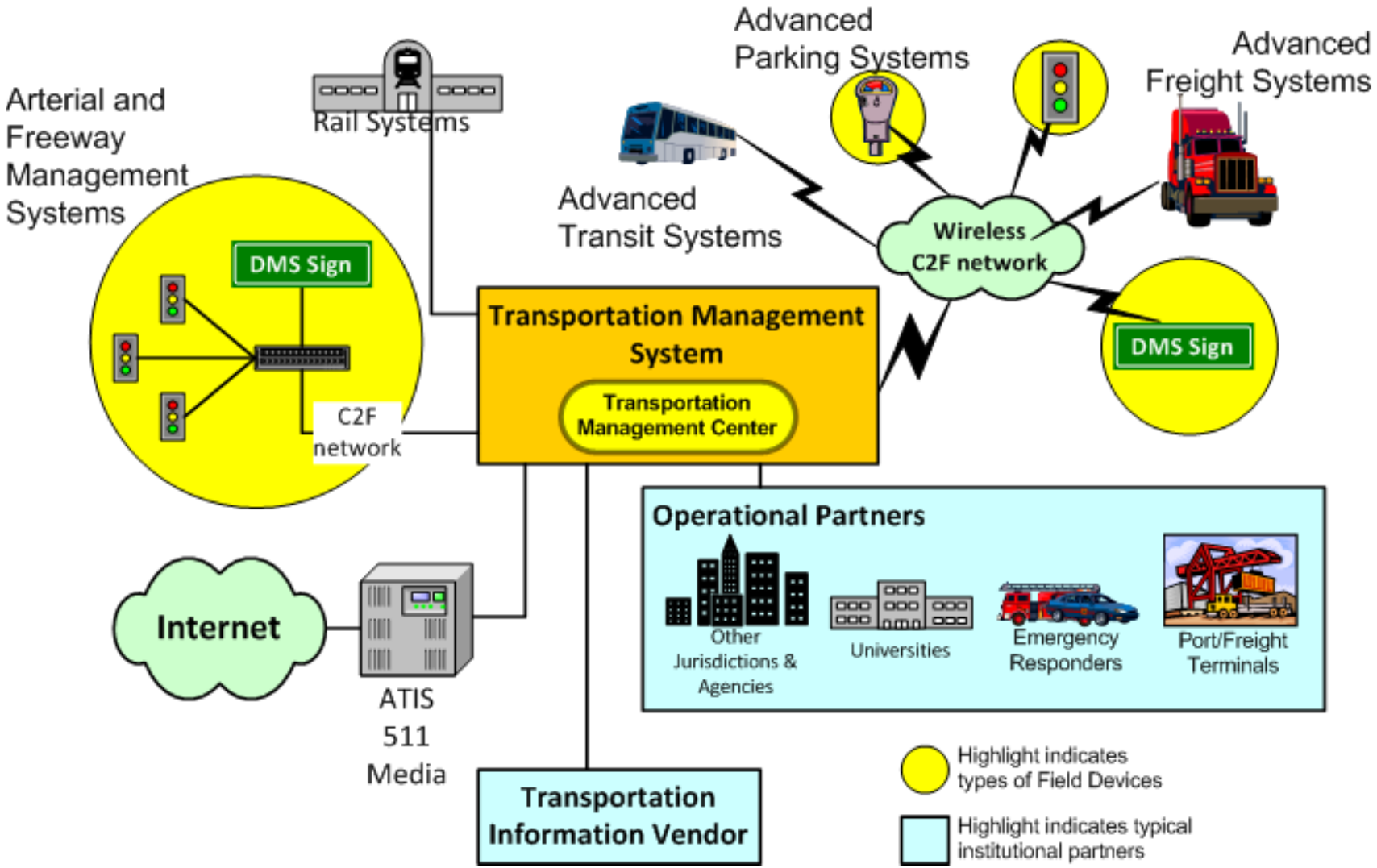
Surmountable Challenge

U.S. Department of Transportation
Federal Highway Administration

- 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

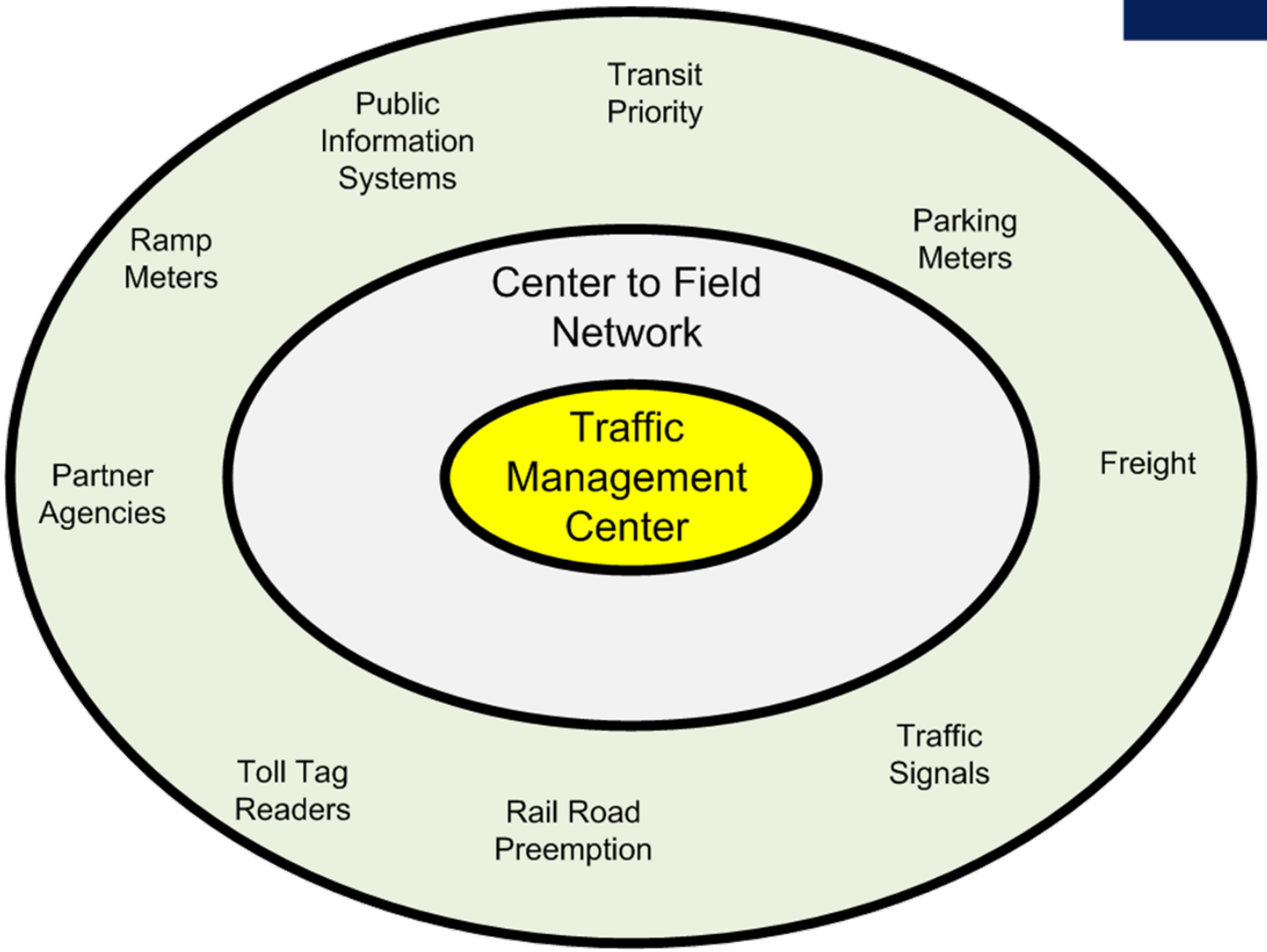
So where are we vulnerable?

U.S. Department of Transportation
Federal Highway Administration



Source: USDOT

So where are we vulnerable?



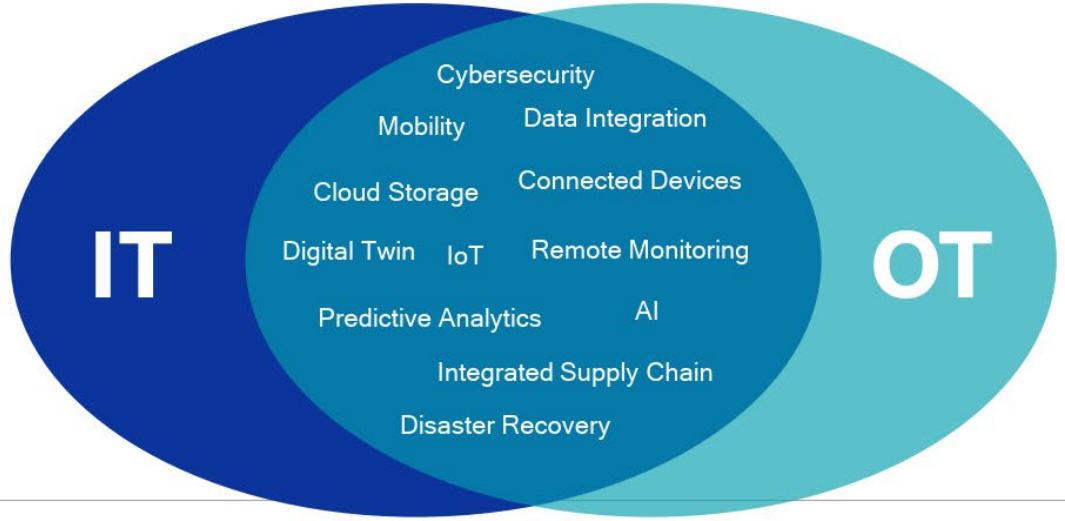
Source: USDOT

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

U.S. Department of Transportation
Federal Highway Administration

The Past

The Future

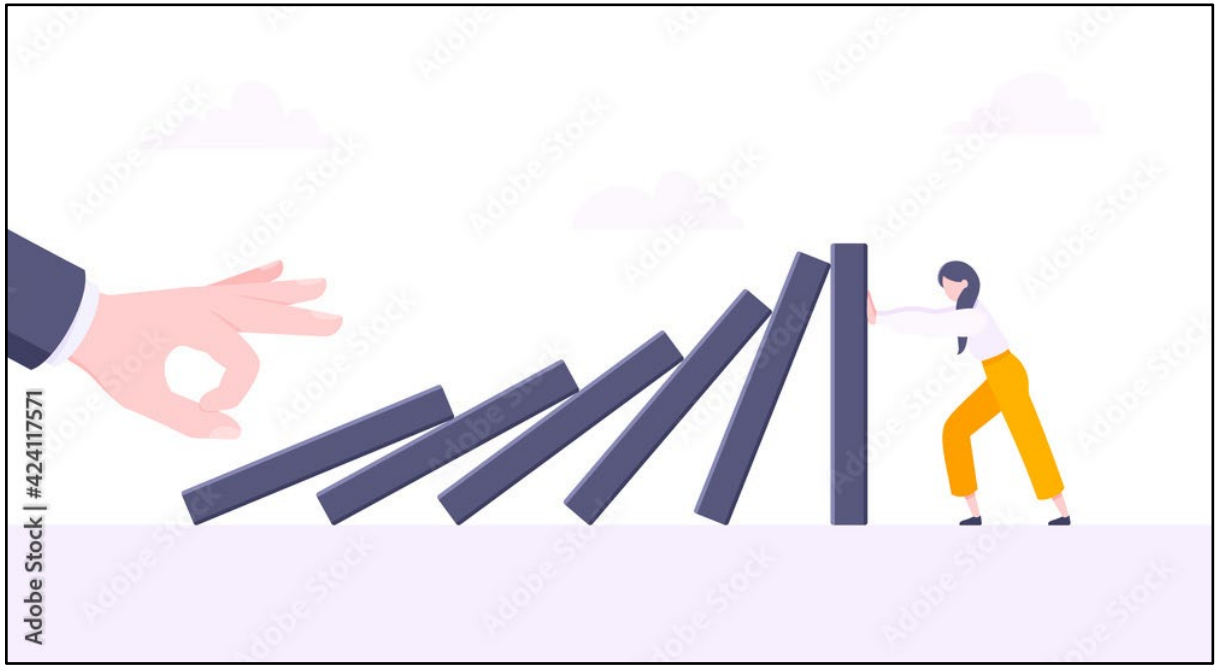


(Source: M. Rao, Virginia Department of Transportation. National Operations Center of Excellence (NoCoE) Webinar Series, October 6, 2020, webinar-series-part-2-how-leverage-it-resources-improve-tsmo)

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



Principles of Protection

U.S. Department of Transportation
Federal Highway Administration

- 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

Context of an Attack

U.S. Department of Transportation
Federal Highway Administration

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

Staff is the line between disaster and hero

U.S. Department of Transportation
Federal Highway Administration

- **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

U.S. Department of Transportation
Federal Highway Administration

- **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

Teams should be functionally cross-cutting

U.S. Department of Transportation
Federal Highway Administration

- **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

U.S. Department of Transportation
Federal Highway Administration

- **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)

State Laws on incident disclosure

U.S. Department of Transportation
Federal Highway Administration

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

Possible Next Steps for your Organization

U.S. Department of Transportation
Federal Highway Administration

- 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

U.S. Department of Transportation
Federal Highway Administration

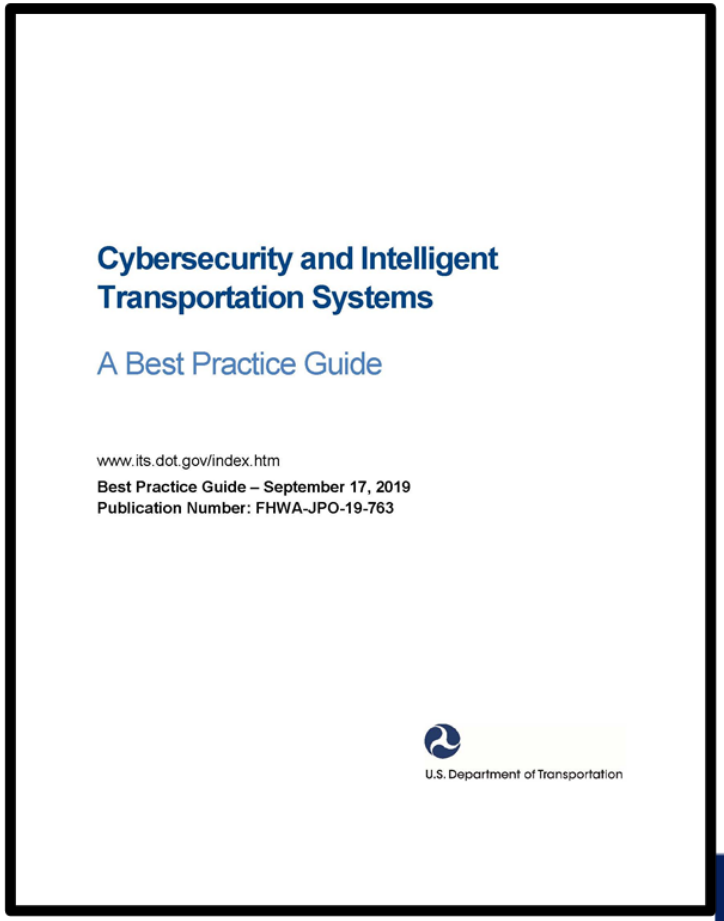
- Identify and address existing gaps in vulnerability and exploit information sharing
- A framework for communication and information sharing for vulnerabilities and incident response
- Develop of glossary of common terms
- "Transportation Cybersecurity Incident Response and Management Framework" (available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

Source: USDOT

Intelligent Transportation Systems Penetration Testing Guide

U.S. Department of Transportation
Federal Highway Administration

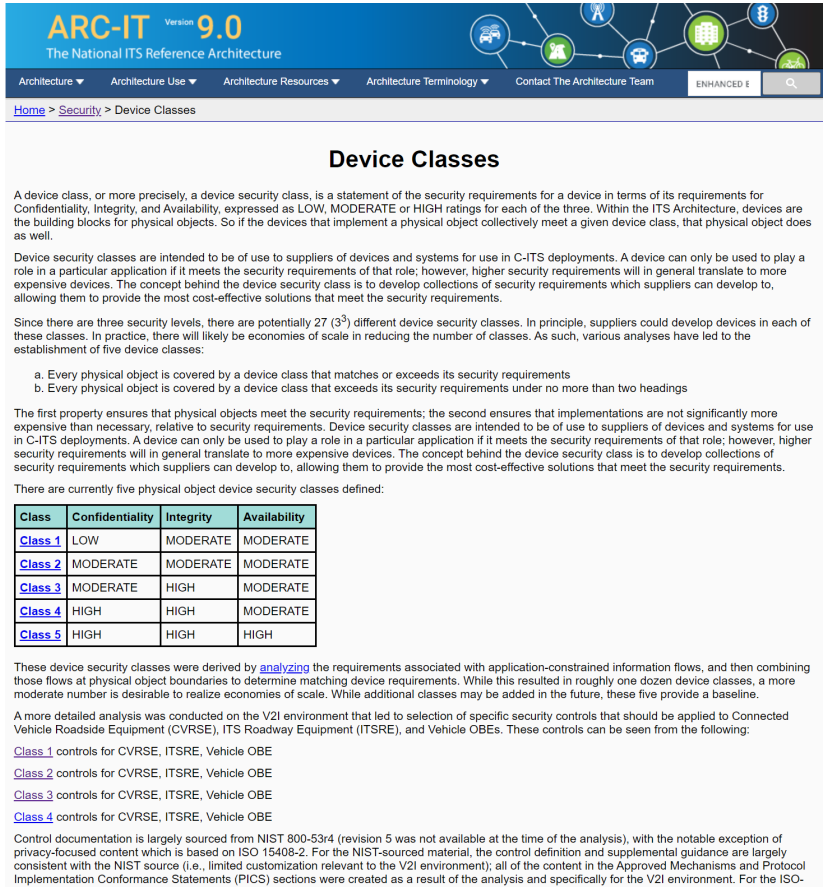
- Methodology of scoping a test: type, management, and test readiness
- Template test plan for your own penetration testing
- "Cybersecurity and Intelligent Transportation Systems – A Best Practice Guide" (source: ROSA-P)



Source: USDOT

Updated National ITS Architecture

U.S. Department of Transportation
Federal Highway Administration



ARC-IT Version 9.0
The National ITS Reference Architecture

Architecture | Architecture Use | Architecture Resources | Architecture Terminology | Contact The Architecture Team | ENHANCED E

Home > 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 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.

Since there are three security levels, there are potentially 27 (3^3) 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:

a. Every physical object is covered by a device class that matches or exceeds its security requirements
b. 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-constrained 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 (ITSRE), and Vehicle OBEs. These controls can be seen from the following:

Class 1 controls for CVRSE, ITSRE, Vehicle OBE

Class 2 controls for CVRSE, ITSRE, Vehicle OBE

Class 3 controls for CVRSE, ITSRE, Vehicle OBE

Class 4 controls for CVRSE, ITSRE, 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 15408-2. 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 Conformance Statements (PICS) 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 | Architecture Use | Architecture Resources | Architecture Terminology | Contact The Architecture Team | ENHANCED E

Home > Security > Device Class 1 Controls

Device Class 1 Controls

Device Class 1 Security Requirements:

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

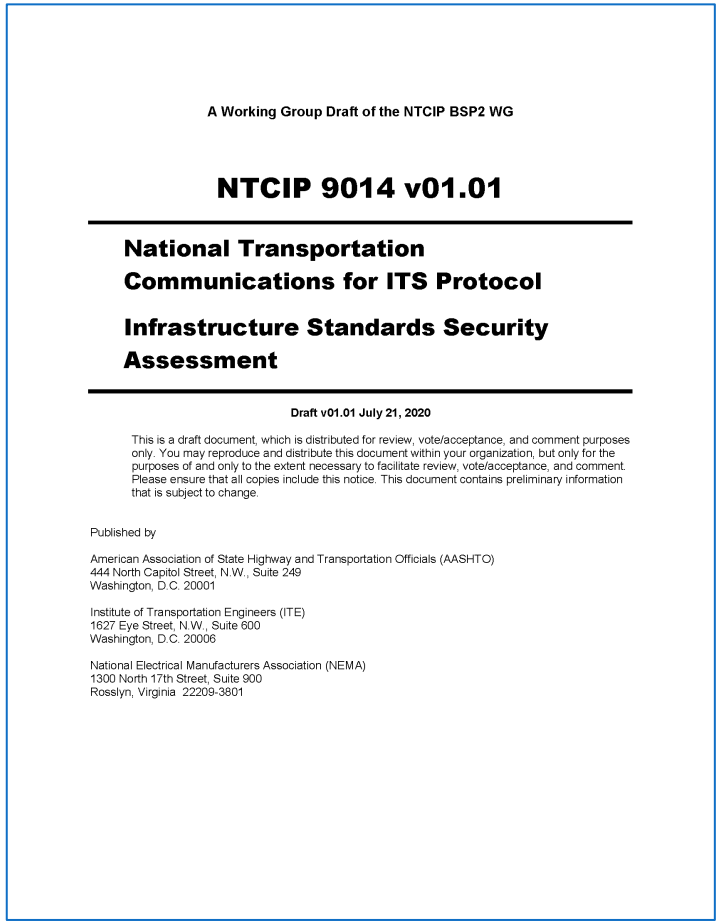
Devices of class 1 must meet controls from NIST 800-53 and ISO/IEC 15408 in the following areas:

- 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 Lock (**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 Failures (**Class 1**)
  - AU-7 Audit Reduction 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-7 Least Functionality (**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-5 Authenticator Management (**Class 1**)
  - IA-6 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 FPR_PSE.1 Pseudonymity (**Class 1**)
  - ISO FPR_PSE.2 Reversible Pseudonymity (**Class 1**)
  - ISO FPR_UNL.1 Unlinkability (**Class 1**)
- Risk Assessment
  - RA-5 Vulnerability Scanning (**Class 1**)
- System and Communications Protection

Source: USDOT

Updated National Transportation Communications for ITS Protocol (NTCIP) Standards

U.S. Department of Transportation
Federal Highway Administration



A Working Group Draft of the NTCIP BSP2 WG

NTCIP 9014 v01.01

National Transportation Communications for ITS Protocol

Infrastructure Standards Security Assessment

Draft v01.01 July 21, 2020

This is a draft document, which is distributed for review, vote/acceptance, and comment purposes only. You may reproduce and distribute this document within your organization, but only for the purposes of and only to the extent necessary to facilitate review, vote/acceptance, and comment. Please ensure that all copies include this notice. This document contains preliminary information that is subject to change.

Published by

American Association of State Highway and Transportation Officials (AASHTO)
444 North Capitol Street, N.W., Suite 249
Washington, D.C. 20001

Institute of Transportation Engineers (ITE)
1627 Eye Street, N.W., Suite 600
Washington, D.C. 20006

National Electrical Manufacturers Association (NEMA)
1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209-3801

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

ITS Profile for NIST Cybersecurity Framework

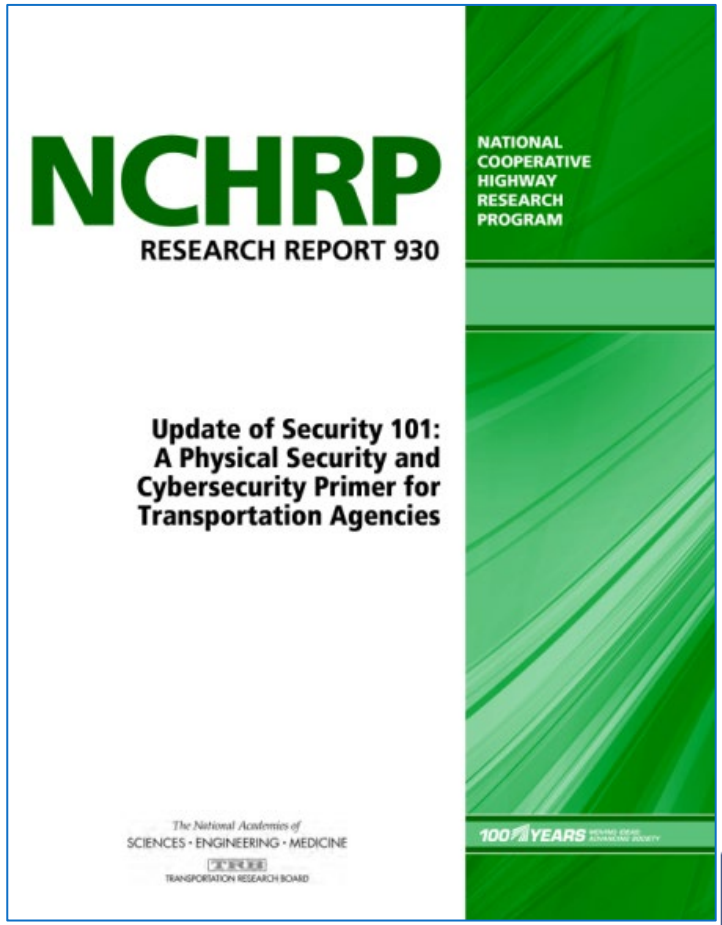
U.S. Department of Transportation
Federal Highway Administration

- 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)

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)

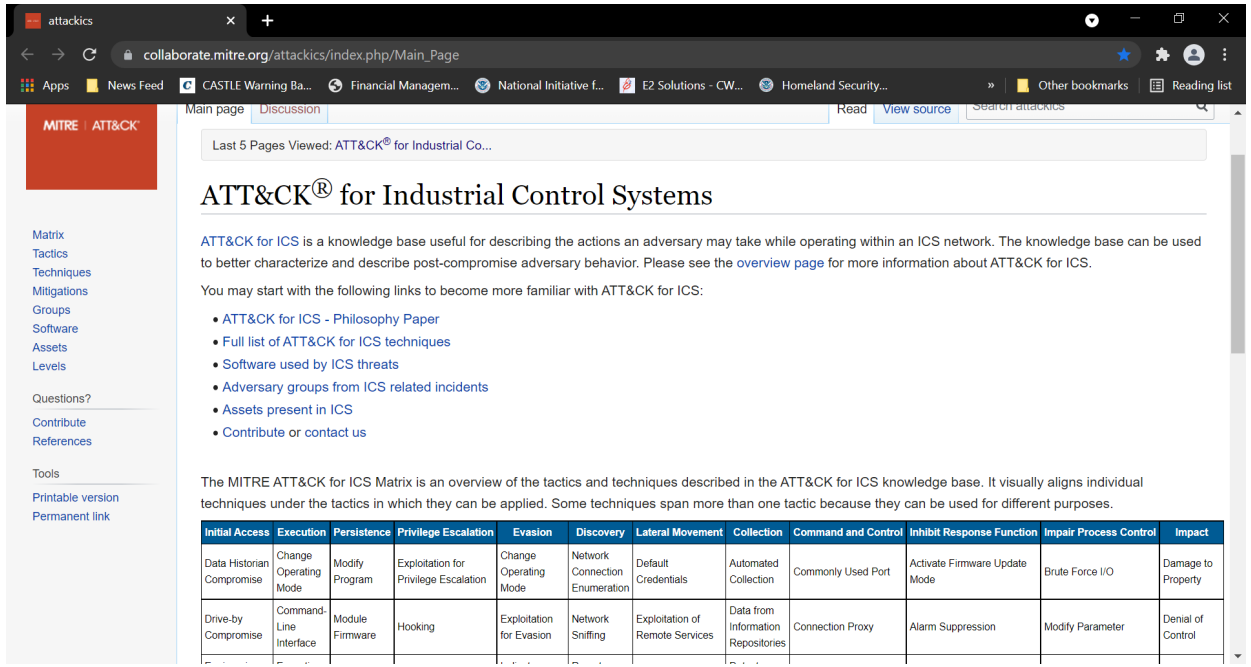


Source: TRB

Additional Resources

U.S. Department of Transportation
Federal Highway Administration

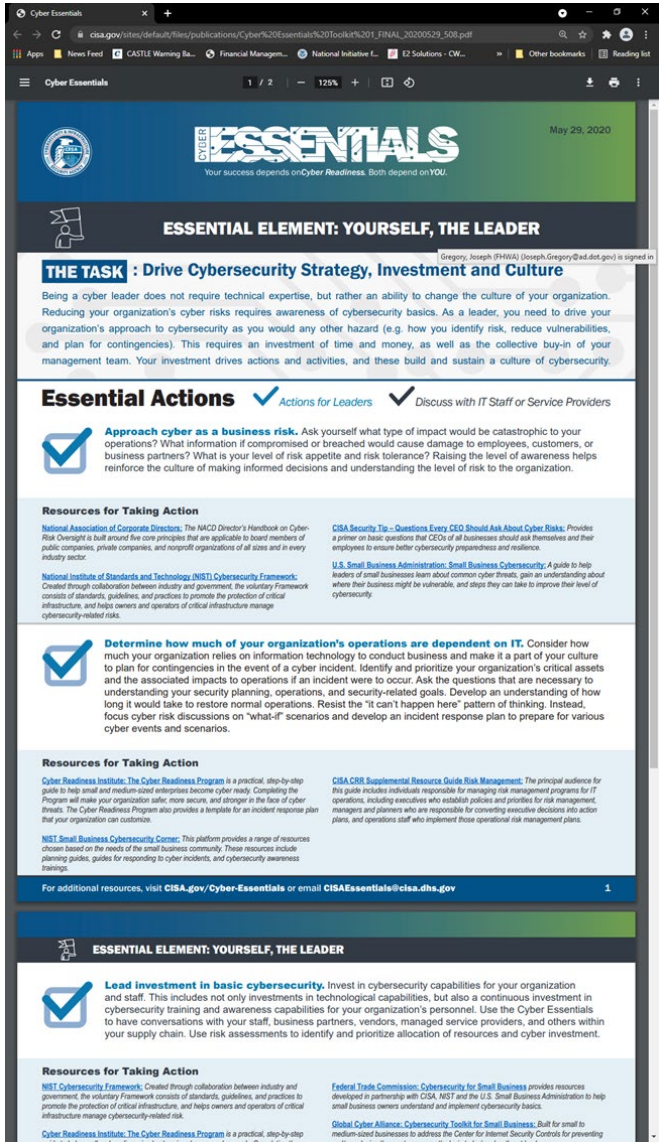
- MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) searchable terms
- Transportation Management Center Information Technology Security (available from ROSA-P)
- ITS Joint Program Office Professional Capacity Building Program for additional training



Source: MITRE

Additional Resources (continued)

U.S. Department of Transportation
Federal Highway Administration



CYBER ESSENTIALS
Your success depends on *Cyber Readiness*. Both depend on *YOU*.
May 29, 2020

ESSENTIAL ELEMENT: YOURSELF, THE LEADER

THE TASK : Drive Cybersecurity Strategy, Investment and Culture

Being a cyber leader does not require technical expertise, but rather an ability to change the culture of your organization. Reducing your organization's cyber risks requires awareness of cybersecurity basics. As a leader, you need to drive your organization's approach to cybersecurity as you would any other hazard (e.g. how you identify risk, reduce vulnerabilities, and plan for contingencies). This requires an investment of time and money, as well as the collective buy-in of your management team. Your investment drives actions and activities, and these build and sustain a culture of cybersecurity.

Essential Actions ✓ *Actions for Leaders* ✓ *Discuss with IT Staff or Service Providers*

Approach cyber as a business risk. Ask yourself what type of impact would be catastrophic to your operations? What information if compromised or breached would cause damage to employees, customers, or business partners? What is your level of risk appetite and risk tolerance? Raising the level of awareness helps reinforce the culture of making informed decisions and understanding the level of risk to the organization.

Resources for Taking Action

National Association of Corporate Directors: *The NACD Director's Handbook on Cyber-Risk Oversight is built around five core principles that are applicable to board members of public companies, private companies, and nonprofit organizations of all sizes and in every industry sector.*

National Institute of Standards and Technology (NIST) Cybersecurity Framework: *Created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure, and helps owners and operators of critical infrastructure manage cybersecurity-related risks.*

CISA Security Tip – Questions Every CEO Should Ask About Cyber Risks: *Provides a primer on basic questions that CEOs of all businesses should ask themselves and their employees to ensure better cybersecurity preparedness and resilience.*

U.S. Small Business Administration: Small Business Cybersecurity: *A guide to help leaders of small businesses learn about common cyber threats, gain an understanding about where their business might be vulnerable, and steps they can take to improve their level of cybersecurity.*

Determine how much of your organization's operations are dependent on IT. Consider how much your organization relies on information technology to conduct business and make it a part of your culture to plan for contingencies in the event of a cyber incident. Identify and prioritize your organization's critical assets and the associated impacts to operations if an incident were to occur. Ask the questions that are necessary to understanding your security planning, operations, and security-related goals. Develop an understanding of how long it would take to restore normal operations. Resist the "it can't happen here" pattern of thinking. Instead, focus cyber risk discussions on "what-if" scenarios and develop an incident response plan to prepare for various cyber events and scenarios.

Resources for Taking Action

Cyber Readiness Institute: The Cyber Readiness Program *is a practical, step-by-step guide to help small and medium-sized enterprises become cyber ready. Completing the Program will make your organization safer, more secure, and stronger in the face of cyber threats. The Cyber Readiness Program also provides a template for an incident response plan that your organization can customize.*

NIST Small Business Cybersecurity Corner: *This platform provides a range of resources chosen based on the needs of the small business community. These resources include planning guides; guides for responding to cyber incidents; and cybersecurity awareness trainings.*

CISA CRR Supplemental Resource Guide Risk Management: *The principal audience for this guide includes individuals responsible for managing risk management programs for IT operations, including executives who establish policies and priorities for risk management, managers and planners who are responsible for converting executive decisions into action plans, and operations staff who implement those operational risk management plans.*

For additional resources, visit **CISA.gov/Cyber-Essentials** or email **CISAEssentials@cisa.dhs.gov** 1

ESSENTIAL ELEMENT: YOURSELF, THE LEADER

Lead investment in basic cybersecurity. Invest in cybersecurity capabilities for your organization and staff. This includes not only investments in technological capabilities, but also a continuous investment in cybersecurity training and awareness capabilities for your organization's personnel. Use the Cyber Essentials to have conversations with your staff, business partners, vendors, managed service providers, and others within your supply chain. Use risk assessments to identify and prioritize allocation of resources and cyber investment.

Resources for Taking Action

NIST Cybersecurity Framework: *Created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure, and helps owners and operators of critical infrastructure manage cybersecurity-related risk.*

Cyber Readiness Institute: The Cyber Readiness Program *is a practical, step-by-step*

Federal Trade Commission: Cybersecurity for Small Business *provides resources developed in partnership with CISA, NIST and the U.S. Small Business Administration to help small business owners understand and implement cybersecurity basics.*

Global Cyber Alliance: Cybersecurity Toolkit for Small Business: *Built for small to medium-sized businesses to address the Center for Internet Security Controls for preventing*

- 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

Questions?

Ed Fok

FHWA Operations Technical Services Team

Edward.Fok@dot.gov

U.S. Department of Transportation
Federal Highway Administration

M1