

Traffic Management System (TMS) Cybersecurity Practices

Transportation Management Center (TMC) Pooled Fund Study⁽¹⁾

Federal Highway Administration (FHWA)

June 25, 2026



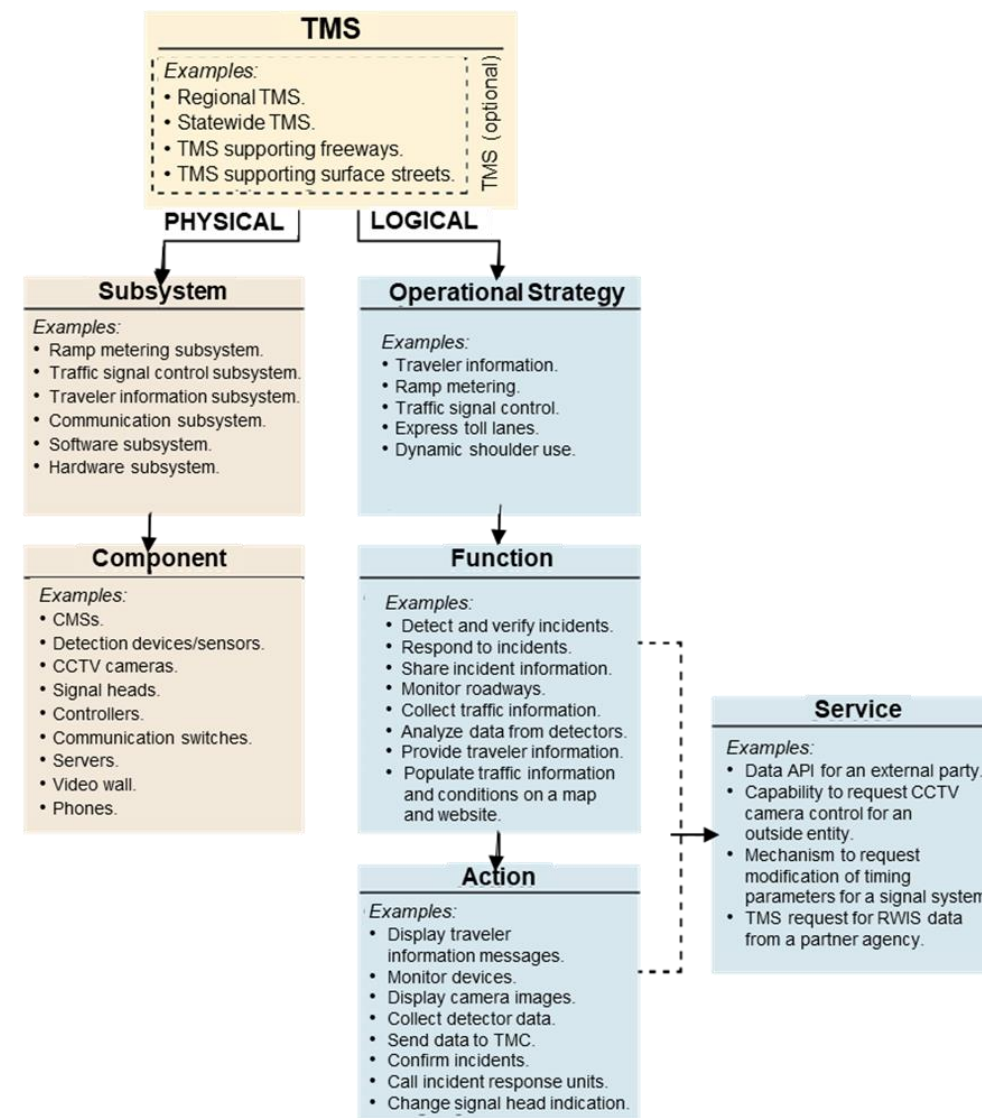
Presentation Outline

Topic	Slides
1. Background	2-4
2. TMS Cybersecurity Ecosystem	5
3. Threat Landscape and Likely Impacts	6-8
4. Standards-Based Foundation that Fits TMS Realities	9
5. TMS Distinctions vs. Generic Enterprise Information Technology (IT) Systems	10-11
6. Recommended Zones and Key Architectural Controls	12
7. Implementing a TMS Cybersecurity Program	14-18
8. Addressing Common Implementation Gaps	19
9. Scenario: Access Control	20-21
10. Additional Information on TMS Practices	22
11. References	23



Background (1 of 2)

- What are traffic management systems (TMSs):
 - Complex, integrated blend of hardware, software, processes, and people performing a range of functions and actions.
 - Physical elements of a TMS that can be managed, including subsystems, components, devices, support resources, and other items.
 - Logical elements include the operational strategies, functions, actions, and service

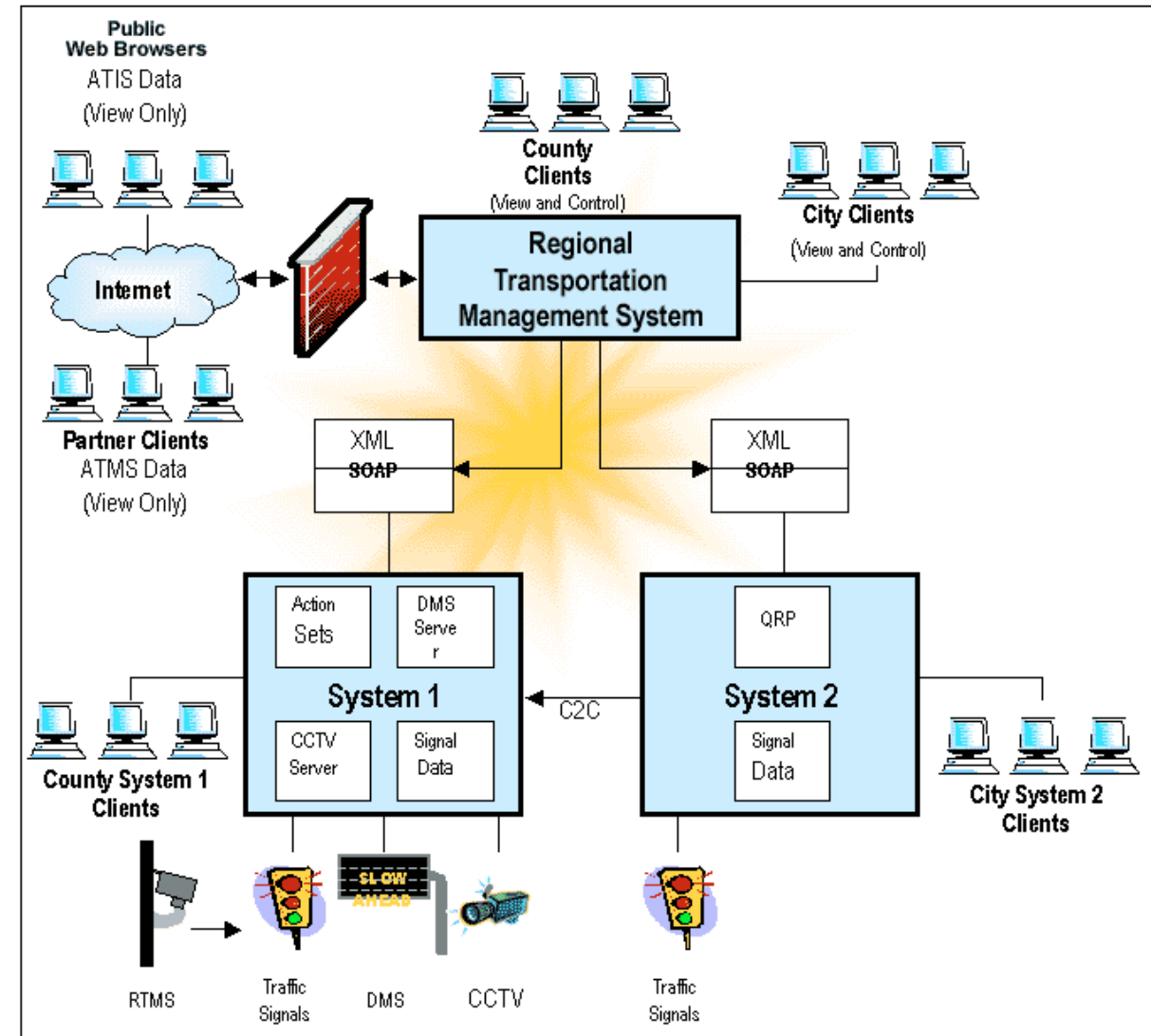


Source: FHWA



Background (2 of 2)

- Why is TMS Cybersecurity Different Now?
 - Modern TMSs have evolved from closed systems into highly connected cyber-physical ecosystems.
 - Connectivity also expands the cyber threat surface and introduces safety, reliability, and public trust risk issues.
 - Historically, TMS were designed and operated with limited external connectivity.
 - Internet Protocol (IP) networking, wireless links, remote access, cloud services, and routine data exchange with external stakeholders are now common.



Source: FHWA



TMS Cybersecurity Ecosystem

Dimension	Description/Focuses
Center-Side (TMC)	Operator workstations, video wall controllers, printers, building/internet of things (IoT) devices, internal applications, identity systems, storage/backup, and security monitoring tooling.
Field-Side	Field network equipment to consider includes controllers and edge devices such as traffic signal controllers, dynamic message signs (DMS), closed circuit television (CCTV), roadway weather information systems (RWIS), connected-vehicle roadside equipment (RSE), and their management planes.
External Data, Application Programming Interfaces (APIs), and Supply Chain	Includes third-party data subscriptions, Software as a Service (SaaS)/Platform as a Service (PaaS)/Infrastructure as a service (IaaS) hosting patterns, vendor remote access, contractor operations, and shared networks.
Communications and Integration Fabric	Enables interconnections among centers, field cabinets, maintenance laptops, and partner networks. Includes physical and air communications interfaces such as cellular, microwave, radio, wireless fidelity (Wi-Fi) but also networks and architectures such as virtual private networks (VPNs), considerations of network segmentation.

Threat Landscape – Attack Types and Likely Impacts

- TMSs face many of the same threat categories as enterprise IT, but with distinctive operational consequences.
 - Credential-based attacks such as password spraying, credential stuffing, and brute-force attempts.
 - Remote hijacking or unauthorized manipulation of management interfaces, including field-device management tools and controller-configuration software.
- Malware and ransomware that disrupt operations and back-office systems.
- Insecure or misconfigured communication links.
- Compromised vendor software updates, risky third party integrations, or contractor laptops.
- Insider risks, both malicious and unintentional.



Pathways and Threat Consequences (1 of 2)

Pathway	Description
Operational	• Can lead to several distinct categories of harmful outcomes. • Availability loss where disruptions prevent operators from accessing critical systems (e.g., video surveillance and traveler-information). • Results in slower incident detection, reduced situational awareness, and diminished ability to manage traffic or communicate accurate information to the public during emergencies.
Integrity Loss	• Attacker alters control plans, modifies roadside messages, or corrupts event data feeds. • May not be immediately obvious to operators. • Can mislead staff, distort operational decision-making, or even provide incorrect or hazardous information to the public. • Directly undermine trust in the TMS and can contribute to unsafe roadway conditions.



Pathways and Threat Consequences (2 of 2)

Pathway	Description
Confidentiality Loss	- Occurs when sensitive information is exposed, including operational datasets, network diagrams, device configurations, credentials, or vulnerability details. - Breaches give adversaries valuable insight into system architecture and weaknesses, increasing the likelihood of more damaging follow-on attacks. - Create reputational, legal, and regulatory consequences when information about critical infrastructure or privileged access credentials is leaked.
Safety Hazards for Road Users	Direct safety hazards for road users, as compromised field devices create life-critical failures (e.g., manipulation of traffic signal controllers can risk red-light violation or crossing path crashes, including pedestrian strikes)



Standards-Based Foundation that Fits TMS Realities (1 of 2)

- National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 provides the organizing backbones for managing cybersecurity risk.
 - Updated framework preserves the familiar core functions while elevating governance.
- Cybersecurity and Infrastructure Security Agency (CISA's) Transportation Systems Sector Cybersecurity Framework Implementation Guidance further adapts this structure for real-world use in transportation.
 - Designed to apply the NIST CSF in a manner that reflects the realities of multimodal transportation systems.
- NIST Guide to Operational Technology (OT) Security (SP 800-82, Revision 3).
 - Emphasizes that industrial/control systems have unique performance, reliability, and safety constraints that change how cybersecurity should be implemented (e.g., patch timing, segmentation, compensating controls).



Standards-Based Foundation that Fits TMS Realities (2 of 2)

- USDOT Intelligent Transportation Systems Joint Program Office (ITS JPO) has also developed the ITS Cybersecurity Framework Profile.
 - Contextualizes CSF for ITS and Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) service packages.
- Department of Energy (DOE) Cybersecurity Capability Maturity Model (C2M2)
 - Well-established method for evaluating cybersecurity maturity across both IT and OT.
- FHWA's TMC IT Security guidance.
 - Provides practical, implementation-ready advice on how to strengthen cybersecurity in TMC systems.



TMS Distinctions vs. Generic Enterprise IT Systems

Heterogeneous, Long-Life Field Assets	Mixed IT/Operational Technology (OT)/Communication Technology (CT) Convergence	Availability and Safety Dominate	Remote Access is Unavoidable	Multi-Network Realities and Shared Infrastructure	Public-Facing Information Integrity Matters	Resource Constraints and Uneven Maturity
Operate with a wide variety of field devices spanning different vendors, models, firmware versions, and patch histories.	Modern TMS blends enterprise IT systems, operational technology components, and communications technologies .	Operators should always preserve operational continuity, which means that security practices common in enterprise IT.	Vendors, contractors, field technicians, and distributed cabinets need remote connectivity for diagnostics and maintenance.	TMSs often depend on shared fiber, third-party communications networks, and partner interconnections.	TMS systems routinely publish roadside messages, travel-time data, and information feeds consumed by multiple entities.	Differences in agency size, mission, staffing levels, and funding mean that transportation organizations often have uneven cybersecurity maturity.
Devices can remain in service for decades with limited vendor support	OT performance and safety constraints need implementation patterns that differ significantly from traditional IT systems.	May introduce unacceptable risks if they destabilize field networks.	Remote access should be engineered as a controlled and secure service rather than treated as an occasional exception.	Increases the complexity of boundary management and makes clear.	Integrity of these outputs becomes a public-safety and public-trust concern rather than merely a data-quality issue.	Makes risk-based prioritization essential for determining which protection(s) can be implemented.



Recommended Zones and Key Architectural Controls (1 of 2)

	Category	Description
Recommended Zones	Enterprise IT Zone	TMC operations zone.
	TMC Operations Zone	Operator workstations, video systems, and operational applications supporting real-time traffic management.
	TMS Management Zone	Device-management servers, configuration tools, and secured jump hosts used for administrative tasks.
	Field Device Zone(s)	Segmented groups of field devices—organized by corridor, region, device type, or criticality—to ensure isolation and limit blast radius.
	Partner/External Data Zone	DMZ, API gateways, and data-broker infrastructure handling exchanges with external partners.
	Vendor remote access zone	Isolated and monitored providing tightly controlled and just-in-time vendor or contractor access.

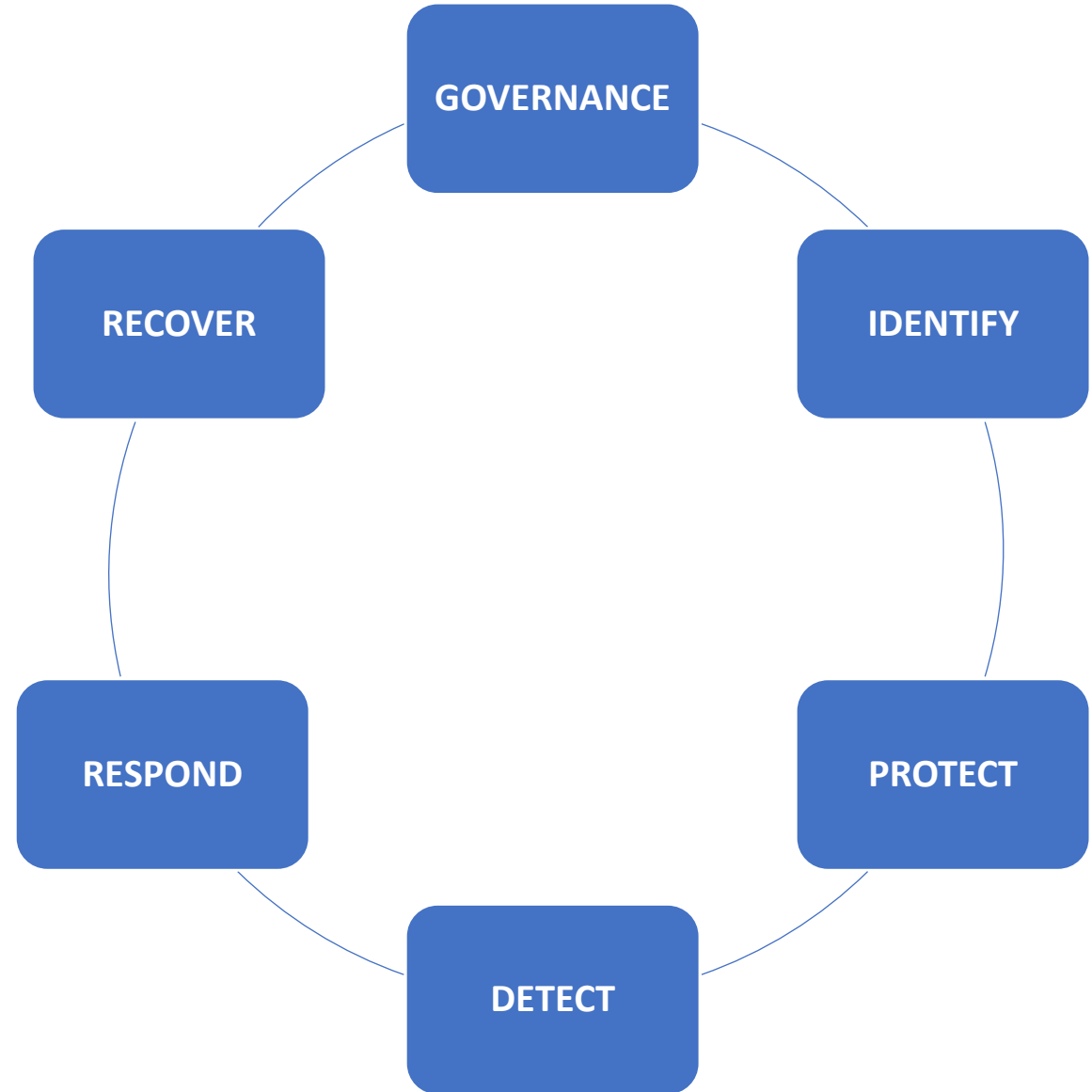


Recommended Zones and Key Architectural Controls (2 of 2)

	Category	Description
Key Architectural Controls	Network Segmentation	Use of segmentation and deny-by-default conduits to strictly manage traffic between zones.
	Jump Hosts/PAWs	Dedicated jump hosts or privileged access workstations for secure administrative and vendor access.
	Strong Identity	Enforcement of Multi-Factor Authentication (MFA), least-privilege access, and privileged access-management processes.
	Central Logging and Detection	Consolidated telemetry with detection logic tuned for OT-like behaviors and device interactions.
	Backup and Recovery	Isolated backups and regularly tested recovery playbooks to ensure resilience during incidents.

Implementing a TMS Cybersecurity Program

- Leverage CSF playbook in establishing a TMS cyber program
- Entails organization-wide operational principles.
- Focused on securing the entire TMS ecosystem.
 - Core applications.
 - Data.
 - APIs.
 - Partner integrations.
 - Mobile/driver apps.
 - Analytics.
 - OT/field interfaces.



TMS Cybersecurity Lifecycle (1 of 3)

- **Assessing TMS Performance and Capabilities**

- Evaluate as a core of system capability.
- Identify full scope of the TMS and use frameworks (NIST Cybersecurity Framework).
- Examine authentication processes, logging coverage, patch management, remote access pathways, and vendor practices.

- **Planning and Developing Strategic TMS Plans (e.g., 5–10-year plans)**

- Treat as a foundational safety and infrastructure needs.
- Embed cybersecurity expectations in strategic plans.
- Engage IT and security teams continually.
- Aligns long-range TMS planning with long-range cybersecurity resilience.

- **TMS Planning and Feasibility Studies**

- Incorporate cybersecurity objectives into preliminary technical architecture.
- Evaluate devices for lifecycle support (e.g., firmware update mechanisms, credential management, secure boot where available).
- Ensure integrations between IT and OT do not introduce unacceptable risks or compromise reliability.



TMS Cybersecurity Lifecycle (2 of 3)

- **TMS Programming, Administration, and Resource Allocation**

- Integrate into program administration, staffing, and resource allocation.
- Ensure that roles and governance structures support continuous vulnerability and configuration management, backup and recovery capabilities, segmentation maintenance, and incident response.
- Reflect the need for secure development, monitoring tools, and protection when OT is constrained.
- Formalize contractor access controls, periodic access reviews, and secure handling of diagnostic and maintenance tools.

- **TMS Procurement, Project Development, and Implementation**

- Embed in all RFPs, contracts, and vendor deliverables.
- Document all zones, ports, protocols, and secure deployment patterns; outline expectations for MFA, logging, patching, SBOMs where feasible, and incident notification timelines
- Define remote access architecture system requirements.
- During development and integration, secure SDLC practices including code reviews and dependency management should be applied. Integrations should follow NIST SP 800-82 safeguards to ensure new field connections do not compromise operational safety.



TMS Cybersecurity Lifecycle (3 of 3)

- **TMS Monitoring, Evaluating, and Reporting**

- Operationalize continuous cybersecurity activities.
- Perform vulnerability management and configuration reviews.
- Routine access reviews for contractors and vendors.
- Agencies should monitor operational baselines to detect anomalies.
- Register, document, and continuously validate all APIs.
- Integrate cybersecurity monitoring with real-time asset condition reporting.

- **Maintenance and Repairs**

- Secure maintenance practices are essential for long-term resilience.
- Maintenance laptops and diagnostic tools should be secured.
- Firmware updates should follow controlled processes with rollback plans. Apply secure data wiping and follow handling protocols when resources are repaired or replaced.
- Maintenance activities should reinforce, rather than degrade, secure deployments.



Three Phases of Risk-Based Prioritization

Phase	Timeline	Objectives	Key Activities
Phase 1: Reduce Catastrophic Risk Quickly	0–90 days	Rapidly limit the likelihood and impact of high-severity cyber events.	- Implement MFA on all remote access. - Disable direct-to-field remote administration paths. - Establish a “good enough to act” asset inventory. - Isolate backups and perform restore testing on critical systems.
Phase 2: Stabilize and Operationalize	3–12 months	Build repeatable processes and stabilize foundational security operations.	- Develop a formal incident response plan and run tabletop exercises. - Stand up central logging / SIEM ingestion for critical network zones. - Implement vendor-access governance. - Establish configuration baselines and enforce change control.
Phase 3: Optimize and Mature	12–24 months	Improve detection, resilience, and strategic planning across IT and OT.	- Advance detection engineering, threat hunting, and OT-aware monitoring capabilities. - Expand segmentation granularity based on corridor and device criticality. - Conduct a maturity assessment using models such as C2M2 to guide ongoing investments.

Addressing Common Implementation Gaps

Phase 1 - Reduce Catastrophic Risk Quickly

Uncontrolled vendor access and weak identity governance, along with flat networks and over-trusting interconnections.

Backups that are not isolated or not tested at operational tempos, particularly since unverified recovery is a single point of failure during high-impact incidents.

Phase 2 - Stabilize and Operationalize

Remediate incomplete inventories across center, field, and communications.

Institutionalize configuration and access hygiene so that identity, segmentation, logging, and restoration practices become repeatable processes.

Phase 3 - Optimize and Mature

Confront persistent workforce constraints in both transportation operations and cybersecurity.

Deepen analytics, detection engineering, and continuous improvement so earlier fixes evolve into durable capabilities.



Scenario: Access Control | Part 1 - Implementing Standards-Based Access Control

- Access Control family of controls supporting the CSF Protect function.
- The NIST SP 800-82 Rev. 3 publication includes system requirements for restricting and monitoring remote access to OT systems.
- Access control recommendations per NIST 800-82 Rev 3 and the CSF Protect function would:
 - Enforce multi-factor authentication (MFA) for vendors and field technicians,
 - Route all maintenance activities through secured jump hosts (or privileged access workstations) in the TMS management zone.
 - Apply network segmentation (deny by default conduits) to limit what remote users can access, especially across corridor field subnets.
 - Monitor and log remote sessions for anomalies, including session recording and alerting on unusual commands or off-hours access.
 - Validate configurations after maintenance, comparing to golden baselines and necessitate change tickets for administrative actions.



Scenario: Access Control | Part 2 – Access Control Compromise and TMC Recovery

- A TMC uses a vendor-managed remote access channel to maintain field devices.
- Due to missing controls from Part 1 [no MFA/Just-in-Time (JIT)], no jump-host enforcement, weak segmentation, limited session monitoring), a credential compromise leads to suspicious configuration changes and lateral-movement attempts.
 - Containment (minutes–hours): disable vendor remote channel; isolate affected corridor subnet at zone boundary.
 - Continuity (hours): shift to minimum safe operations; use manual messaging workflows if needed.
 - Eradication (days): rotate credentials, re-image jump hosts, validate controller configs against known-good templates.
 - Recovery (days): restore affected servers from isolated backups, then validate integrity before reconnection.
 - Hardening (weeks): implement just-in-time vendor access and MFA; enable session logging and recording, tighten segmentation, and update procurement language to require these controls.



Additional Information on TMS Practices

National Operations Center of Excellence (NOCoE) website,
<https://transportationops.org/>, last accessed March 27, 2025.

TMC Pooled-Fund Study Website, <https://tmcpfs.ops.fhwa.dot.gov/index.htm>, last
accessed March 27, 2025.



References

1. NIST. The NIST Cybersecurity Framework (CSF) 2.0 (CSWP 29), Feb 26, 2024.
2. CISA. Transportation Systems Sector Cybersecurity Framework Implementation Guidance, Dec 2020.
3. USDOT (ROSA/Volpe). Intelligent Transportation Systems (ITS) Cybersecurity Framework Profile, 2023.
4. FHWA. Transportation Management Center Information Technology Security (FHWA-HOP-19-059), Sept 2019.
5. FHWA. Assessing and Reporting on Traffic Management System (TMS) Capabilities and Performance – Current Practices (FHWA-HOP-24-99), April 2024
6. NCHRP 03-127. Cybersecurity of Traffic Management Systems.
7. NIST SP 800-82, Rev 3. Security Guidance for Industrial Control Systems (ICS) Security.
8. DOE. Cybersecurity Capability Maturity Model (C2M2), Version 2.1, June 2022.
9. CIS. CIS Critical Security Controls v8.1.
10. ARC-IT Version 9.3. The National ITS Reference Architecture.
11. ITS Cybersecurity Framework Profile



Disclaimer

This presentation was created and is being co-presented by both Federal Highway Administration (FHWA) and a contractor. The views and opinions expressed in this presentation are the presenters' and do not necessarily reflect those of FHWA or the U.S. Department of Transportation (USDOT). The contents do not necessarily reflect the official policy of the USDOT.

The U.S. Government does not endorse products or manufacturers. Trademarks or manufacturers' names appear in this presentation only because they are considered essential to the objective of the presentation. They are included for informational purposes only and are not intended to reflect a preference, approval, or endorsement of any one product or entity.

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





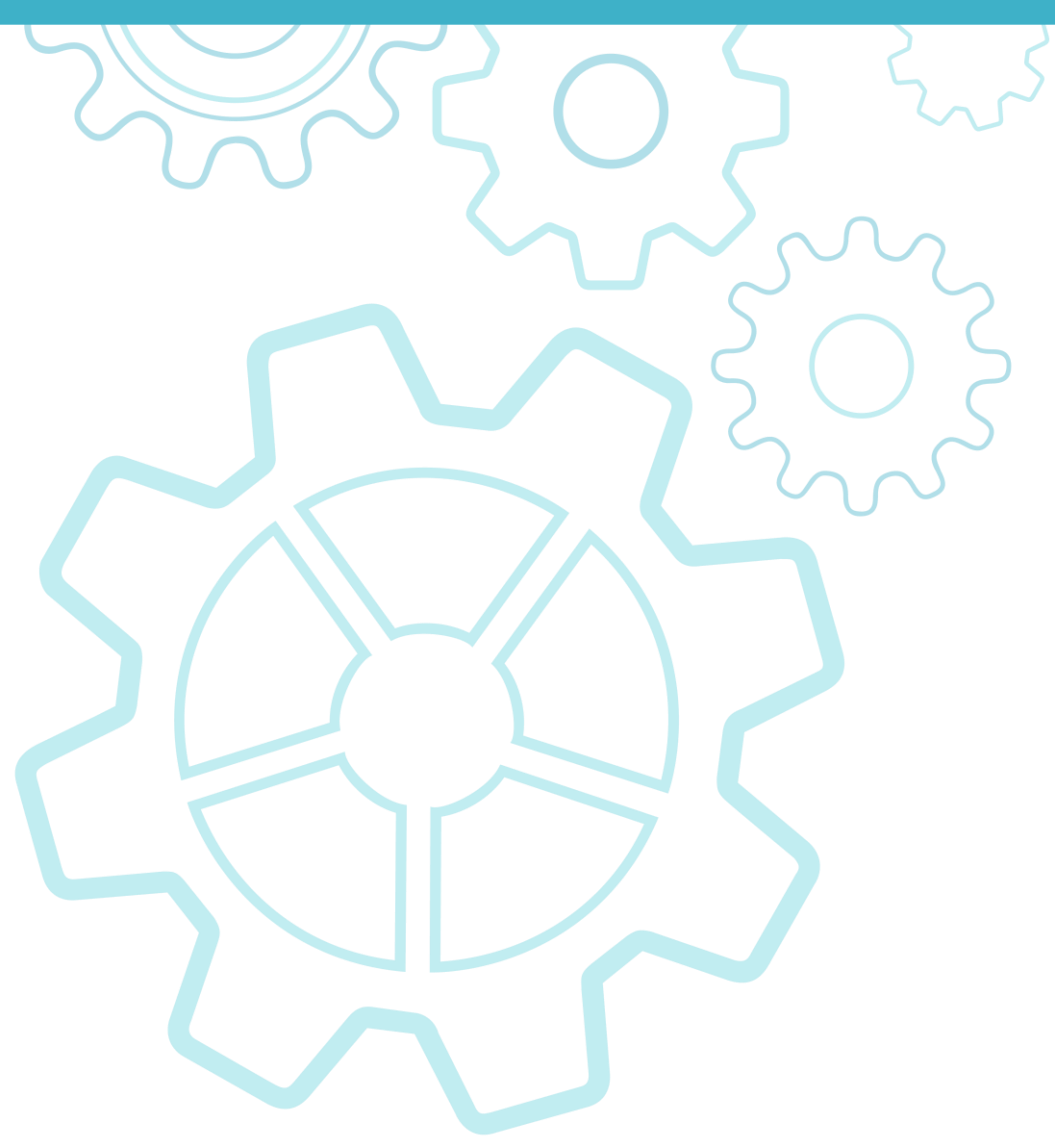
From Research to Roadway

Overview

Issues (Research VS IT)

El Camino Real – Application Development Platform

Virtual Roadside Unit (vRSU)



Primary Issues

- Research issues are driven by uncertainty and exploration
- IT issues are driven by stability and control
- Standard VS Non-Standard VS Newly Developed Application
- TMS Integration Constraints
- IT Security Policies
- Legacy system integration

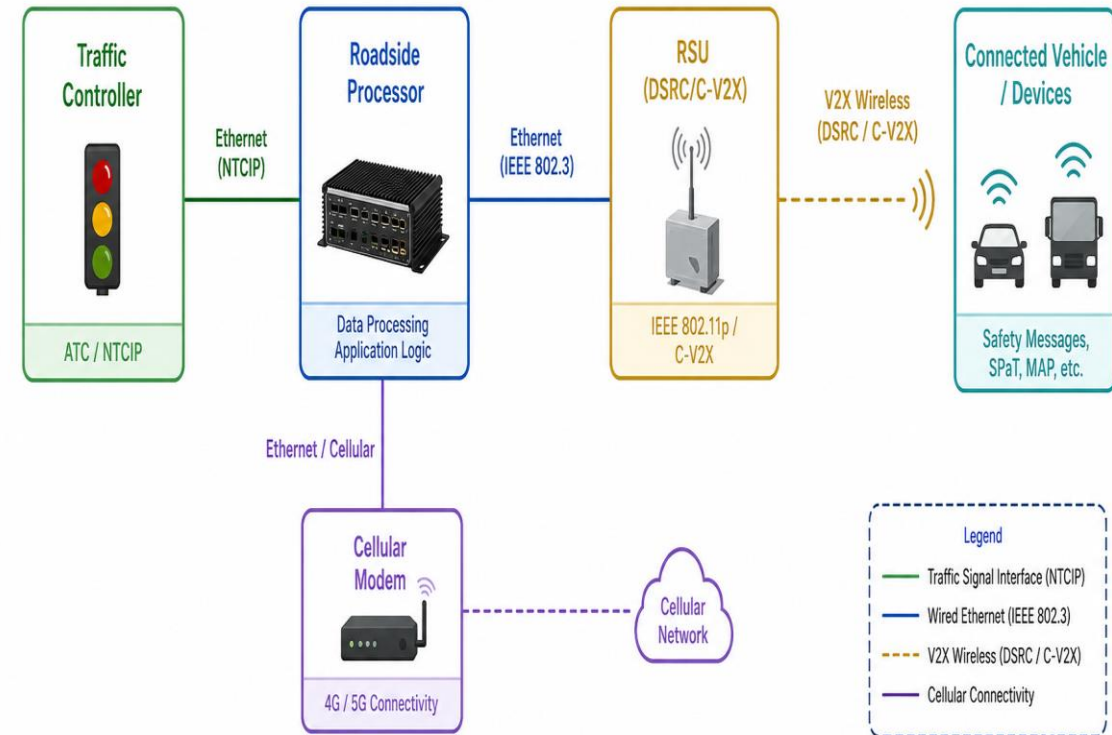
El Camino Real

APPLICATION DEVELOPMENT PLATFORM

Cyber Issues

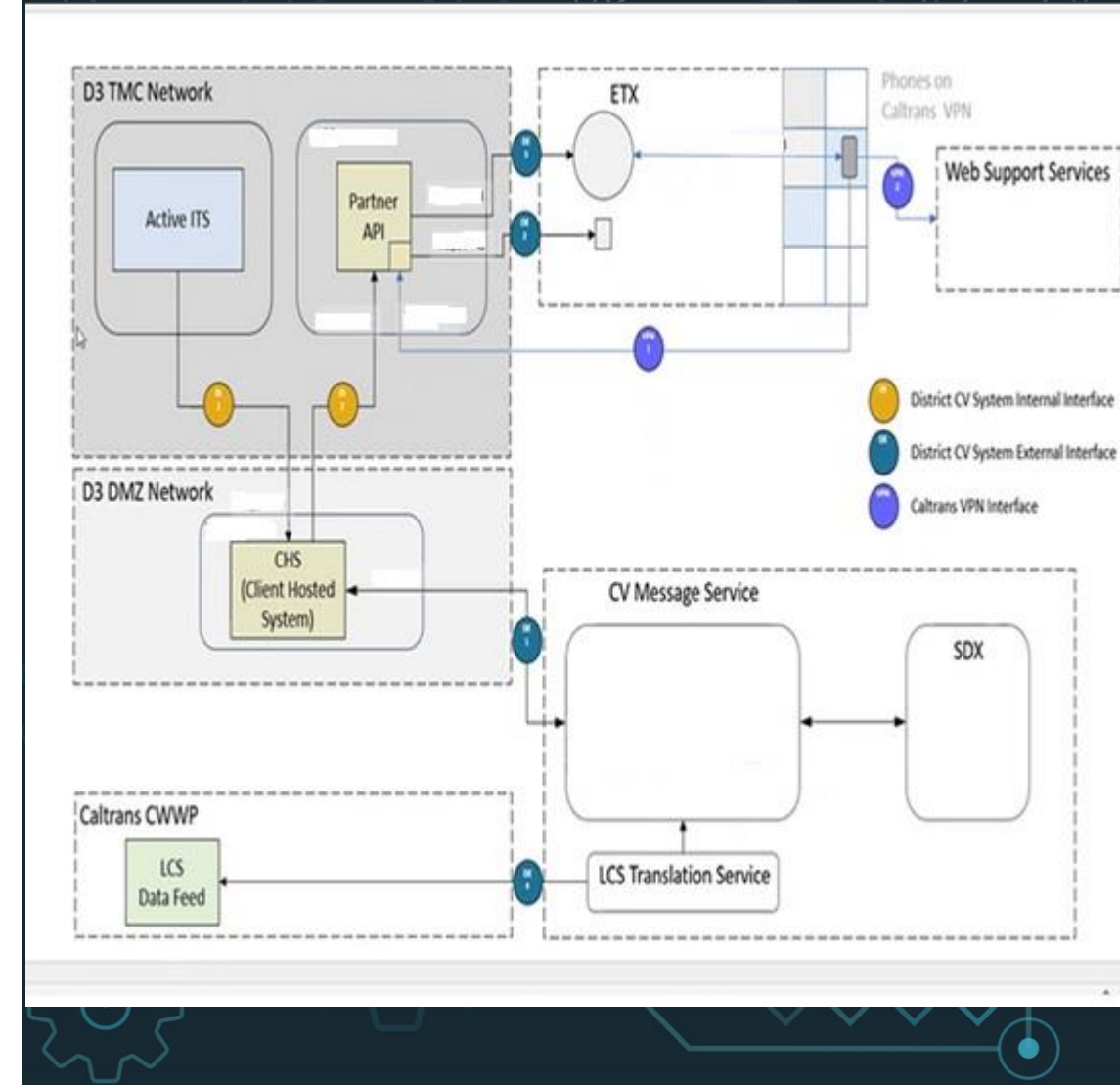
- Control handed over to District
- RSUs can be compromised
 - Public IP exposure
- Some CAV applications require cloud access
 - External Cloud provider approval
- High trust on the system as it existed for long period of time
- New application: Operations and maintenance, ultimate responsibility

Caltrans CAV Roadside Architecture – Single Line Diagram



Virtual Roadside Unit

- Contractual issues
 - Catch 22
- No Macs for you
- CT equipment for vendors
 - Admin access
- Simple in concept
 - Difficult in implementation
- CT departments work in silos
 - We have experts
- DMZ setup



QUESTIONS



Traffic Management System

Cybersecurity Practices

Stephanie Tanner, Information Security Manager
Florida Department of Transportation
Office of Transportation Technology



We Started In A Place You Maybe Familiar With

No Real Asset Inventory

No One Trained in Cybersecurity

Minimal Collaboration With Customary IT

Every TMC Setup A Little Differently

Not Cyber-Focused

No Dedicated Cyber Manager over ITS

No Cyber Budget

Don't Know Where To Start

The Trigger For Change



Staff Awareness



Peer Incident



Audit



Your Incident

Quick Impacts



Risk Assessment



Vulnerability Assessment

But I Don't Have Money for an Assessment!

Self Assessment

- Your Staff
- Your Consultant
- Your Internal Auditors

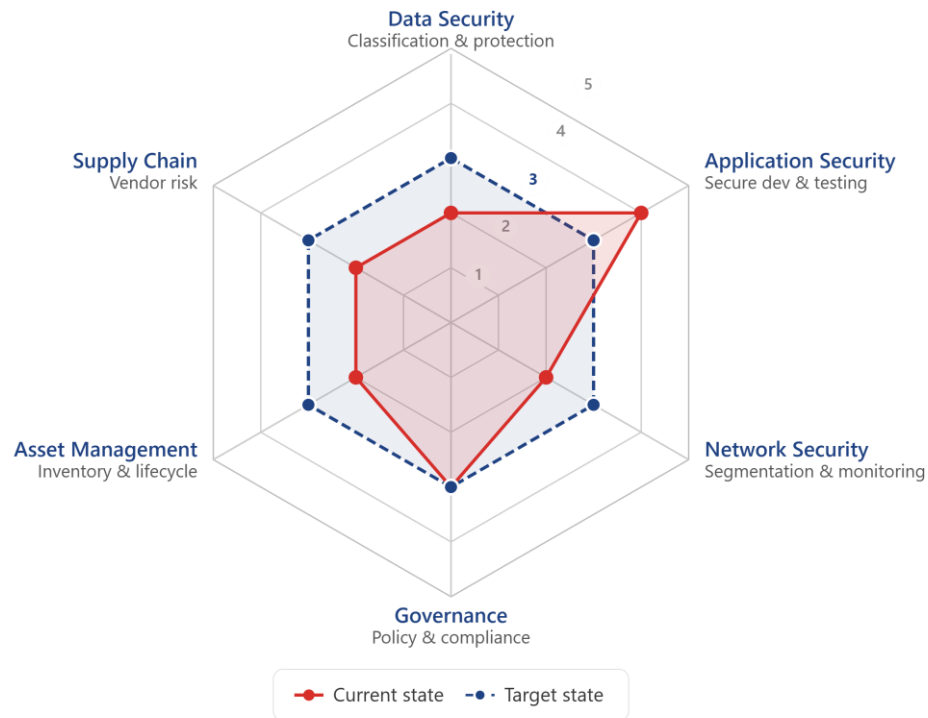
Grants

Partnerships with Higher Ed

My First Assessment

Cybersecurity program maturity

Score: 1 (Initial) — 5 (Optimized)



A Great Place To Start

While it may be painful to read those reports — it is great to have a starting place!

1

The Report

Your Baseline

You may end up with a report full of problems — but you now have a defined starting point. Gaps identified, risks quantified.

2

The Roadmap

Your Plan

Hopefully, the report came with a roadmap of recommendations — what to tackle first, adjusted based on funding and organizational priorities.

3

The Action

Your Next Step

What can we do now? What needs funding? How will this impact staff? A roadmap turns findings into a manageable plan.

Build Your Program Incrementally

No organization builds a mature cyber program overnight. Start small, show progress, and layer by layer.

Crawl: Get Assessed

Start with a risk or vulnerability assessment to establish your baseline. You can't fix what you don't know about — and you can't prioritize without data.

Walk: Build the Basics

Start patching, segment your network, stand up monitoring. You don't need everything at once — tackle the highest-risk gaps first.

Run: Mature & Scale

Integrate SOC, add tabletop exercises, share threat intel. Each year's budget cycle is an opportunity to advance another layer of your program.

Repeat: Reassess Regularly

Run follow-up assessments to measure progress and find new gaps. The threat landscape changes — your program needs to evolve with it.

Building Defenses

With a roadmap in hand, the TMS team tackled defenses one layer at a time — prioritizing highest-risk gaps first.

Vulnerability Assessments & Monitoring

Vulnerability management is a foundational component of a cyber program. Depending on which stats you use – 20% - 30% of breaches start with a vulnerability.

Security Operations Center (SOC)

Security alerts centralized from district-specific Security Incident and Event Management (SIEM) systems. A single vendor monitors multiple SIEMs and correlates activity.

Statewide SIEM Integration

FDOT funneled all alerts into a single statewide system — giving the vendor a unified view of security events across all districts.

Device Isolation Capability

District offices use the SOC to quickly isolate devices showing suspicious activity — containing threats before they spread.

Ongoing: IT & OT Working Together

IT Learning About OT

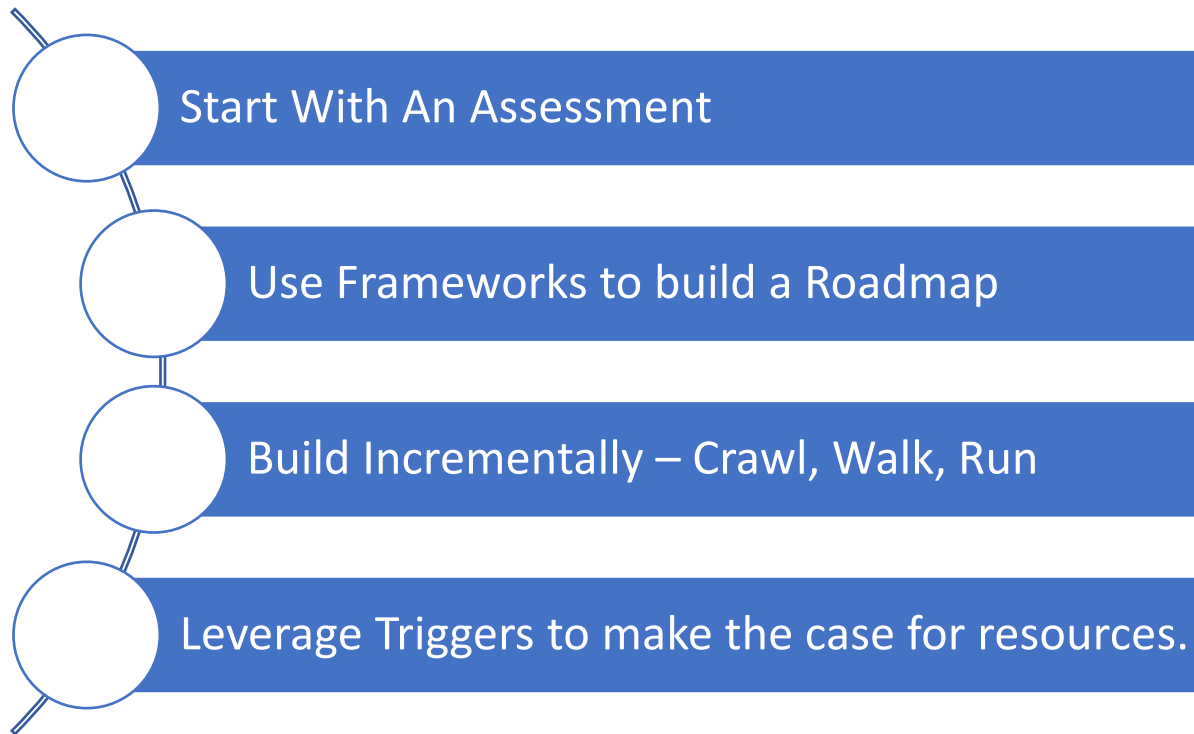
More Intel Sharing

Statewide Cybersecurity Tabletop Including TM Staff

Defining How We Work Together

Keeping OT In Mind

Key Takeaways



Cyber is not a destination — it's a continuous, evolving program.

★ *This Summer, Declare Independence From Your Phone!* ★



Focus on the Road. Not Your Phone.

If you need to text or call, pull over to
a Safe Phone Zone first.



PUT IT **DOWN**





VDOT OPERATIONS TECHNOLOGY CYBERSECURITY PERSPECTIVES

NOCoE TMS Emerging Topics webinar

Phil Davis

Assistant Division Administrator / Operations Technology Division

Virginia Department of Transportation

phil.davis@VDOT.Virginia.gov

June 25, 2026

Agenda

- **Introduction**
- **VDOT Operations Technology Overview**
- **Cybersecurity perspectives**
- **Operations Technology Critical Infrastructure - OTCI**
- **Suggestions for starting or improving cybersecurity**

By the Numbers

Traffic Operations Centers - 5

CCTV Camera - 1500

CMS Sign - 750

Weather Stations - 100

Traffic Signals - 3200

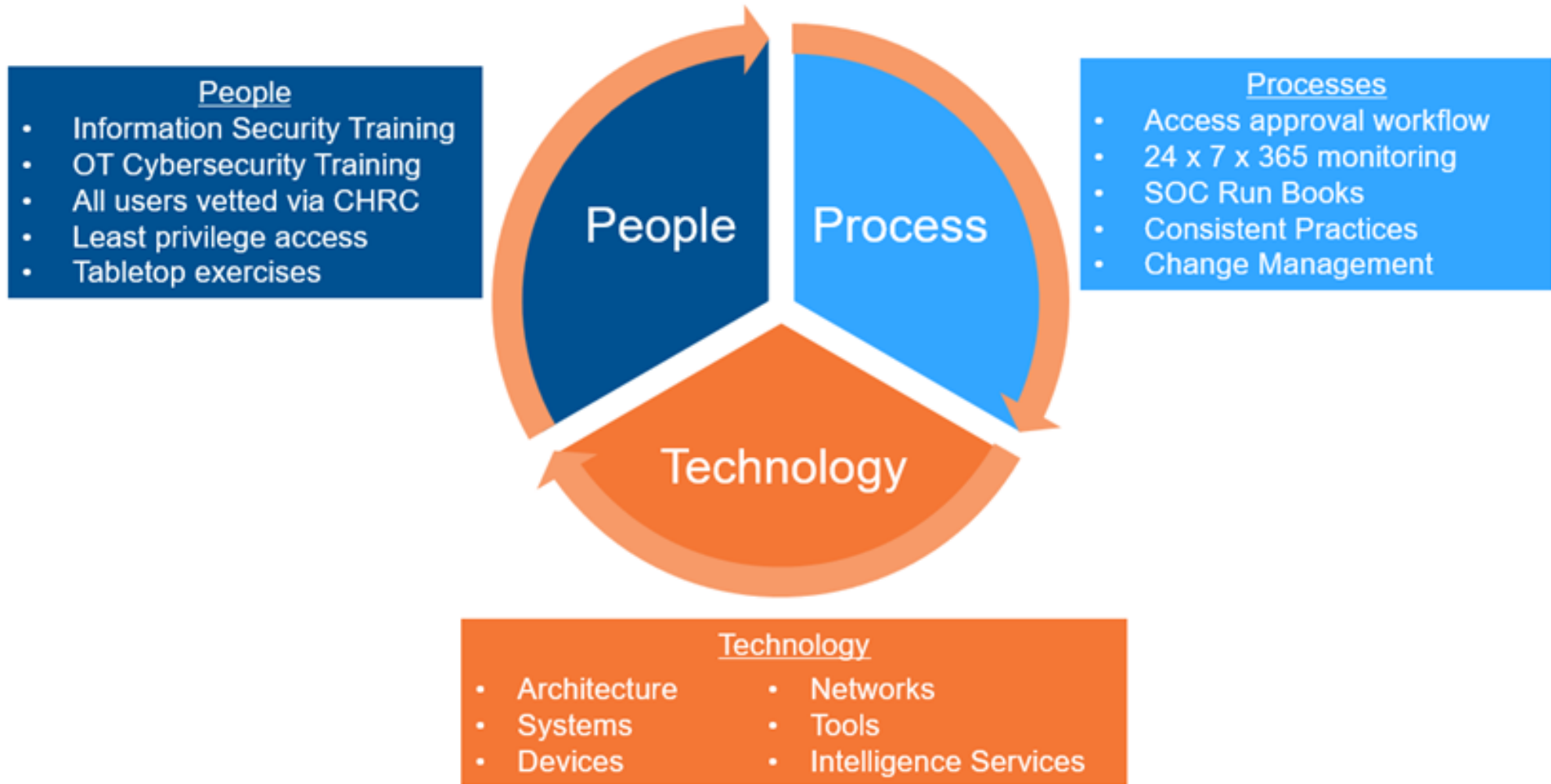
Lane Miles of fiber – 5000

VDOT Operations Technology Perspectives

VDOT Northern Virginia Public Safety Transportation Operations Center



VDOT OT Cybersecurity Model



VDOT Operations Technology Security Architecture



Cybersecurity Systems - Review

- **Server/Endpoint Device Monitoring**
 - **Symantec Endpoint Security** – *antivirus, anti-malware, internet access management*
- **Vulnerability Management**
 - **Tenable.SC** – *scans for compliance with security updates*
- **Network Detection & Response (NDR)**
 - **Forescout eyeInspect** – *network level monitoring for anomalous / malicious traffic*
- **Security Incident Event Management (SIEM)**
 - **Splunk Enterprise Security** - *scans logs from OT environment for indications of potential security breaches/malicious activity. Aggregation point for other tools.*
- **Identity and Access Management (IAM)**
 - **SailPoint IdentityIQ** – *OT access request/approval provisioning tool*

Security Operations - Monitor, Analyze, Respond



- Industry best of breed products
- \$2.1M Initial investment
- \$1.3M Annual License / Support cost

VDOT Operations Technology Perspectives

- **For Mission success Eliminate Risks where possible**
 - No inbound Email
 - Highly restricted Internet Access
 - DENY ALL and judicially approve only mission required websites
 - Encryption always
- Requires staff who think like our adversaries

VDOT Operations Technology Perspectives

Cybersecurity is Porus

- Patch Often, Test more often
- “MFA is never going away”
- Digital locks on cabinets add tremendous value
 - If Layer one is compromised, then not much else matters
- AI advancements are aiding threat actors as well as industry

VDOT Operations Technology Perspectives

- **Culture Change is HARD**
- Transportation technology is not always current technology
 - Trust very little, verify much
- Leadership buy in is essential

OT Critical Infrastructure Security Assessment

Purpose - Evaluate risk, controls, and compliance of any new VDOT OT field device to ensure baseline cybersecurity standards are met or exceeded.



OTCI Key Takeaways

- Candidate devices require a VDOT employee as sponsor
- One device/system per submission (Database Entry)
- OT device security assessment timing – submit on the project commencement
- Ensure assessment form is complete and accurate



Useful links:

- VDOT OTCI Certification Process Information: <https://www.vdot.virginia.gov/doing-business/technical-guidance-and-support/traffic-operations/operations-technology-field-device-critical-infrastructure-certification/>
- VITA COV Ramp (for cloud services): <https://www.vita.virginia.gov/services/cov-grade/cov-ramp/>
- Virginia standards on Artificial Intelligence use by state agencies: <https://www.vita.virginia.gov/policy--governance/governance/artificial-intelligence/>

Suggestions

- **Start small**
- **Obtain sanction from Leadership**
- **Develop a plan and a budget**
- **Investments in tools and staff training are vital**
 - **Align Inventory into useable data sources**
 - **OS Patch Levels**
 - **Firmware revisions**

Suggestions

- **Encrypt everything that involves command and control by policy**
- **Report Active Vulnerabilities Daily**
- **Trend Carefully – emerging threats will change your targets**
- **Balance Change Management with Operational constraints**

Suggestions

- **Build momentum from success from previous planned accomplishments**
- **Don't commit to dashboards and deliverables without sufficient resources and QA review.**
- **Do not build the house from the chimney down to the foundation**

Questions

Phil Davis

*Assistant Division Administrator / Operations
Technology Division*

Virginia Department of Transportation

phil.davis@VDOT.Virginia.gov