Traffic Management System (TMS) Cybersecurity Practices

TMSs span TMCs, field devices and networks, communications backbones, cloud services, and third-party data and application programming interface (API) integrations. Modern TMSs are highly connected cyber-physical ecosystems: connectivity improves coordination and decision support but also expands the cyber threat surface, creating safety and continuity risks beyond traditional enterprise information technology (IT). In TMS contexts, cybersecurity is an operational safety and continuity imperative, not just a data-protection task.

WHY TMS CYBERSECURITY MATTERS NOW

TMCs and intelligent transportation system (ITS) devices no longer function as closed systems. Internet Protocol networking, remote access, cloud services, and routine data exchanges are now common, increasing cybersecurity risks to transportation operations. Cyber incidents can degrade incident response, traveler information, traffic control, and coordinated operations, with safety consequences that exceed typical business IT impacts.

WHAT TMS INCLUDES IN CYBERSECURITY TERMS

Partitioning the scope into four categories is the first step toward making cybersecurity manageable:

1. *Center-side (TMC)*: Servers, operator workstations, video systems, identity and logging platforms, storage/backup, and security tooling.
2. *Field-side*: Signals, ramp meters, dynamic message signs (DMSs), closed-circuit television, road weather information system, detectors, connected vehicle roadside equipment, and associated management planes.
3. *External data, APIs, and supply chain*: Third-party data subscriptions, cloud hosting, vendor or contractor access, and shared networks.
4. *Communications and integration fabric*: Fiber, cellular, microwave, radio, wireless network; virtual private networks (VPNs); and segmentation and managed conduits between zones.

THREAT LANDSCAPE AND IMPACTS

There are a host of threats, including the following:

- Credential attacks against remote access and vendor portals can result in unauthorized manipulation of management interfaces and controller software.
- Malware and ransomware can disrupt TMC operations and back-office systems due to misconfigured links that enable session hijacking and data tampering.
- Supply-chain risks can happen via compromised updates, contractor devices, or insider risks (malicious or accidental).

The effects on safety can be significant and may include compromised grade-crossing gates, conflicting signal indications, hijacked DMSs causing wrong-way or hazardous diversions, and unsafe ramp metering.

STANDARDS-BASED FOUNDATION THAT FITS TMS REALITIES

Standards have been created and adapted in practice for TMS operations to address these cyber threats. The following resources are available to TMS cybersecurity implementers:

- National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) 2.0 (including the Govern function).[1]
- NIST Special Publication (SP) 800-82 Revision 3 *Guide to Operational Technology (OT) Security*.[2]
- Cybersecurity and Infrastructure Security Agency's (CISA) *Transportation Systems Sector Cybersecurity Framework Implementation Guide*.[3]
- U.S. Department of Transportation's *ITS Cybersecurity Framework Profile*.[4]
- Security controls using CSF implementation (strategic) and Center for Internet Security (CIS) Critical Security Controls (tactical).[5]
- U.S. Department of Energy (DOE) Cybersecurity Capability Maturity Model (C2M2) for maturity modeling.[6]
- CISA's Cyber Security Evaluation Tool (CSET) for assessments.[7]

TMS DISTINCTIONS VERSUS ENTERPRISE IT

Many TMC internal controls resemble standard enterprise IT, but TMS cybersecurity complexity differs materially when field-side elements and operational missions are considered. TMS systems have the following characteristics:

- Are heterogeneous, with long life field assets.

- Use supervisory control and data acquisition-like OT components and communications systems in blended setups consisting of enterprise IT systems.
- Work continuously, which means that IT practices that might disrupt operational continuity, such as vulnerability scanning, rapid patch deployment, or configuration changes, would destabilize operations.
- Are available to vendors, contractors, and field technicians who interact with distributed cabinets. Remote access is unavoidable and needs to be engineered as a controlled service.
- Operate in multinetwork systems with shared infrastructure (e.g., fiber and communications networks) and complicated boundaries and ownership, necessitating clear ownership and firewall rules.
- Are tasked with providing public-facing information that has a high standard for integrity, as these messages affect public trust and safety.
- Are subject to resource constraints and uneven maturity across agencies, necessitating risk-based prioritization.

Given their complexity, defensible TMS setups are differentiated from enterprise setups and typically implement a strictly managed zoned architecture, as shown in table 1.

Table 1. Recommended zones and key architectural controls.

Element	Category	Description
Recommended zones	Enterprise IT zone	Agency corporate network hosting business systems and internal IT services.
	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 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 zone	Demilitarized zone, API gateways, and data broker infrastructure handling exchanges with external partners.
	Vendor remote access zone	Isolated, monitored systems providing tightly controlled and just-in-time vendor or contractor access.
Key architectural controls	Network segmentation	Use of segmentation and deny by default conduits to strictly manage traffic between zones.
	Jump hosts or privileged access workstations (PAWs)	Dedicated jump hosts or PAWs for secure administrative and vendor access.
	Strong identity	Enforcement of multifactor 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 NIST CSF-ALIGNED TMS CYBERSECURITY

Using the CSF playbook to establish a TMS cyber program entails organization-wide operational principles that secure the TMS ecosystem: core applications, data, APIs, partner integrations, mobile and driver applications, analytics, and OT and field interfaces. The following is a TMS-oriented interpretation of CSF outcomes, which constitutes a framework for a TMS cyber program:

- *Govern*: Assign owners (operations and IT) shared key performance indicators, define risk acceptance for legacy field devices, require security-by-contract for vendors, and exercise governance and supply-chain controls.
- *Identify*: Maintain inventories across centers, fields, and communications; track versions; map critical services to CSF outcomes; and classify APIs and feeds by integrity and availability.
- *Protect*: Perform baseline hardening; multifactor authentication (MFA), least privilege, and just-in-time (JIT) for remote access; session recording; configuration management and allow-listing; and operator training.
- *Detect*: Centralize logs, OT events, and behavior-driven analytics; monitor interzone choke points; and integrate sector intel.
- *Respond*: Initiate preauthorized containment (disable vendor VPN, isolate corridor subnets, and launch manual traveler information); define minimum safe operations; and run tabletops.
- *Recover*: Initiate offline, tamper-resistant backups for crown jewels; test restorations; verify integrity before re-enabling interzone traffic; and aim for continuous improvement.

CYBERSECURITY LIFECYCLE

TMS cybersecurity succeeds when embedded across the full lifecycle, not added after deployment. The TMS lifecycle begins with understanding system performance and extends through planning, development, monitoring, and maintenance. Integrating cybersecurity into each of the following seven stages ensures resilience, safety, and operational continuity:

1. *Assessing TMS Performance and Capabilities*: Evaluate cybersecurity as a core system attribute by identifying the full TMS scope and using frameworks such as the NIST CSF to assess posture, gaps, and prioritized risks.[1] Review authentication, logging, patching, remote access, and vendor practices early so risks are understood before major decisions are made.
2. *Planning and Developing Strategic TMS Plans (5–10 yr)*: Treat cybersecurity as a foundational safety and infrastructure requirement. Embed expectations such as MFA, logging, segmentation, software bill of materials (SBOMs) (where feasible), device lifecycle support, and vulnerability disclosure. Incorporate secure architectures, API governance, and incident response, engaging IT and security teams early.
3. *TMS Planning and Feasibility Studies*: Translate cybersecurity objectives into preliminary technical design, defining zones, conduits, trust boundaries, demilitarized zones, and secure API expectations (e.g., object-level authorization and strong authentication). Assess device lifecycle support and ensure new IT and OT integrations do not introduce unacceptable risks.
4. *TMS Programming, Administration, and Resource Allocation*: Integrate cybersecurity into governance, staffing, and budgeting. Support continuous vulnerability and configuration management, backups, segmentation maintenance, and incident response. Formalize contractor access controls, access reviews, and secure handling of diagnostic and maintenance tools.
5. *TMS Procurement, Project Development, and Implementation*: Embed cybersecurity requirements in all requests for proposal and contracts. Require documentation of zones, ports, protocols, and secure deployment patterns, along with MFA, logging, patching, SBOMs (when feasible), incident notification, and secure remote access. Apply secure software development lifecycle practices and follow NIST SP 800-82 safeguards for field integrations.[2]
6. *TMS Monitoring, Evaluating, and Reporting*: Operationalize continuous cybersecurity through vulnerability and configuration management suited to OT systems. Review contractor and vendor access regularly, monitor baselines for anomalies, and register and validate all APIs. Integrate cybersecurity monitoring with real-time asset condition reporting where possible.
7. *Maintenance and Repairs*: Apply secure maintenance practices, including securing diagnostic tools, controlling firmware updates with rollback plans, and detecting configuration drift through golden baselines. Ensure secure data wiping and handling during repairs or replacements so maintenance reinforces secure deployment patterns.

RISK-BASED PRIORITIZATION FOR AGENCIES AND COMMON IMPLEMENTATION GAPS

Implementation of this lifecycle does not have to occur all at once. The three-phase implementation plan shown in table 2 and contingent on agency risk-based prioritization, provides an example path to deploying cybersecurity practices to a TMS.

TMS cybersecurity implementers should be aware of and avoid these common implementation gaps, delineated by the phases described in table 2:

- *Phase 1*: Uncontrolled vendor access and weak identity governance, flat networks and over-trusting interconnections, and nonisolated or untested backups.
- *Phase 2*: Incomplete inventories across center, field, and communications and mature identity, segmentation, logging, and restoration into repeatable processes.
- *Phase 3*: Workforce constraints (scarcity of transportation-savvy cybersecurity talent), deepened analytics, and continuous improvement.

EXAMPLE SCENARIO: ACCESS CONTROL—COMPROMISE AND RECOVERY

A TMC uses a vendor-managed remote-access channel to maintain field devices. In the absence of enforced jump-host pathways, strong segmentation, and session monitoring, a credential compromise leads to unauthorized configuration changes and lateral movement:

- *Containment (minutes–hours)*: Disable vendor channel and isolate the affected corridor subnet at the zone boundary.
- *Continuity (hours)*: Shift to minimum safe operations and use manual traveler-information workflows.
- *Eradication (days)*: Rotate credentials, reimage jump hosts and privileged access workstations, and validate controller configurations against golden templates.
- *Recovery (days)*: Restore from isolated backups and verify integrity before reconnecting.
- *Hardening (weeks)*: Implement JIT and MFA, enable session logging/recording, tighten segmentation, and update procurement language.

Table 2. Three phases and risk-based prioritization.

Phase	Timeline	Objective	Key Activities
Phase 1: Reduce Catastrophic Risk Quickly	0–90 d	Rapidly limit the likelihood and impact of high-severity events.	• MFA implementation on all remote access. • Disabling of direct-to-field administrative paths. • Establishment of a "good enough" asset inventory. • Backup isolation and restore testing on critical systems.
Phase 2: Stabilize and Operationalize	3–12 mo	Build repeatable processes and stabilize foundational security operations.	• Formal incident response plus tabletops. • Central logging and security information and event management for critical zones. • Vendor access governance (contract plus technical). • Configuration baselines and change control.
Phase 3: Optimize and Mature	12–24 mo	Improve detection, resilience, and strategic planning across IT and OT.	• Detection engineering, threat hunting, and OT-aware monitoring. • Finer grained segmentation by corridor and device criticality. • C2M2 maturity assessments to guide investments.[6]

REFERENCES

1. NIST. 2024. *The NIST Cybersecurity Framework (CSF) 2.0* Report No. NIST CSWP 29. Gaithersburg, MD: National Institute of Standards and Technology.
2. Stouffer, K., M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule, and M. Thompson. 2023. *Guide to Operational Technology (OT) Security*. Report No. NIST SP 800-82r3. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf, last accessed June 15, 2026.
3. U.S. Department of Homeland Security. 2020. *Transportation Systems Sector Cybersecurity Framework Implementation Guide*. Washington, DC: U.S. Department of Homeland Security.
4. Tran, H., C. Sames, C. BF Casey, J. Nethery Snyder, and D. Weitzel. 2023. *Intelligent Transportation Systems (ITS) Cybersecurity Framework Profile*. Report No. FHWA-JPO-23-120. Washington, DC: U.S. Department of Transportation. https://rosap.ntl.bts.gov/view/dot/72769, last accessed June 15, 2026.
5. CIS. 2024. *CIS Critical Security Controls* (software). Version 8.1. https://www.cisecurity.org/controls/v8-1, last accessed June 15, 2026.
6. DOE. 2022. *Cybersecurity Capability Maturity Model (C2M2)*: Version 2.1. Washington, DC: U.S. Department of Energy. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2, last accessed June 15, 2026.
7. CISA. 2025. *CSET* (software). Version 12.4.0.4.
8. Federal Highway Administration. 2025. "TMC Pooled-Fund Study" (web page). https://tmcpfs.ops.fhwa.dot.gov/index.htm, last accessed March 27, 2025.

FOR MORE INFORMATION ON THE TMC POOLED-FUND STUDY:

TMC Pooled-Fund Study website, https://tmcpfs.ops.fhwa.dot.gov/index.htm.[8]

FHWA-HRT-26-062
HRSO-40/08-26(WEB)E

Recommended citation: Federal Highway Administration, *Traffic Management System (TMS) Cybersecurity Practices* (Washington, DC: 2026) https://doi.org/10.21949/59n7-1a34

250
U.S. Department of Transportation
Federal Highway Administration