ITS DEPLOYMENT EVALUATION

Executive Briefing

Source: Shutterstock/vectorfusionart

Highlights

- Utilizing NIST's Cybersecurity Framework can help protect ITS assets and data by guiding holistic cyber planning, detection, and quick response procedures. Emerging deployments like CVs need to utilize the framework extensively at every stage to ensure secure operations.
- State Departments of Transportation (DOTs) realize tangible benefits from tactical cybersecurity measures such as penetration testing, red-team exercises, and adversarial simulations.
- By implementing a "Defense in Depth" approach, a TMC can significantly hinder cyberattacks by disrupting the attacker's progress at multiple stages.

This brief is based on past evaluation data contained in the ITS Databases at: www.itskrs.its.dot.gov. The databases are maintained by the U.S. DOT's ITS JPO Evaluation Program to support informed decision making regarding ITS investments. The brief presents benefits, costs and best practices from past evaluations of ITS projects.

U.S. Department of Transportation
Intelligent Transportation Systems
Joint Program Office

ITS Cybersecurity (2025 Update)

Introduction

The success of Intelligent Transportation Systems (ITS) relies on robust cybersecurity, as these systems increasingly rely on the secure collection, processing, and transmission of vital safety and mobility data. ITS cybersecurity refers to the protection of transportation technologies and digital infrastructure from cyber threats that could compromise safety, reliability, and performance of the transportation system. This includes the use of secure communication and response protocols, encryption, intrusion detection systems, regular audits, and other safeguards to manage vulnerabilities and incidents across complex cyber-physical environments.

This executive briefing builds upon the 2022 version [1] by integrating recent developments, research, and real-world deployments, with a particular focus on benefits, costs, and lessons learned. The release of the NIST Cybersecurity Framework (CSF) 2.0 in February 2024 offers an updated, more flexible approach to addressing evolving cyber risks. It enhances the earlier version [2] by adding a new "Govern" function and expanding guidance on supply chain risk management and continuous improvement. In parallel, the ITS Cybersecurity Framework Profile, published in 2023, adapts National Institute of Standards and Technology (NIST) principles to the transportation sector [3], providing agencies with a structured way to prioritize cybersecurity investments based on mission-specific goals and risk exposure. These updates are part of a broader set of federal, state, and local efforts aimed at strengthening cybersecurity in transportation.

The National Academies of Sciences (NAS) published a 2023 report identifying eleven categories of cybersecurity initiatives currently being implemented by state Departments of Transportation (DOTs), ranging from governance and risk management to training, penetration testing, and procurement practices [4]. These efforts reflect a growing recognition of both the complexity and the urgency of protecting transportation systems against cyber threats.

Benefits

Investing in cybersecurity for ITS yields substantial operational, financial, and safety benefits. As these systems become increasingly digitized and interconnected, the risks associated with cyber incidents grow more consequential. A single security breach can disrupt traffic management, compromise public safety, or paralyze mobility services. According to IBM's Cost of a Data Breach Report 2025, the global average cost of a breach has reached $4.44 million, with U.S.-based breaches averaging a staggering $10.22 million per incident, underscoring the value of proactive security investments in preventing catastrophic losses [5].

> By staying ahead of evolving threats, agencies can safeguard public trust, ensure operational continuity, and achieve lasting performance.

Proven Agency Benefits: Numerous transportation agencies have already seen benefits from cybersecurity efforts. For example, the Federal Transit Administration's (FTA) Cybersecurity Assessment Tool for Transit (CATT) has enabled agencies to identify system vulnerabilities, prioritize mitigation strategies, and track cybersecurity maturity over time. This structured approach improves preparedness and fosters institutional resilience [6].

Real-Time Defense: Similarly, secure, private, and trusted real-time communications have demonstrated strong operational benefits. An Security Credential Management System (SCMS) certificate is a digital credential issued by the SCMS to vehicles, roadside units, or infrastructure in a Vehicle-to-Everything (V2X) ecosystem. Its primary function is to secure real-time communication between vehicles and infrastructure. A key benefit of this system is that it offers a secure and privacy-preserving method for V2X devices to share information via digital certificates (2023-L01192). In freeway environments, active traffic management (ATM) cybersecurity simulations demonstrated that continuous cyber monitoring can detect and respond to attacks quickly enough to maintain core system functions and prevent service disruptions (2019-B01345). When deploying "defense in depth" strategies, agencies utilize multiple, different, and overlapping countermeasures to protect information and systems at the system level. By layering protections across devices, networks, and data channels within Traffic Management Centers (TMCs), they improve their ability to detect threats early and sustain safe, efficient mobility operations [7].

Outcomes-Driven Cybersecurity Planning: A more structured and scalable approach has emerged through the *ITS Cybersecurity Framework Profile*, a sector-specific adaptation of the NIST Cybersecurity Framework. This profile helps transportation agencies align cybersecurity efforts with mission objectives, map maturity levels, and prioritize investment based on real risk exposure. By guiding organizations through the identify, protect, detect, respond, and recover phases, it supports effective risk management and enhances overall resilience. The framework contextualizes NIST principles within transportation operations, enabling consistent, outcomes-driven planning while remaining adaptable to unique operational needs, risk tolerances, and desired future cybersecurity states [3].

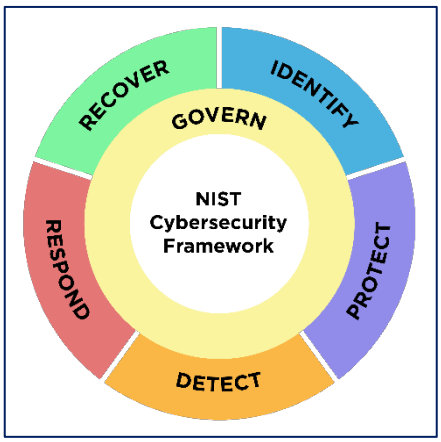

Figure 1: NIST Cybersecurity Framework 2.0 (Source: NIST)

Tactical Cyber Measures: Beyond frameworks and assessments, states have realized direct operational and financial benefits from tactical cybersecurity measures (2025-B01996). Penetration testing and red-team exercises have allowed agencies to uncover system weaknesses and remediate them before exploitation, enhancing readiness and reducing potential downtime. In Tennessee, for example, cybersecurity awareness and training programs were credited with reducing successful phishing attempts and improving overall cyber hygiene. Virginia DOT's procurement process includes an approved product list that favors acquiring devices with security hardening already in place, enabling the agency to secure funding for new, pre-hardened devices (2025-B01996). In California, Caltrans has implemented tactical cybersecurity measures such as endpoint and network protection, annual penetration testing, and mandatory employee and contractor training, collectively reducing risk and improving system resilience (2025-B01996).

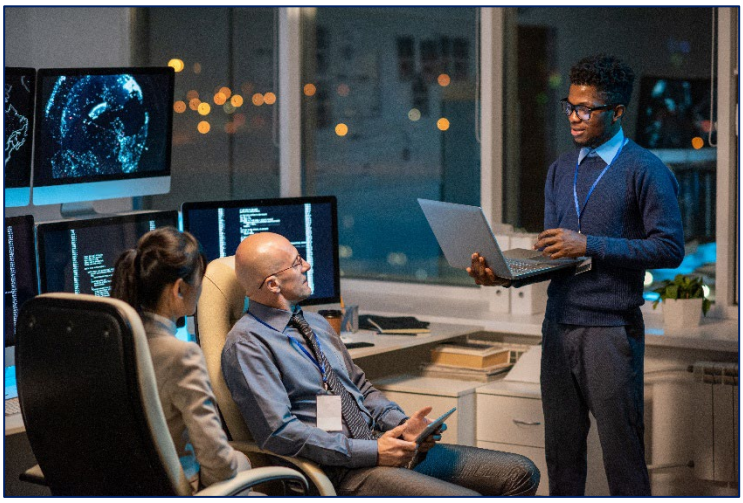

Figure 2: A group of professionals engaged in a cybersecurity training session (Source: Shutterstock/Pressmaster).

Cyber Hygiene in Practice: Routine practices such as patching, encryption, asset inventory, and access control continue to prove effective. Organizations utilizing Cybersecurity and Infrastructure Security Agency's (CISA) Cyber Hygiene services typically reduce their risk and exposure by 40 percent within the first 12 months, with most seeing improvements within the first 90 days [8]. The services identify vulnerabilities in internet-facing systems that might otherwise remain unmanaged, enabling organizations to address proactively potential security gaps. By integrating vulnerability insights with existing threat detection and risk management efforts, enrolled organizations can increase the accuracy and effectiveness of their response activities, reducing false alarms and improving threat detection. Additionally, a dedicated control set has been developed by U.S. Department of Transportation (USDOT) Volpe National Transportation Systems Center to address security risks specific to traffic signal controllers functioning as ITS Roadway Equipment (ITSRE) under the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) TM04 framework [9]. These technical safeguards focus on protecting the confidentiality, integrity, and availability of both the controllers and their information flows, ensuring resilience as more advanced features are deployed [10].

Beyond these technical safeguards, establishing a formal incident response capability provides an additional layer of protection, particularly by helping to mitigate financial risk. For example, Tennessee DOT has been able to negotiate lower insurance premiums by demonstrating formal incident response capabilities (2025-B01996). This illustrates how proactive security measures can lead to tangible cost savings. These outcomes collectively reinforce the value proposition of cybersecurity as not merely a compliance obligation but a strategic enabler of safe, resilient, and cost-effective transportation infrastructure. As threats evolve, agencies that proactively implement cybersecurity best practices will be better positioned to protect public trust, maintain operational continuity, and unlock long-term performance gains.

Costs

Securing ITS involves a multi-layered investment, from individual edge devices to enterprise-wide cybersecurity infrastructure. The cost landscape varies depending on the scale and technology involved.

Cybersecurity Staffing Costs

Many ITS-related projects increasingly rely on cybersecurity and specialized technical staff such as those managing train control systems like Communications-Based Train Control (CBTC), to ensure secure, reliable operations. For example, the San Franciso Municipal Transportation Agency's (SFMTA) Train Control Upgrade Project (TCUP) uses skilled cybersecurity subject matter experts with negotiated hourly billing rates ranging from approximately $197 to $220 per hour, depending on role and whether services were field-based or office-based [11]. Some DOTs may not be able to directly fund or train a cybersecurity position and may lean on outside contractors to perform security tasks, assign them to non-cyber focused IT staff, or rely on larger statewide government cybersecurity employees, both of whom may not be particularly familiar with ITS specific security needs.

SCMS and Certificate Costs

Within the Smart Columbus Connected Vehicle Environment, regular IPv6 internet connectivity cost approximately $150 per month per roadside unit (RSU), and SCMS certificate renewals for each RSU ran around $60 annually (2025-SC00515). Utah DOT estimates certificate costs at $50 to $75 per year per RSU, with lower costs for vehicle units (OBUs) [12]. Georgia DOT roughly estimated the cost of implementing an SCMS for the full deployment of planned V2X infrastructure at 1,700 intersections in metro Atlanta to be $240,000 [13]. Beyond per-unit fees, ITS America's deployment guidance indicates that agencies may incur annual license or portal management costs ranging from $10,000 to $100,000, depending on statewide scope and desired features for managing SCMS [14].

Best Practices

Operational Preparedness at TMCs

ITS devices like traffic signals and dynamic message signs (DMS) rely on TMCs to manage increasingly complex and connected systems, necessitating foundational cybersecurity practices. Commonly employed safeguards include routinely scanning network-attached devices, placing vendor-supported software within a demilitarized zone (DMZ) separate from the core network, and implementing access control lists (ACLs) to restrict access to only essential devices and services—all practices aligned with Center for Internet Security (CIS) Controls and promoting robust defense-in-depth architecture (2021-L01016).

> Conduct regular penetration tests, and red-team exercises to uncover and remediate system weaknesses before they are exploited.

Incident Response and Information Sharing

Effective cybersecurity also hinges on prompt collaboration. Sharing incident-related information among TMCs and stakeholders improves situational awareness and coordination during response activities (2022-L01087). Agencies may also find vulnerabilities in vendor

products and should report them as vulnerability disclosures, allowing the vendor to address the issue and patch any system used by other DOTs. These findings may also be published by Cybersecurity and Infrastructure Security Agency (CISA) [15], alerting the public to known risks.

Planning for SCMS Deployment

For V2X deployments, deploying SCMS functionalities needs careful pre-deployment validation. For instance, the Connected Vehicle Pilot Deployment (CVPD) team collaborated with USDOT SCMS developers and vendors to develop a national SCMS, yet certain features disrupted local operations, prompting a rollback to earlier versions. In New York City, proactive risk mitigation across site deployments (including TMCs and network security) helped avoid such delays (2023-L01176). Furthermore, agencies deploying onboard units (OBUs) should anticipate additional time for SCMS registration, particularly as Original Equipment Manufacturers (OEMs) may face challenges scaling and enrolling units, which can delay broader deployment timelines (2023-L01192).

Digital Infrastructure and Workforce Readiness

The DOT workforce must be prepared to manage the advances in digital infrastructure (DI), the massive amount of data required to enable it, and associated risks. Managing DI requires managing and harnessing ITS data through careful identification of data needs, data types, and analytics, as well as strategic investments in cybersecurity for data streaming and storage. DOTs can strengthen institutional readiness by allocating resources to workforce development in emerging technologies and cybersecurity, while also deploying real-time traffic and connected and automated vehicle (CAV) data dashboards to equip TMC operators with the tools needed to securely access, analyze, and act on critical data and any cyber incidents (2023-L01178).

Table 1: Summary of Key Considerations for ITS Cybersecurity

ITS Cybersecurity Topic	Key Considerations
Network Preparedness	Routine device discovery and network scanning; deploying vendor-supported systems within a DMZ; implementing ACLs to limit access to essential devices and services.
Incident Response	Establishing information-sharing protocols to enhance situational awareness and coordinated cybersecurity response.
SCMS Deployment	Conducting pre-deployment testing and validation of SCMS functionalities; developing contingency plans for potential interoperability issues; allowing adequate time for device registration and coordination with OEMs to avoid deployment delays.
Audit & Monitoring	Maintaining regular audit logs to support oversight, detect anomalies, and facilitate early incident detection and response.

ITS Cybersecurity Topic	Key Considerations
Digital Infrastructure and Workforce Readiness	Investing in workforce development for emerging technologies and cybersecurity; managing CAV and real-time traffic data through secure analytics platforms; deploying dashboards to enhance operator visibility and secure decision-making.

Success Story

Overview

The Georgia Department of Transportation (GDOT) launched a comprehensive cybersecurity initiative to protect its extensive edge network of more than 8,000 remote devices, including traffic signals, ramp meters, cameras, dynamic message signs, weather sensors, and roadside units [16]. This effort was driven by the growing cybersecurity threat landscape and the need to modernize aging communications infrastructure.

Background

As GDOT's legacy communications hardware approached end-of-life, the agency recognized the opportunity to refresh its technology with a strong focus on cybersecurity. The Office of Information Technology (IT) worked closely with the Transportation Systems Management & Operations (TSMO) teams to establish requirements for new edge devices. These requirements included:

- Multi-modal communications (fiber and cellular)
- Port availability
- Field-hardening
- Power over Ethernet (PoE)
- Advanced network management
- Embedded firewall capabilities

Figure 3: Georgia DOT deploying Palo Alto Networks PA-450 series firewalls to secure edge network communications, enhancing cybersecurity across the state's transportation infrastructure (Source: NOCoE)

GDOT selected a firewall solution that met its evaluation criteria of durability, security, and connectivity needs across diverse deployment contexts.

Deployment & Execution

Delivering the initiative required cross-functional collaboration across TSMO, ITS operations, maintenance, communications design, and IT. Together, teams developed standardized installation procedures, template-based configurations, and one-touch provisioning guides.

This standardized approach enabled rapid scaling, with field crews deploying an average of 50 devices per week while minimizing setup errors. In addition, the framework provided over 100 cities, counties, and regional agencies with secure, replicable deployment models and practices.

Outcomes, Benefits, and Learnings

By embedding cybersecurity into system design rather than treating it as an afterthought, GDOT established a proactive and resilient infrastructure posture. Benefits included:

- Reduced system outages and emergency response needs
- Lower downstream recovery costs
- Improved readiness for major event management and evolving cyber threats
- Replicable cybersecurity practices for statewide and partner use

Figure 4: Georgia DOT wins 2025 TSMO Award for Cybersecurity and TSMO (Source: NOCoE)

This initiative not only enhanced GDOT's operational resilience but also earned the agency the **Cybersecurity and TSMO Award** in the 2025 TSMO Awards from the National Operations Center of Excellence (NOCoE), recognizing its forward-looking and strategic deployment approach.

References

[1] "ITS Cybersecurity | ITS Deployment Evaluation." Accessed: Sept. 22, 2025. [Online]. Available: https://www.itskrs.its.dot.gov/briefings/executive-briefing/its-cybersecurity

[2] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 04162018, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[3] H. Tran, C. Sames, C. B. Casey, J. N. Snyder, and D. Weitzel, "Intelligent Transportation Systems (ITS) Cybersecurity Framework Profile." Accessed: Sept. 22, 2025. [Online]. Available: https://rosap.ntl.bts.gov/view/dot/72769

[4] M. C. Ramon, A. T. Dodson, J. P. Wolff, and J. R. Sapphire, Cybersecurity Issues and Protection Strategies for State Transportation Agency CEOs. Washington, D.C.: Transportation Research Board, 2023. doi: 10.17226/27024.

[5] "Cost of a data breach 2025 | IBM." Accessed: Sept. 22, 2025. [Online]. Available: https://www.ibm.com/reports/data-breach

[6] "Cybersecurity Assessment Tool for Transit (CATT): Self-Assessment Package | FTA." Accessed: Sept. 22, 2025. [Online]. Available: https://www.transit.dot.gov/research-innovation/cybersecurity-assessment-tool-transit-catt-self-assessment-package

[7] R. Jolly, "Transportation Management Centers: Data and Cybersecurity," Best Practices.

[8] "Cyber Hygiene Services | CISA." Accessed: Sept. 22, 2025. [Online]. Available: https://www.cisa.gov/cyber-hygiene-services

[9] "Connected Vehicle Traffic Signal System." Accessed: Sept. 22, 2025. [Online]. Available: https://www.arc-it.net/html/servicepackages/sp43.html

[10] R. Gabel, C. Sames, H. Martinez, P. Miller, and M. Vanderveen, "Intelligent Transportation Systems (ITS) Security Control Set for Traffic Signal Controllers." Accessed: Sept. 22, 2025. [Online]. Available: https://rosap.ntl.bts.gov/view/dot/72772

[11] San Francisco Municipal Transportation Agency (SFMTA), "Agreement between the City and County of San Francisco and WSP/PGH Wong Joint Venture", Contract No. SFMTA-2024-20-FTA. Available: https://www.sfmta.com/media/40167

[12] Connected Intersections Program: Program Management and Technical Support, "Connected Intersections Guidance Document – Revision 1, May 2024". Accessed October 6, 2025. Available: https://engineering.virginia.edu/sites/default/files/Connected-Vehicle-PFS/Resources/CI%20Guidance%20Document%20Revision%201%20FINAL.pdf

[13] "Vehicle-to-Everything (V2X) Technology | ITS Deployment Evaluation." Accessed: Sept. 22, 2025. [Online]. Available: https://www.itskrs.its.dot.gov/briefings/executive-briefing/vehicle-everything-v2x-technology

[14] ITS America, "ITS America V2X Deployment Plan," ITS America, 2023. [Online]. Available: https://itsa.org/wp-content/uploads/2023/04/V2XDeploymentPlan.pdf

[15] "Coordinated Vulnerability Disclosure Program | CISA." Accessed: Dec. 11, 2025. [Online]. Available: https://www.cisa.gov/resources-tools/programs/coordinated-vulnerability-disclosure-program

[16] "Deployment of Palo Alto Firewalls to Secure GDOT's Edge Network | National Operations Center of Excellence." Accessed: Sept. 22, 2025. [Online]. Available: https://transportationops.org/case-studies/deployment-palo-alto-firewalls-secure-gdots-edge-network