National Operations Center of Excellence

Peer Exchange Report

Cybersecurity for TSMO

Virtual Peer Exchange
August 4–5, 2026

Table of Contents

Executive Summary 3

Background 4

What Every Agency Can Do Now 4

Day 1 — August 4, 2026 6

Welcome and Purpose 6

Session 1 — The Threat Landscape and Overall Context 6

Perspective from Cipher Roadways (Ed Fok) 6
Perspective from New Jersey DOT (Jeff Rockower) 7
Perspective from New Jersey DOT (Steven Prichard) 8
Perspective from the USDOT ITS Joint Program Office (Justin Anderson) 8
Discussion 8

Session 2 — People, Process, and Technology 9

Perspective from Utah DOT (Troy Peterson) 9
Perspective from Caltrans (Dirk Spaulding) 11
Perspective from Caltrans, statewide (Kevin Riley) 12

Session 3 — Securing the Existing TSMO Environment 12

Perspective from Southwest Research Institute (Lynne Randolph) 12
Perspective from New Jersey DOT (Jeff Rockower) 13
Perspective from Texas DOT (Edward Darnell) 14
Perspective from Cipher Roadways (Ed Fok) 14
Discussion 14

Day 2 — August 5, 2026 15

Session 4 — Tools, Procurement, and Vendor Management 15

Perspective from Southwest Research Institute (Sabrina Mosher) 15
Perspective from EtherWAN (Jim Toepper) 16
Discussion 16

Session 5 — Agency Case Studies 17

Perspective from New Hampshire DOT (Nicholas King and Steve Lemire) 17
Perspective from the Greater Dayton Regional Transit Authority (Shawn Prince) 18
Perspective from Georgia DOT (Justin Hatch, Steve Ainsworth, and Joshua Miller) 18

Session 6 — National Cooperative Efforts and What's Next 20

Perspective from FHWA (Joseph Gregory) 20
Perspective from Clemson University and TraCR (Ronnie Chowdhury) 20
Perspective from ITE and the standards community (Siva Narla) 20
Discussion and 90-day actions 21

Key Learnings and Next Steps 21

Resources 23

Appendix A — Agenda 24

Executive Summary

Six findings carried across the two days:

- **The threat landscape changed materially in the past year.** Presenters described nation-state cyber tools now in wide use, adversaries using transportation systems as an intelligence and targeting platform, and artificial intelligence (AI) collapsing the time between finding a vulnerability and fielding a working exploit. The panel's recurring conclusion: preventing every attack is no longer realistic, so detection speed and the ability to recover now matter as much as prevention.
- **"Who owns cybersecurity" remains unsettled, and the fix is governance, not tools.** The agencies making progress all formalize the relationship between operations and the state Chief Information Officer (CIO) or Chief Information Security Officer (CISO) through memoranda of understanding (MOUs), embedded staff, a clear line for who owns what past the firewall, and a named authority to accept risk and make security decisions. But CISO offices often lack an understanding of operational technology (OT), and OT operators rarely see the CISO's security requirements.
- **Segmentation is the single highest-return control.** Every technical panel converged on it. Dividing the network so a compromise cannot spread limits the damage "to just what you can afford to lose." The panels ranked asset inventory and visibility next, on the principle that you cannot protect what you cannot see. Patching came third. It is uniquely hard in the field, because a patch can break compatibility or disable a device that must run for 15 to 20 years.
- **Procurement decides cybersecurity outcomes.** No single mandated cybersecurity standard governs intelligent transportation systems (ITS). Presenters pointed to NCHRP Report 03-127, the ISA/IEC 62443 series, federal supply-chain rules, software bills of materials, and shared model specification language as the available levers. The hardest part of the problem is the installed base; the equipment agencies bought before cybersecurity became a requirement.
- **The agency case studies followed a repeatable arc.** Modernize the network from a flat design to a routed one, build in redundancy, gain visibility into devices and traffic, automate routine work, and only then add continuous monitoring. New Hampshire DOT, Georgia DOT, and the Greater Dayton Regional Transit Authority each arrived at this pattern independently. The body of this report walks through each session of the Peer Exchange in the order of the agenda, with figures drawn from the presenters' own slides. It closes with consolidated key learnings, the next steps to advance the adoption of AI for TSMO, and the public resources referenced during the event.
- **The national pipeline is active but uncoordinated, and information-sharing is the systemic gap.** Federal research centers, cooperative research projects, a forthcoming ITE standard, and a pooled-fund study are all in motion. Yet no mandatory standard exists, no cyber testing regime covers devices, and no mechanism lets agencies share incident details the way the National Transportation Safety Board shares crash findings. Several speakers asked FHWA to condition federal funding on meeting a cybersecurity standard.

Background

The National Operations Center of Excellence (NOCoE) convened a two-day virtual peer exchange, Cybersecurity for TSMO: Strategies and Applications, on August 4 and 5, 2026. Transportation Systems Management and Operations (TSMO) is the discipline of running the existing transportation network safely and efficiently, and it now depends on thousands of networked field devices: signal controllers, cameras, message signs, detectors, and roadside units. A peer exchange is a working, peer-to-peer conversation among the people who operate those systems. The agencies in the room came to compare what they are doing, not to hear a set of lectures.

This exchange followed NOCoE's 2025 Cybersecurity and Information-Technology Peer Exchanges. Those earlier sessions established that cybersecurity is now foundational to transportation operations rather than an information-technology (IT) afterthought. NOCoE Director Nicholas Ramfos opened the Peer Exchange by moving the group from awareness to action, and he organized both days around three questions: Who owns cybersecurity inside an agency? How do you secure the field? And what works? Ramfos asked every participating agency to leave with a concrete 90-day action plan.

The program ran as six sessions across two days. Day 1 mapped the threat landscape, examined the relationship between TSMO and state IT and cybersecurity offices, and got concrete about securing existing field equipment. Day 2 turned to procurement, agency case studies, and the national research and standards pipeline. Speakers came from state departments of transportation and a transit authority, from the U.S. Department of Transportation (USDOT) and the Federal Highway Administration (FHWA), Clemson University, and the standards and industry community, including the Institute of Transportation Engineers (ITE), the American Association of State Highway and Transportation Officials (AASHTO), and ITS America.

This report follows the order of the sessions and addresses a reader who was not in the room, so it explains each program, standard, and term at first use.

What Every Agency Can Do Now

The recommendations below recur across all six sessions. They run roughly in the order an agency can take them on: governance first, because every other item depends on someone owning it, then from the quickest to start to those that reduce the most risk over time. None requires new legislation, and most can begin with existing staff and budget.

#	*Action every agency can take now*	*Why it matters*	*Where it came up*
1	**Establish governance in writing** — an MOU that names who owns what past the firewall, who can accept risk, and who leads during an incident.	Removes the ambiguity that stalls incident response and leaves OT requirements unshared.	Peterson (DTS), Spaulding/Riley (CalSTA), King
2	**Inventory every field device** — model, firmware, location, age, and connections.	You cannot protect what you cannot see, and you cannot plan a lifecycle or a patch you cannot find.	Rockower, Randolph, Mosher, King; GDOT (NetBox)
3	**Segment the network** so one compromised device cannot reach the rest.	The single highest-return control; it limits the blast radius to what you can afford to lose.	Every technical panel; unanimous in Session 3

#	*Action every agency can take now*	*Why it matters*	*Where it came up*
4	**Separate the IT and OT networks** and keep data-sharing interfaces off the device-control network.	An email-borne IT compromise should never reach signals and safety devices.	Mosher, Randolph, Toepper (dual firewalls)
5	**Kill default passwords and easy cabinet keys.** Force a credential change on first power-on; replace the "number-2" key.	The cheapest, most-exploited way in; keys sell online for about $20.	Fok, Peterson (CyberKeys), Prichard
6	Enforce least-privilege access with multi-factor authentication and background checks.	Most breaches ride in on over-broad access; people are the largest risk surface.	Peterson, Randolph, Toepper (RADIUS/TACACS+)
7	**Write cybersecurity into procurements** — NCHRP Report 03-127 language, a recognized device standard, a software bill of materials, and supply-chain screening.	Procurement decides cyber outcomes before a device is ever in the field.	Prichard, Mosher, Toepper
8	Treat scans, patches, and firmware changes as engineering changes — test, keep a rollback, use a maintenance window.	In OT a routine IT action can brick a device or knock out signals across a region.	Randolph, Darnell, Fok
9	**Give the security team eyes on the OT network** — centralized logging, time sync, and OT-aware monitoring that traffic operations and the security team share.	Blind spots between IT and OT are where attackers dwell; every case study added visibility before continuous defense.	King/Lemire (Cyber Vision, MSSP), Miller (NDR, logging), Mosher, Spaulding
10	**Write an incident response plan and exercise it** — name who leads (the CISO-triage model Riley described), put public safety first, run tabletops, and build or refresh a continuity-of-operations plan.	It moves leadership to fund the work and finds gaps before an incident does.	Riley, Contestabile, Darnell, Prince, King (CISA)
11	**Do a "level-zero" self-assessment and repeat it** — baseline the agency, then show whether controls are reducing risk.	Establishes a baseline, a first step for agencies just getting started, and a yardstick for progress.	Prichard, Narla, Lemire (90-day action)
12	**Share what happens to you.** Support disclosing incidents so peers can learn from them.	The community's biggest systemic weakness is that breaches go unreported.	Fok (both days), Session 6 panel

Day 1 — August 4, 2026

Welcome and Purpose

Nicholas Ramfos welcomed the group and framed the two days as a move from awareness to action. He set the three organizing questions and asked each agency to commit to a 90-day action, which the group would capture at the close of Day 2.

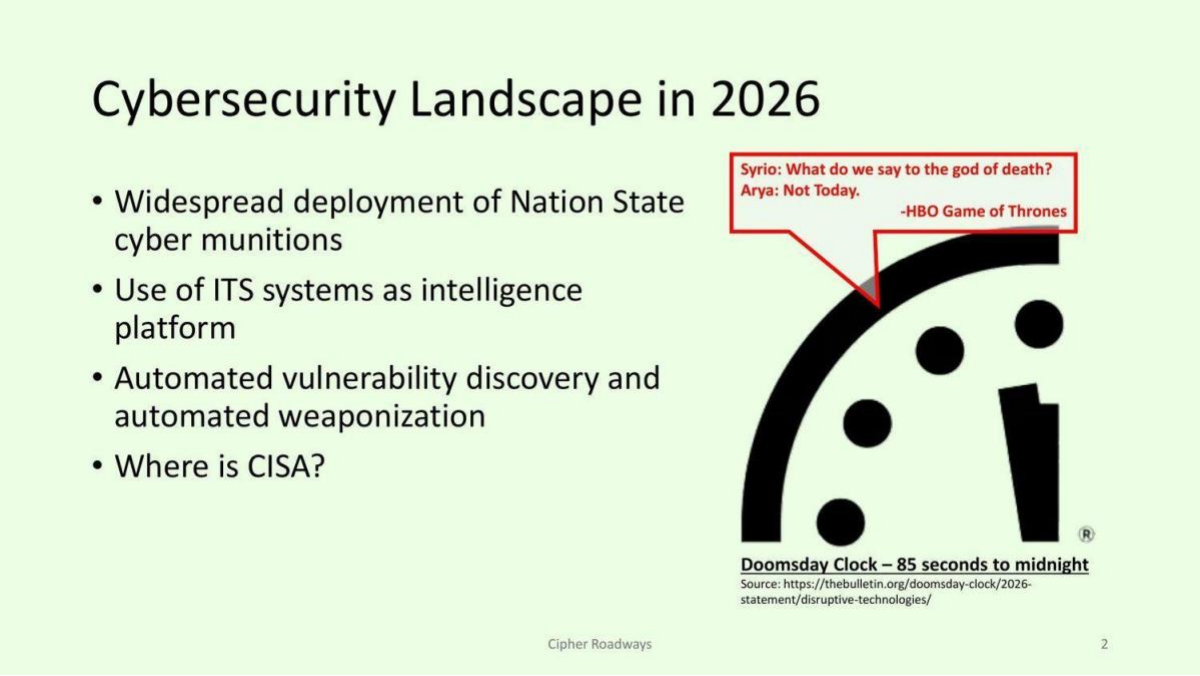
Session 1 — The Threat Landscape and Overall Context

Moderator: Laurie Matkowski, NOCoE Technical Advisory Committee. Panel: Jeff Rockower, New Jersey DOT; Steven Prichard, New Jersey DOT; Ed Fok, Cipher Roadways; Justin Anderson, USDOT ITS Joint Program Office.

Matkowski opened with the two documents meant to guide the field: the ITS Cybersecurity Framework Profile and the FHWA Transportation Cybersecurity Strategic Plan. She asked the panel which threats are genuinely new, where the frameworks help and where they stop short, and what exposure is most under-appreciated.

Perspective from Cipher Roadways (Ed Fok)

Fok, representing ITE and reporting back from the year's major security conferences, argued that what was true a year ago is no longer true today. Theoretical threats have become realized ones, and the transportation sector now sits inside the blast radius. He organized the shift around four points.



Ed Fok's threat brief opened the exchange: nation-state cyber tools in wide use, transportation systems used as an intelligence platform, and the automation of both vulnerability discovery and weaponization. Source: Cipher Roadways.

First, nation-states now deploy cyber tools widely, and the sector has seen a supply-chain implant reach a single targeted device through the manufacturing chain of an ordinary consumer product. Second, and most novel, adversaries have begun using transportation systems as an intelligence platform. Rather than disrupting operations, a capable actor can use ITS cameras and data to build a pattern of life, to target, and to assess damage after an event. Third, AI now finds vulnerabilities and weaponizes them automatically, compressing a process that used to take years into days and putting capable offensive tools in the hands of low-skilled actors. Fourth, agencies can no longer count on the free, publicly funded threat-intelligence resources they have leaned on, which makes their own preparation more important.

Fok's practical message was blunt. Advanced persistent threats are patient and quiet, so an agency should assume a capable adversary may already sit on the network. Most agencies built their procedures around ransomware, phishing, and financial fraud. Few have planned for a harder case: what an operator sees on a workstation may not match what is happening in the field. He urged agencies to practice their recovery procedures, test their backups, and design systems to fail safely. He closed on the theme he would return to on Day 2: the community does not share its breaches, so attackers exploit the same entry points repeatedly, and no one learns how they got in. An attacker, Fok noted, can be bad at offense and still know it, but a defender can be bad at defense and never find out.

Looking forward, Fok pointed to concrete fixes within reach. The forthcoming ATC 5501 specification for advanced transportation controllers will reduce field-system vulnerabilities, including retiring the trivial cabinet key and ending default credentials such as a five-zero access code. He pressed agencies to abandon weak passwords, to collaborate with vendors to obtain patches and then deploy them, and to treat AI as a tool that will strengthen resilience if used deliberately.



Fok's "looking forward" slide: ATC 5501, an end to weak passwords, real patch deployment, and a call to share experiences. Source: Cipher Roadways.

Perspective from New Jersey DOT (Jeff Rockower)

Rockower, an ITS engineer with a cybersecurity master's degree and a representative of the ITS America Cybersecurity Community of Practice, argued that security starts with knowing what you have. An agency needs an inventory of its field assets, their age, and their vulnerabilities before it can defend anything. He urged agencies to build cybersecurity from the problem-statement stage of a project rather than bolt it on

after a construction contract has locked the scope. Traffic signal cabinets, he noted, are largely "set-and-forget" equipment that sits physically exposed, and an intruder who buys a cabinet key online can get in and interfere. Rockower also flagged the trend toward software-based conflict monitors as a concern, and he warned that decades-old controllers carry a looming clock-rollover problem.

Perspective from New Jersey DOT (Steven Prichard)

Prichard, New Jersey DOT's agency Chief Information Security Officer and chairman of AASHTO's Transportation Cybersecurity Community of Practice, named three primary threats: phishing and ransomware that now reach both enterprise and OT systems, exploitation of legacy OT that lacks modern security, and sophisticated probing of the agency's external-facing infrastructure. He used both national frameworks to build New Jersey DOT's first cybersecurity strategic plan, a multi-year plan spanning IT, OT, and connected devices. On procurement, he wrote contract language so that purchased assets are not already years old or near end-of-life on the day they arrive, and he generalized that language to share through the AASHTO group. He advised agencies just starting to master the basics first, from consistent network protocols to synchronized clocks, and to take the first step. On the reality of patching legacy devices one at a time, he offered a line that landed with the room: out of 200 devices, he had bricked only two, and he would take that result.

Perspective from the USDOT ITS Joint Program Office (Justin Anderson)

Anderson manages the Joint Program Office's work on ITS architecture, standards, cybersecurity, interoperability, and vehicle-to-everything (V2X) communications. He described a global benchmarking effort, now feeding a forthcoming report, that took FHWA staff to Estonia, the United Kingdom, and Germany. He highlighted AI-crafted phishing convincing enough to fool cybersecurity professionals, the case for funded collaborative threat-hunting across federal, state, and local partners, and the need to make the ITS Cybersecurity Framework readable for transportation staff who are not career cyber specialists. He recounted Estonia's "digital embassy," a complete backup of the national government hosted in another country that could restore digital services within hours, and he asked whether U.S. agencies have thought about geographically separate backups. For the whole field, Anderson argued that it is not a question of whether attackers will compromise an agency, but when. That makes fast detection nearly as valuable as prevention. From the United Kingdom benchmark, he offered a concrete cost: attackers changed a message sign to read "event canceled," turned attendees away, and cost the event real money.

Discussion

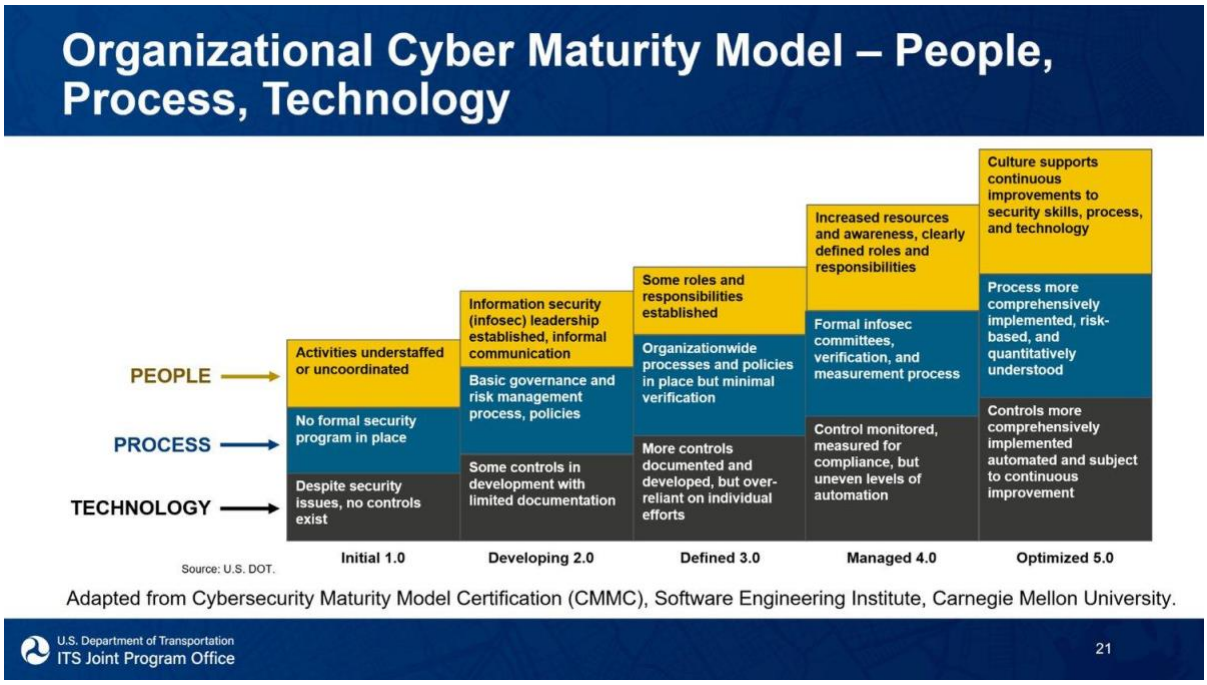
The panel agreed that the genuinely new threat is the shift from disruption to intelligence use of transportation systems, combined with the speed of AI-driven exploitation. On the frameworks, the panel valued them as visioning and starting tools but noted they are not mandatory. Rockower suggested FHWA tie funding to a verified cybersecurity protection level. When asked about the most under-appreciated exposure, the panel pointed to patching, the shortage of vendor-agnostic tools for administering OT devices, and the difficulty of getting a software bill of materials for old equipment. Prichard described a low success rate, roughly one in seven, when he asks vendors to build interim security fixes for legacy gear.

The conversation closed on special events. New Jersey DOT came through the FIFA World Cup matches with no security incidents across a region that included Philadelphia, a result Prichard credited to public-private information sharing, a constant CISA presence, and the state's cybersecurity integration cell. A major event such as FIFA sets requirements rather than asking, he noted, and the DOT was one player among many. Anderson broadened the point to natural events such as wildfires, hurricanes, and evacuations, which can serve as cover for an attack. Fok tied the thread back to information sharing: the Cyber Incident Reporting for Critical Infrastructure Act arrived because the sector has not reported on its own.

Session 2 — People, Process, and Technology

Moderator: John Contestabile, Skyline Technology Solutions. Panel: Troy Peterson, Utah DOT; Dirk Spaulding, Caltrans District 8; with Kevin Riley, Caltrans.

Contestabile, a former Maryland DOT assistant secretary who has run cybersecurity assessments of several state DOTs, framed the session around three dimensions that must line up: people, process, and technology. In his experience, the technology is the least of the problem. The harder work is a culture in which everyone understands their role, and a workforce whose technical staff, often acting as system administrators in a traffic management center, are not yet career cyber engineers. He presented a maturity model that decomposes the widely used federal cybersecurity framework across those three dimensions, from an initial state to continuous improvement.

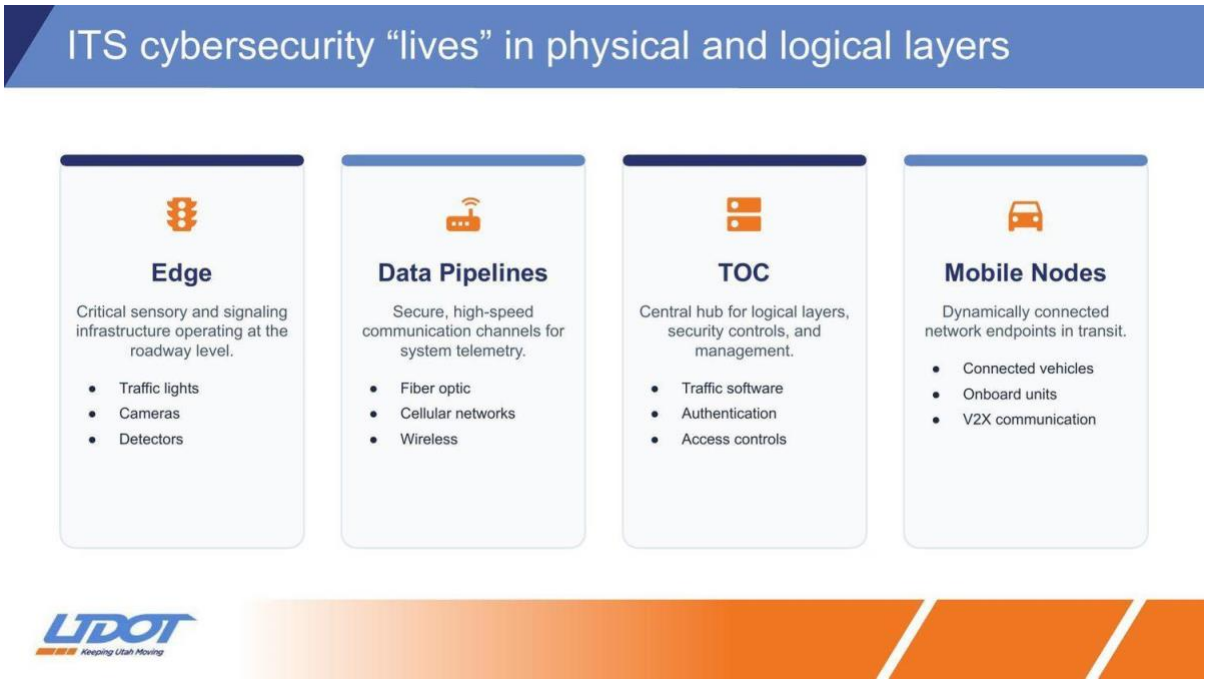


The organizational cyber maturity model Contestabile used to frame the session: people, process, and technology each climb from Initial (1.0) to Optimized (5.0). Source: USDOT ITS Joint Program Office, adapted from the Cybersecurity Maturity Model Certification (Software Engineering Institute, Carnegie Mellon University).

Perspective from Utah DOT (Troy Peterson)

Peterson, Utah DOT's Director of Operations, walked through how his agency built its program, and he grounded it in two cautionary stories. In the first, from 2014, university researchers took control of a municipal signal system by exploiting unencrypted radio, default passwords, and physical access. Utah DOT's early instinct, he admitted, had been to assume that a closed, on-premises system sat above such risks. In the second, from 2019, someone reported suspicious people inside a Utah DOT cabinet; they turned out to be the agency's own consultants working without proper identification. That prompted the agency to rethink who can open a cabinet and how it controls that access.

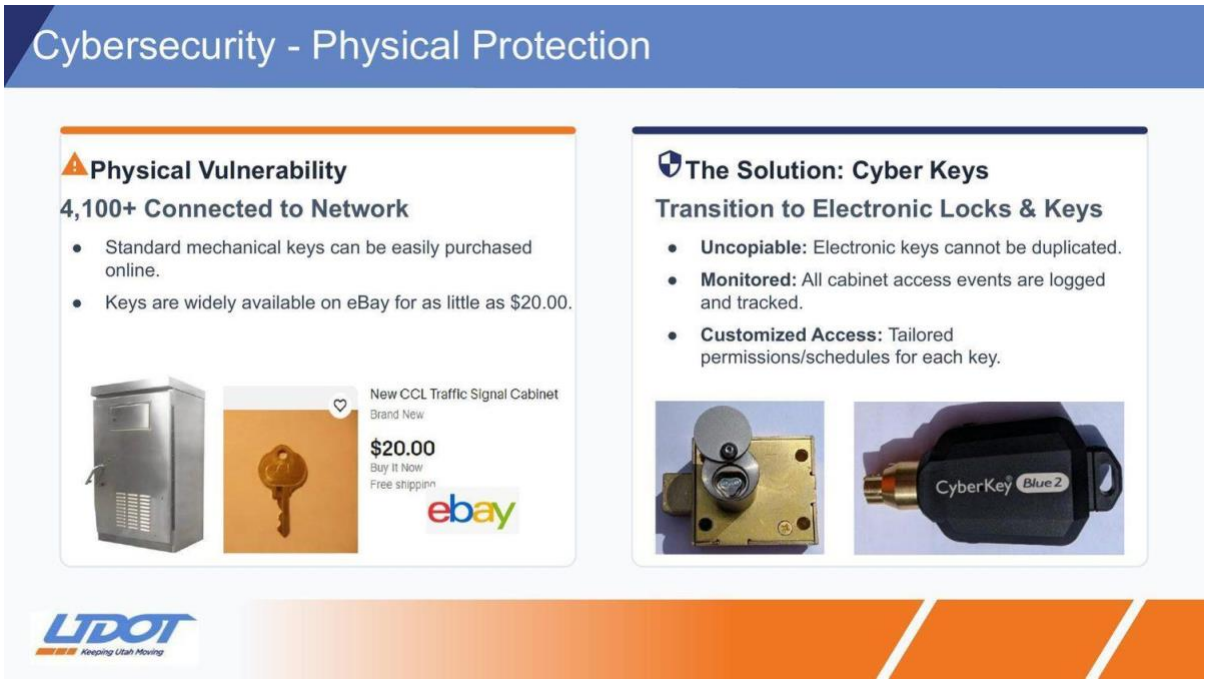
From there Peterson laid out a defense-in-depth model in which cybersecurity lives in both physical and logical layers, spanning the roadway edge, the data pipelines, the operations center, and the mobile nodes of connected vehicles. Employees, he stressed, are the first line of defense and therefore the primary layer of protection, so the agency treats awareness and training as foundational.



Utah DOT frames ITS cybersecurity as living in physical and logical layers, from the roadway edge to the operations center to connected-vehicle mobile nodes. Source: Utah DOT.

On policy and access, Utah DOT requires annual cybersecurity awareness training under state code, uses multi-factor authentication for system access, and requires background checks and formal approval for any network user, including consultants. The agency strictly limits and monitors access, a deliberate move away from the sweeping rights it granted in earlier years. The relationship with the state Department of Technology Services (DTS) defines the Utah model: dedicated DTS staff sit inside the traffic operations center under an MOU and bring network and cybersecurity expertise. The line stays clear: DTS owns everything past the firewall, and Utah DOT owns the transportation and signal systems.

On physical security, Peterson was pointed about the humble cabinet key. Standard mechanical keys sell online for as little as $20, so Utah DOT moved to electronic CyberKeys that no one can duplicate, which log every cabinet access, and carry tailored permissions and schedules. The agency connects more than 4,100 devices to the network, and it locks the operations center around the clock.



Utah DOT replaced mechanical cabinet keys — available online for about $20 — with electronic keys that no one can copy and that log every access. Source: Utah DOT.

The network underpins all of it. Utah DOT runs a 4,000-mile private fiber network protected by both state and agency firewalls, with tightly controlled access and encryption for any sensitive data crossing public infrastructure. Peterson described the Utah DOT and DTS networks as physically separate but functionally integrated, and he invoked Robert Frost's line that "good fences make good neighbors." The separate fibers and dedicated hardware limit the agency's exposure to the larger and more attractive state network, restrict the ITS network's entry and exit points, and preserve operational independence in a crisis, while unified cloud services and support keep the two sides working together.

Perspective from Caltrans (Dirk Spaulding)

Spaulding, from Caltrans District 8 (San Bernardino and Riverside counties), presented the Caltrans experience. Kevin Riley, who provides statewide oversight, deliberately stepped aside so the room could hear from someone doing the work in a district. Spaulding argued that asset visibility is the prerequisite to securing OT. After an extensive selection process, Caltrans chose Cisco Cyber Vision to see its OT assets and Cisco Identity Services Engine with network access control to enforce policy, and it is deploying both on the OT networks in every district statewide.

The biggest challenge is the legacy equipment: a wide range of device types and ages on a roughly 10-year lifecycle standard, a long time in cybersecurity terms. Older equipment supports modern authentication protocols inconsistently and demands heavy tuning, and the vendors themselves were still learning OT networks. On the human side, Spaulding argued plainly that the CISO office needs a deeper understanding of OT. He recounted a pointed exchange in which a CISO worried about answering for an incident on the OT network, and Spaulding replied that the CISO should answer for it, because that office had not shared its security requirements with the people running those networks. Caltrans has since worked for years to establish the MOUs between operations and IT that put those responsibilities in writing. On procurement, the agency is moving away from letting a contractor select minimum-specification networking gear and toward standardized, pre-tested, statewide-consistent equipment, alongside a program to replace aging field equipment out of the risk pool.

Perspective from Caltrans, statewide (Kevin Riley)

Riley added the statewide context. Caltrans operates 12 traffic management centers whose evolution mirrors the changing relationship between traffic operations and IT: the older centers remain more traffic-operations-centric and are shifting toward shared responsibility, and a new statewide project will define the centralized relationship more concretely. Under state policy, security is an IT responsibility, and an MOU with the state transportation agency traces back to the 1993 traffic management center master plan. Riley was candid that much of his job is managing the turf between IT and traffic operations. On incident response, a quick top-down decision from the CISO determines whether the operations team or the enterprise IT organization leads, and Riley named clearer roles and responsibilities as the biggest gap to close.

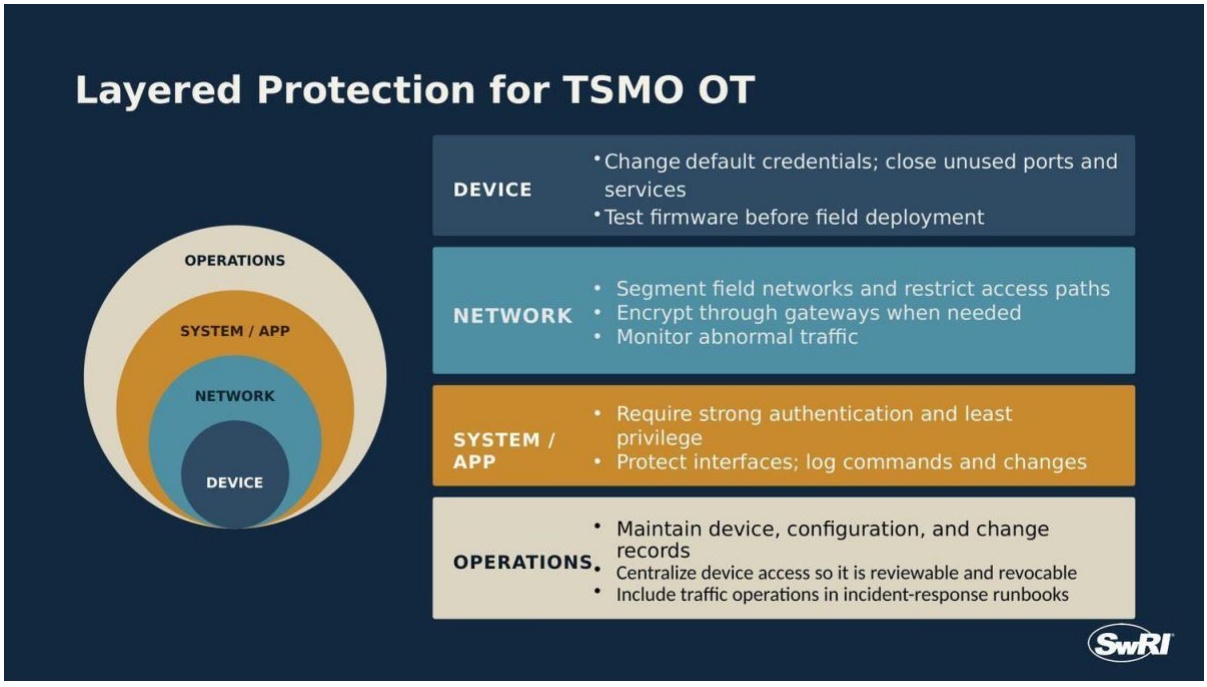
Session 3 — Securing the Existing TSMO Environment

Moderator: Jim Toepper, EtherWAN. Speakers: Lynne Randolph, Southwest Research Institute; Jeff Rockower, New Jersey DOT; Edward Darnell, Texas DOT; Ed Fok, Cipher Roadways.

This session got concrete about the convergence of IT and OT, and about securing equipment no one designed for today's threats.

Perspective from Southwest Research Institute (Lynne Randolph)

Randolph, an Institute Engineer at Southwest Research Institute, laid out a layered protection model for connected field environments. Field devices that once sat isolated on their own networks now connect to central systems, enterprise IT, vendors, and the cloud, and no one designed them for that exposure.



Southwest Research Institute's layered model: push protection to the device where possible, and when a device cannot support a control, move the protection outward to the network, system, and operations layers. Source: Southwest Research Institute.

Her model works from the device outward. At the device, change default credentials, close unused ports, and test firmware before field deployment. At the network, segment field networks, restrict access paths, encrypt through gateways when the device itself cannot, and watch for abnormal traffic. At the system layer, require strong authentication and least-privilege access and log every command and change. At the operations layer, keep device and configuration records, centralize access so it stays reviewable and revocable, and write traffic operations into incident-response runbooks. Her governing principle: when a device cannot support a control, move the protection outward to the next layer.

Randolph then warned that a security control can itself become an operational risk. Aggressive vulnerability scanning can overwhelm and shut down field devices. Patching can fix a vulnerability but break protocol compatibility. Many field devices cannot support encryption, certificates, multi-factor authentication, or monitoring agents at all. And full replacement is slow and expensive, because field device lifecycles run 15 to 20 years and swapping one device can require installation work and central software updates.



A control that is routine in enterprise IT can be a hazard in the field: scans can knock devices over, patches can break compatibility, many devices cannot support modern controls, and replacement runs on a 15-to-20-year cycle. Source: Southwest Research Institute.

Randolph concluded that agencies should treat scans, patches, and configuration changes in the field as engineering changes, not routine IT administration. She also noted that data sharing with vendors, the cloud, and connected-vehicle platforms widens the security boundary, so an agency should document each new connection and keep its interface separate from the device-control network. Her closing line captured the balance the session was after: “OT should not get a pass on cybersecurity, but securing it requires controls that respect how transportation systems operate.”

Perspective from New Jersey DOT (Jeff Rockower)

Rockower explained why OT security is different by inverting the classic security priorities. Enterprise IT protects confidentiality first. OT runs backward, prioritizing availability, then integrity, then confidentiality, because the systems have to keep running and may not have rebooted in years. He contrasted a hardened data center, with its biometric access and fire suppression, against a field cabinet exposed to weather, power fluctuations, and cheap keys. Many field devices still speak older, plaintext network protocols or serial connections, and encryption from 15 years ago breaks in seconds. He pointed to the international standard

for industrial control zoning as a way to group devices, and he praised micro-segmentation as one of the best things to happen to networking. He cited a cautionary example of the supply-chain risk hiding inside open-source software: the recently discovered backdoor in a common compression utility, slipped into a barely maintained dependency, that nearly reached widely used systems. He also flagged the quiet risk of losing institutional knowledge as staff turn over.

Perspective from Texas DOT (Edward Darnell)

Darnell argued that no agency is alone in this: the work repeats, and peers are solving the same problems. He found it hardest to define assets and boundaries across a state with 25 districts that had each configured edge equipment differently, some with default passwords still in place. Because OT does not tolerate the network sweeps that standard IT tools use, Texas DOT procured an OT-specific tool. He described a case in which someone reassigned network address space from the business side to traffic without warning the cybersecurity team, so a routine scan knocked out signals and roughly 100 municipalities had to roll trucks to recover. The agency now runs monthly tabletop exercises built around realistic scenarios, which build the relationships and shared contact lists that matter during a real incident. It also pushes security upstream through an architecture-review and change-management process. That process caught and redesigned a proposed solution that would have plugged public-facing cellular equipment directly into the business network.

Perspective from Cipher Roadways (Ed Fok)

Fok demonstrated Shodan live. Shodan is a search engine that indexes internet-connected devices, and as the moderator put it, getting in is sometimes as simple as clicking on an exposed device. On screen Fok found exposed transportation equipment, including a cellular field modem running old firmware that carried a vulnerability first exploited years earlier, and signal controllers showing familiar weak points. He urged agencies to triage what AI-assisted scanning surfaces by its real-world impact. A cosmetic display bug differs from a flaw in a device's clock, communications, or authentication, and not all technical debt is worth fixing. He also flagged a structural blind spot: the commercial tools that monitor OT networks largely stop at the point where the network converts to a serial connection, so the serial bus where many field devices talk stays invisible, and an agency cannot see an attacker there either. There is no magic solution, Fok said, and an agency is only as secure as its weakest link.

Discussion

Asked to name the riskiest device class, the panel divided. Rockower named the cabinet. Randolph named people, arguing that the biggest cybersecurity risk is human and that policy, enforced by leadership, is the answer. Darnell agreed the human is the biggest threat and added the risk of third-party equipment procured through construction projects that simply appears on the network. Asked for the single best return on investment among segmentation, monitoring, and patching, the panel was unanimous: segmentation. Fok recalled penetration tests in which fine segmentation confined a tester to one or two signals, limiting the damage to what an agency could afford to lose. Toepper cautioned that many cities still run large flat networks with no internal routing at all. On reaching devices that are hard to get to, the panel agreed the answer depends on what the device does. On what a vendor should deliver, the room converged on hardened devices shipped with all ports closed and a forced password change on first power-on, and on requiring proof of compliance with a recognized standard. The chat surfaced working examples too, including an agency running centralized authentication in its OT environment on infrastructure kept separate from enterprise IT.

Ramfos closed Day 1 by naming his takeaways: technology is moving faster than expected, so employees are the first line of defense; coordination is essential because everyone is only as strong as the weakest link; and the new term of the day was "threat hunting." Two images stuck with him: a hacked message sign that caused real economic loss in the United Kingdom benchmark study, and the Shodan demonstration.

Day 2 — August 5, 2026

Session 4 — Tools, Procurement, and Vendor Management

Moderator: Mike Brooks, ITS America. Speakers: Sabrina Mosher, Southwest Research Institute; Jim Toepper, EtherWAN.

Brooks, a former cooperative-research program officer, framed the session as the practical follow-on to Day 1: once an agency knows it needs to buy equipment, how does it do so without everything going sideways?

Perspective from Southwest Research Institute (Sabrina Mosher)

Mosher, a Senior Computer Scientist at Southwest Research Institute, presented the risk-assessment method from NCHRP Report 03-127, a cooperative research project on cybersecurity for field equipment. She opened with the scale of the gap: more than 300,000 traffic signal systems operate nationwide, growing by about 2,550 a year, and they run ordinary computing platforms rather than isolated ones. Agencies deployed most of them before cybersecurity was a procurement requirement, and while central traffic-management networks get enterprise-grade attention, field networks often do not.

The method sorts all field equipment into four classes by worst-case consequence, from safety-critical devices such as signal controllers and conflict monitors down through active systems, networking equipment, and passive devices such as cameras. It then scores each device by combining two established techniques, one that classifies the type of threat and one that rates the severity of the risk, weighted across four categories of consequence: harm to people, damage to infrastructure, travel disruption, and public perception.



The NCHRP 03-127 output ranks field devices by risk. Traffic signal controllers and conflict monitors score highest; speed displays and arrow boards score lowest. Source: Southwest Research Institute.

Mosher's mitigations matched the rest of the exchange: maintain an asset inventory, use role-based access, separate the IT and OT networks completely, keep safety-critical devices apart from passive ones, patch and

verify continuously, and carry cybersecurity diligence into procurement, where she has seen brand-new devices arrive that do not support current encryption or meet federal cryptographic standards. She pointed agencies to the project's full reports, the federal cybersecurity framework, the ITS Cybersecurity Framework Profile, the OWASP application-security verification standard, and the ITS control-set templates for signal controllers, message signs, cameras, and roadside units.

Perspective from EtherWAN (Jim Toepper)

Toepper offered a detailed procurement checklist, and it began with a problem statement: unlike the energy sector, which has a mandatory reliability standard, or the federal government, which has cryptographic mandates, ITS has no single mandated cybersecurity standard. Agencies must therefore assemble their own requirements. He used Florida DOT's strict product-qualification process and Caltrans's demanding cyber requirements as the two reference points other agencies can learn from.

For selecting hardware, Toepper walked through five screens. First, screen the supply chain and country of origin, because federal rules automatically disqualify equipment from named foreign manufacturers and their many affiliates. Second, look for recognized security-management accreditation such as the international information-security standard. Third, check the vendor's public vulnerability record through the federal catalog. Fourth, ask for a software bill of materials, because the embedded software inside a device, down to the version of a common cryptographic library, carries its own known flaws. Fifth, and most important, require third-party cybersecurity certification. Here he recommended the ISA/IEC 62443 series, which covers both the development process and the device itself, a rare joint U.S.-and-European standard he expects to become the de facto benchmark for a secure transportation device.

For software and cloud services he added parallel questions: where the company, its engineering staff, and its cloud hosting sit; whether it holds a recognized service-organization audit; and the same vulnerability and software-inventory checks. His questions for any vendor were pointed: how many vulnerabilities, scored how severely, remediated how quickly, disclosed through what process, communicated to customers how, and supported with security updates for how long, and does the company even run a dedicated product security incident response team? On secure hardware itself he listed the features to demand: encrypted firmware, no default username or password, secure boot, multiple user privilege levels, a hardware trust module, and system logging.

On the installed base, Toepper was realistic. No agency can afford to replace everything at once, so he advised agencies to segment the network like an onion, isolate old equipment from new, program the newer devices to shield the older ones from network storms, and adopt a technology-refresh policy on a five-to-seven-year cycle rather than the 15-year drift that leaves outdated protocols in the field.

Discussion

On replacing passwords, Toepper noted that most OT vendors cannot support multi-factor authentication natively, so agencies fall back to centralized authentication protocols borrowed from IT. Asked about follow-on work to NCHRP 03-127, Mosher explained that the original team has moved on, though she has since worked on guidance for agency executives, on wargaming exercises with FHWA, and on incident-response planning. She noted that one of the project's web tools is no longer available and part of its content is dated. From the floor, Fok disclosed that FHWA had halted a follow-on phase of the research because some of the companies whose products the work identified with problems did not want the findings published. It illustrated his Day 1 theme: the industry does not share in the way that would make it safer. On whether letting the CISO's office see into the OT network breaks segmentation, Mosher answered that agencies need monitoring but IT and OT face different threats. No one in the OT world gets compromised by opening a malicious email, but an IT compromise that crosses into OT can put people on the road at risk. Toepper noted the emerging practice of deploying dedicated OT firewalls, since an agency can run two.

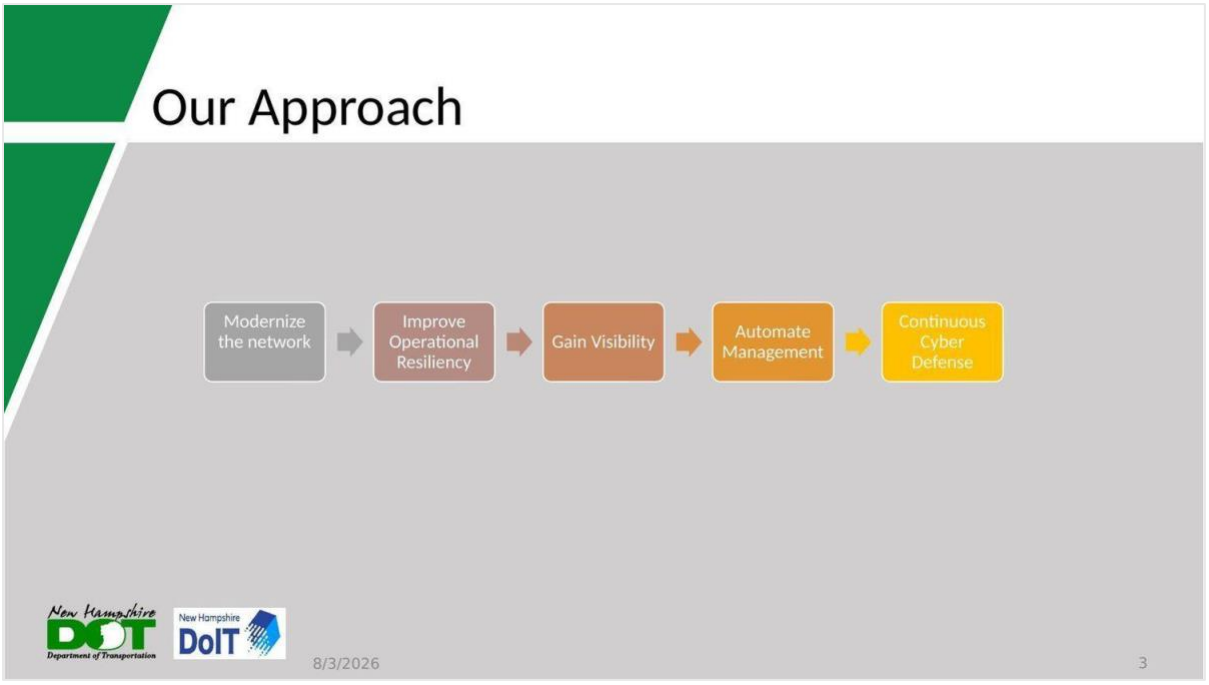
Session 5 — Agency Case Studies

Moderator: Nick Ramfos. Presenters: Nicholas King and Steve Lemire, New Hampshire DOT; Shawn Prince, Greater Dayton Regional Transit Authority; Justin Hatch, Steve Ainsworth, and Joshua Miller, Georgia DOT.

Ramfos asked each agency the same two questions: one decision worth copying, and one to warn against.

Perspective from New Hampshire DOT (Nicholas King and Steve Lemire)

King and Lemire described a journey from infrastructure modernization to cybersecurity operations. New Hampshire's traffic management center became operational in 2007. The agency built it for availability and reliability rather than authentication and monitoring, and as its field technology grew, its exposure grew with it. They could not secure an unreliable network, so modernization came first.



New Hampshire DOT's five-phase path: modernize the network, build operational resilience, gain visibility, automate management, and only then move to continuous cyber defense. Source: New Hampshire DOT / New Hampshire DoIT.

They laid out five phases. First, they built reliable infrastructure, migrating legacy flat networks to standardized routed ones to shrink failure domains. Concrete projects covered the Portsmouth lift bridges, the I-93 backbone, and other corridors, and the move to routing finally solved a reliability problem the old spanning-tree design could not. Second, they built operational resilience with a disaster-recovery site, redundant firewalls and authentication, multiple internet providers, and diverse communication paths. Third, they gained visibility, deploying tools to authenticate devices, automate patching and log collection, and monitor OT communications, on the principle that you cannot protect what you cannot see. Fourth, they automated, using software-defined networking to standardize configurations and provision connections, a step that positions the agency for a zero-trust architecture. Fifth, they moved to continuous defense, issuing a request for proposals for a managed security service provider to deliver around-the-clock monitoring, because transportation incidents, and cyber threats, do not stop at five o'clock. Their decision to copy: build routed backbones. They warned against deploying monitoring sensors everywhere at once and against skipping the asset and fiber inventory, an end to what King called the cowboy days of TSMO. King added that a CISA tabletop exercise had alarmed leadership enough to help secure funding.

Perspective from the Greater Dayton Regional Transit Authority (Shawn Prince)

Prince described a three-year effort to de-complicate the environment before adding to it, using the analogy of a city that grows without a plan versus one built with zones, and the rule that if you cannot secure something, you should isolate it.



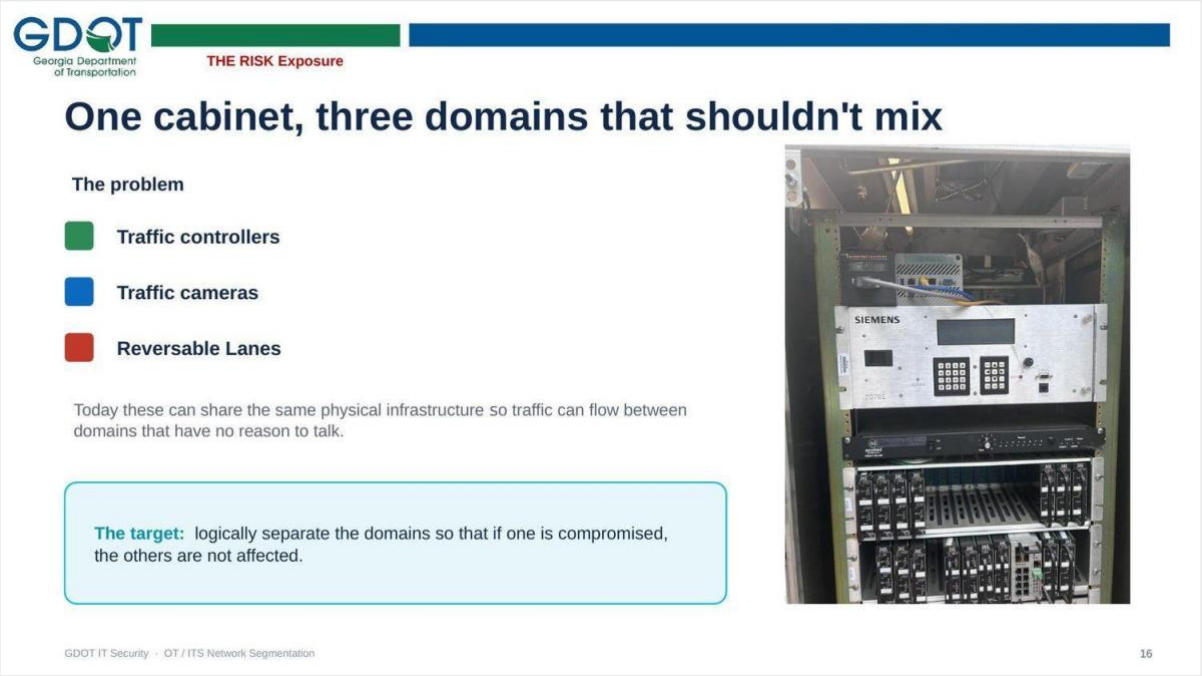
Dayton RTA's framing: networks accrete complexity the way an unplanned city does, which makes every later change harder; de-complicate before re-complicating. Source: Greater Dayton Regional Transit Authority.

In three years the authority replaced its critical infrastructure, from servers and storage to networking and wireless, and retired a legacy phone system the vendor no longer supported. A state requirement for a cybersecurity program and annual audit reinforced work the authority was already doing. It built a 125-page continuity-of-operations plan structured like a choose-your-own-adventure book, stood up governance for its use of AI tools, and ran an IT tabletop exercise that produced three pages of plan updates even on a good run. It is rolling out multi-factor authentication across a multi-union workforce using secure badge cards. Prince advised agencies to reassess cloud versus on-premises choices against their cost profile, since a transit agency is capital-heavy and operating-light, and to define technology platforms first and then consolidate a sprawling low-bid vendor set within them. He would have peers copy two decisions: step back and look at the whole environment rather than tunnel into one part, and do not wait for an incident to act. He warned against letting the business insert poorly scoped, non-emergency projects. Asked for his best investment, he named a privileged-access management system that now brokers and records vendor sessions instead of handing over standing network credentials, a change that sharply reduced the agency's risk.

Perspective from Georgia DOT (Justin Hatch, Steve Ainsworth, and Joshua Miller)

Georgia DOT presented its award-winning edge-network firewall deployment as a cross-office collaboration among traffic operations, IT infrastructure, and IT security. The context is scale: Georgia connects roughly 8,000 of its 10,000 signals to a central system, along with more than 100 local agencies, and runs statewide performance measures with open data and a connected-vehicle program. The team set four criteria for the deployment: security, meaning inspection of cabinet-to-data-center traffic with application-based firewall rules and segmentation; observability of connected devices and their vulnerabilities; resiliency through a routed design; and ease of deployment.

Ainsworth described the network side. The old flat design put whole fiber chains in a single segment, so one break could orphan every cabinet downstream. The redesign puts each cabinet in its own routed segment advertised to two hubs, with cellular backup if the fiber fails. The team automated deployment around a single authoritative inventory system that records each device's model, serial number, location, and change history, so a field technician enters only a cabinet identifier and a firewall serial number, and the back end pushes a standardized configuration and confirms success. Miller described the security rationale.



Georgia DOT's problem statement: in a single cabinet, traffic controllers, cameras, and reversible-lane logic can share the same wire, so a compromise in one domain can reach the others. The goal is to isolate them so a compromise cannot spread. Source: Georgia DOT.

On a flat network a single compromised camera can reach signal controllers and other critical devices, so a device that arrives already compromised from the supply chain becomes a foothold into the whole environment. GDOT's strategy is to isolate each domain within the cabinet, apply consistent network segments across districts, deny traffic by default, and move toward authenticated, certificate-based access instead of a wide-open internal network, treating a public data application differently from the crown jewels of express lanes and signal controllers. Miller framed the budget question this way: it may be safer to build a two-lane bridge than an eight-lane one, and an agency that cannot fund the security of a new initiative may be overextending. Hatch warned against trading away ruggedization and transportation experience for a device that is merely the newest.

Session 6 — National Cooperative Efforts and What's Next

Moderator: Siva Narla, ITE. Panel: Joseph Gregory, FHWA; Mashrur "Ronnie" Chowdhury, Clemson University; with Day 1 and 2 moderators.

Narla framed the closing session around ownership, trust, and securing systems that no one designed with cybersecurity in mind, driving toward each agency's 90-day action.

Perspective from FHWA (Joseph Gregory)

Gregory described FHWA's role as influential and supportive rather than asset-owning or regulatory. FHWA developed the Transportation Cybersecurity Strategic Plan in 2019 and is now updating it to add emerging topics such as AI, V2X, electric-vehicle charging, and cryptography that can withstand quantum computers, and to shift emphasis from keeping attackers out toward resilience, meaning the ability to respond and recover once they are in. He pointed agencies to existing resources that deserve wider use, including federal training, wargaming and incident-response exercises, boilerplate procurement language, and the ITS Cybersecurity Framework Profile, now aligned to the current version of the federal cybersecurity framework. He flagged a new cooperative research project on advancing cyber resilience for TSMO programs, and in the synthesis he pressed asset inventory as the dominant cross-cutting theme, citing recent research on integrating operations with asset management and the traffic management center pooled-fund study.

Perspective from Clemson University and TraCR (Ronnie Chowdhury)

Chowdhury directs the National Center for Transportation Cybersecurity and Resiliency, a USDOT-sponsored consortium of nine universities led by Clemson, running roughly 50 projects across research, prototyping, testbeds, demonstration, technology transfer, education, and workforce development. He walked through tools the center has already built and made available, including a plain-language policy search tool built on large language models that is now in a pilot with a state DOT, a cyber-attack simulation tool, and an automated attack-detection and mitigation tool built on a public catalog of attacker techniques. He described work on encryption that lets an agency send processed rather than raw data to a public cloud, on the transition to cryptography that can withstand quantum computers, and on detecting tampered hardware and side-channel attacks that infer activity from a device's power draw or emissions. His warning about the stakes was blunt: if the global positioning and navigation system falls, everything falls.

Perspective from ITE and the standards community (Siva Narla)

Narla summarized the cooperative work among ITE, AASHTO, and other standards bodies, including connected-vehicle interoperability, controller cybersecurity, a newly published data dictionary for traffic management delivered in a modern machine-readable format, and security for the core ITS communications protocols. He cited a study of five agencies, conducted with federal partners and independent security researchers, which found that about one in three agencies reported a cyber incident. Underreporting means the true number runs higher, with attackers often present but not yet acting. ITE is building a cybersecurity standard aimed at publication late in the year that establishes a baseline self-assessment: firewalls in place, no unmanaged devices, software kept current, no default accounts, and an end to the trivial cabinet-key problem. It defers more advanced capabilities, such as intrusion detection and secure key storage, to a later version. Narla framed the whole effort as a maturity climb meant to carry the entire community up together, not to assign blame.

Discussion and 90-day actions

The synthesis returned repeatedly to three gaps: the absence of a mandatory national standard, the absence of any cyber testing regime for devices, and the failure to share incidents. Toepper argued for conditioning federal-to-state funding on vendors meeting a specific standard, noting that a signal forced into flashing red is one thing but that connected vehicles raise the stakes to human safety. Chowdhury proposed that this community lead a cyber testing and certification strategy, drawing an analogy to crash-testing vehicles before they reach the road. Contestabile pressed for integrating the siloed efforts on inventory, data governance, and cybersecurity, arguing that the data sits at the base of all of it. He also called for real device testing whose results carry across agencies and manufacturers, since today's testing addresses ruggedization rather than cybersecurity. Narla noted that manufacturers and operating agencies share liability today, a model that works for a known system but strains against a diffuse threat from an unknown source. That leaves open the question of who will take responsibility. Fok returned to information-sharing, calling for a way to help agencies disclose incidents at the level of root-cause detail that the National Transportation Safety Board provides for crashes.

The 90-day actions came out more aspirational than concrete, and not as a clean per-agency list, but several speakers voiced one. New Hampshire committed to keep moving aging field equipment into a managed environment, extend its routed backbones, and pursue a self-assessment to find the highest-value fixes within its existing staff. Chowdhury offered to help lead a testing and certification strategy. Contestabile committed to push for integrating the disparate efforts and for real device testing. Toepper committed to advocate a national requirement. Brooks encouraged the DOT community to originate research problem statements into the cooperative programs. Ramfos closed by committing NOCoE to take the exchange's themes to its Technical Advisory Committee for next year's plan, and to circulate a draft of this report for comment before publishing it widely.

Key Learnings and Next Steps

- **People and process, not technology, are the hard part.** The agencies making progress have aligned culture, roles, and written agreements between operations and their state IT and cybersecurity offices. Segmentation, monitoring, and patching only pay off inside a program with named owners, staffing, documented standards, and enforcement.
- **The threat has outpaced prevention.** Nation-state tools, AI-accelerated exploitation, and the use of transportation systems for intelligence mean that fast detection and quick recovery now matter as much as keeping attackers out.
- **Segmentation is the highest-return control,** followed by asset visibility and disciplined patching. Micro-segmentation limits how far a compromise can spread.
- **OT is not enterprise IT.** Field devices prioritize availability, run for 15 to 20 years, and often cannot support standard controls, so agencies must treat security changes as engineering changes.
- **Procurement is where security is won or lost.** With no single mandated standard, agencies lean on cooperative research, the ISA/IEC 62443 series, supply-chain screening, and shared specification language.
- **Modernize before you monitor.** The case studies show a common arc from a routed, resilient network through visibility and automation to continuous monitoring.
- **The community does not yet share incidents**, which slows learning across every agency.

Next Steps

- **Segment first.** Treat network segmentation as the highest-return control and limit the blast radius before investing in monitoring.
- **Inventory everything.** Stand up an authoritative asset inventory as the precondition for lifecycle planning, patching, and risk decisions.
- **Put the operations and IT relationship in writing.** Formalize MOUs and a clear demarcation with the state CIO and CISO, share OT requirements with operators, and bring OT understanding into the security office.
- **Buy security in all procurements.** Embed cybersecurity requirements in ITS solicitations, using cooperative-research language, a recognized device standard, a software bill of materials, and supply-chain screening.
- **Plan for recovery, not just prevention.** Name who leads an incident, put public safety first, build and exercise a continuity-of-operations plan, and use tabletop exercises to move leadership and secure funding.
- **Share incidents.** Support agencies willing to disclose and press for a structured way to share root-cause findings.
- **Engage the national pipeline.** Feed problem statements to the cooperative research and pooled-fund programs, and track the federal strategic-plan update, the forthcoming ITE standard, and the available research tools.
- **Measure the climb.** Baseline the agency with a maturity self-assessment and the NCHRP 03-127 risk scores, then repeat it to show whether controls are reducing risk.
- **Commit to a 90-day action** and report back at the next exchange.

Resources

Federal frameworks and plans

- FHWA Transportation Cybersecurity Strategic Plan
- FHWA/USDOT Transportation Cybersecurity Resources
- ITS Cybersecurity Framework Profile
- NIST Cybersecurity Framework; ITS Control Set templates for signal controllers, dynamic message signs, closed-circuit television, and roadside units
- OWASP Application Security Verification Standard

Research and tools

- NCHRP Report 03-127 — cybersecurity risk assessment and self-assessment tool for traffic management field equipment
- NCHRP 20-102 series; NCHRP research on advancing cyber resilience for TSMO programs; NCHRP research on integrating TSMO and transportation asset management — https://www.nationalacademies.org/publications/29446
- TMC Pooled Fund Study, Inventorying, Documenting, and Configuring TMS Assets — https://tmcpfs.ops.fhwa.dot.gov/projects/inventoringtms.htm
- National Center for Transportation Cybersecurity and Resiliency (TraCR), Clemson University — https://www.clemson.edu/cecas/tracr/index.html
- MITRE ATT&CK knowledge base; Shodan device-exposure search

Standards and communities of practice

- ISA/IEC 62443-4-1 and 62443-4-2; NIST 800-82; ISO 27001; SOC 2; federal supply-chain rules (NDAA/TAA)
- ITS America Cybersecurity Community of Practice
- AASHTO Transportation Cybersecurity Community of Practice; ITE cybersecurity standard (in development); NextGen Traffic Management Data Dictionary
- CISA vulnerability resources — https://www.cisa.gov
- Georgia DOT firewalled-router case study

Appendix A — Agenda

Cybersecurity for TSMO Strategies and Applications — August 4–5, 2026 — Virtual

Day 1 — August 4

Time (ET)	Session	Speakers
12:00 – 12:15 pm	NOCoE Welcome	Nicholas Ramfos, NOCoE
12:15 – 1:30 pm	The Threat Landscape and Overall Context for TSMO Cybersecurity (Moderator: Laurie Matkowski, NOCoE TAC)	Jeff Rockower, NJDOT, ITS America Cybersecurity CoP representative; Steven Prichard, NJDOT, AASHTO CAV/Cyber CoP lead; Ed Fok, Cipher Roadways, ITE representative; Justin Anderson, USDOT ITS Joint Program Office
1:30 – 2:30 pm	The People, Process, and Technology (The TSMO/IT Relationship for Cybersecurity) (Moderator: John Contestabile, Skyline Technologies)	Troy Peterson, Utah DOT; Dirk Spalding, Caltrans
2:30 – 2:45 pm	Break	—
2:45 – 4:15 pm	The Stuff: Evaluating the Threats to the Existing TSMO Environment (Moderator: Jim Toepper, EtherWAN, ITS Cyber CoP	Lynne Randolph, Southwest Research Institute; Jeff Rockower, New Jersey DOT; Edward Darnell, Texas DOT; Ed Fok, Cipher Roadways
4:15 – 4:30 pm	Key Learnings and Next Steps	Nicholas Ramfos, NOCoE

Day 2 — August 5

Time (ET)	Session	Speakers
12:00 – 1:00 pm	Tools, Procurement & Vendor Management (Moderator: Michael Brooks, ITS America)	Sabrina Moser, Southwest Research Institute; Michelle Barnes, Texas A&M Transportation Institute (TTI); Jim Toepper, EtherWAN
1:00 – 2:30 pm	Agency Case Studies in TSMO Cybersecurity	Shawn Donahue, Colorado DOT; Nicholas King, New Hampshire DOT; Shawn Prince, Greater Dayton Regional Transit Authority; Justin Hatch, Georgia DOT
2:30 – 2:45 pm	Break	—
2:45 – 4:15 pm	National Cooperative Efforts & What's Next (Moderator: Siva Narla, ITE)	Joseph Gregory, USDOT FHWA; Ronnie Chowdhury, Clemson University; Session Moderators
4:15 – 4:30 pm	Key Learnings and Next Steps	Nicholas Ramfos, NOCoE