National Operations Center of Excellence

Peer Exchange Report

Cybersecurity for TSMO Peer Exchange

Summary

The Cybersecurity for TSMO Peer Exchange virtually convened transportation professionals for a half day in September 2025 to discuss practical approaches for advancing cybersecurity maturity in transportation operations environments. The sessions explored common barriers, effective practices, and institutional strategies for bridging the gap between information technology (IT) and operations technology (OT) functions from a cybersecurity perspective and within the context of unique needs of transportation agency TSMO programs within enterprise-level cybersecurity priorities.

Participants represented a cross-section of state and local departments of transportation, research institutions, and private-sector technology partners. Across these agencies, there was strong consensus that cybersecurity is now a foundational part of TSMO, not an ancillary function.

The peer exchange emphasized three core themes:

1. **Cyber resilience** — ensuring systems remain safe and operable even under attack.
2. **Integration of IT and OT cultures** — aligning technical standards and governance.
3. **Institutional readiness** — building processes for training, exercises, and after-action reviews.

Key Learnings

1. Shared Ownership Between IT and OT

Many agencies reported that IT and OT functions remain siloed, resulting in unclear ownership of ITS devices, manual and varied connections to the network architecture, and varied response and maintenance procedures. Several DOTs have started embedding OT specialists into enterprise cybersecurity councils and developing shared playbooks.

Key learning: unified governance reduces response times and fosters trust.

2. Asset Inventory is the Foundation

A complete inventory of connected devices including controllers, sensors, servers and other IT/OT resources that can be overlooked in asset management programs is the cornerstone of any cyber program. Without asset visibility, intrusion detection and vulnerability management are incomplete. One midwestern DOT described using automated network discovery tools to identify field devices previously unmanaged by IT.

Key learnings: TSMO Technology asset management programs and plans need to be more detailed than asset management plans from other agency program areas. Asset inventories vary in information tracked, however the most important aspect is they cover the needs of both OT and IT.

3. Tabletop Exercises Build Culture and Coordination

Low-cost tabletop exercises were widely recognized as one of the most valuable tools for improving readiness. Multiple agencies used CISA-provided templates to simulate ransomware, DDoS, or insider threat events. This format is successful because it is familiar to practitioners who often participate in similar events for event and incident response planning.

Key Learning: exercises create shared understanding of roles and escalation paths before a real incident occurs.

4. Clarify Roles and Escalation Paths

Agencies found that documenting roles through RACI (Responsible, Accountable, Consulted, Informed) matrices improved coordination during cyber incidents. By defining who does the work (responsible), who owns the outcome (accountable), who provides input (consulted), and who is kept up to date (informed), agencies could effectively prevent security issues as well as efficiently respond to cybersecurity events. Having predefined communication channels, especially between Traffic Management Center's and enterprise IT, was identified as a major success factor.

Key Learning: Roles and responsibilities are as important, if not more, than the technological aspects. TSMO programs have demonstrated this for decades and it applies equally to managing cybersecurity through a DOT.

5. Flexible Funding Approaches

Cybersecurity upgrades are rarely funded directly, resulting in agencies embedding network security and redundancy work within traditional "state of good repair" or modernization programs. This reframing allows cyber improvements to move forward without new funding streams.

Key Learning: Cybersecurity isn't a program but a "way of life." Its important for practitioners to build in security into every piece of work and improvement they do.

6. Integrate Cybersecurity into Procurement

Agencies increasingly include minimum security standards for vendors and contractors. Requirements such as multi-factor authentication, firmware verification, and routine patch management are being written into contracts to prevent vulnerabilities from entering systems.

Key Learning: Managing the process of procurement and incorporating stakeholders (see RACI above) can efficiently build security into new projects.

7. Implement Least-Privilege Access Controls

Several DOTs have implemented tiered access structures limiting administrative permissions to critical systems. Least-privilege principles were described as simple but transformative: "You can't accidentally break what you can't touch."

Key Learning: The universal key for traffic control boxes no longer works. Access must closely managed and tracked.

8. Use National Frameworks

Rather than developing internal frameworks, participants recommended using national guidance from CISA, NIST, and ARC-IT. Standardization helps align terminology and provides defensible practices during audits and funding reviews.

Key Learning: Resources for cybersecurity are available and effective.

9. Share Information Safely

Participants noted the growing importance of closed communities of practice (AASHTO, ITS America) for sharing threat indicators and lessons learned. Agencies emphasized the need for protected but collaborative environments to exchange actionable intelligence.

Key Learning: Keep the conversation going and continue to convene practitioners around this topic.

10. Institutionalize After-Action Reviews

After every incident, test, or exercise, agencies capture "what worked" and "what failed." The most mature DOTs are now tracking lessons learned across multiple events in a single, searchable database.

Key Learning: Cybersecurity can be approached like a large-scale special event or emergency response exercise. Follow the process as if the event is coming, track the lessons, and expand the knowledge.

Red-Light / Green-Light: Capturing Practices to Overcome Barriers

Participants completed a Red-Light / Green-Light exercise that identified practical lessons from participating agencies. The following table summarizes common barriers ("Red Lights") and effective strategies ("Green Lights") shared across DOTs.

Barriers (Red Lights)	Effective Practices (Green Lights)
Lack of asset inventory and network visibility	Comprehensive asset inventory with firmware and device-level tracking
IT and OT silos with unclear responsibilities	Creation of shared governance councils or liaison roles
Reactive cybersecurity posture	Proactive tabletop exercises and COOP integration
Limited funding for cybersecurity upgrades	Use of "state of good repair" and resilience funds for network hardening
Vendor security inconsistencies	Cybersecurity clauses in contracts and vendor certifications
Staffing shortages	Cross-training of existing TSMO and IT staff on incident response
Minimal after-action documentation	Structured debrief templates following incidents or exercises

Discussion Highlights

During open discussions and chat exchanges, participants reflected on several recurring challenges and themes:

- **Culture gap between IT and OT:** IT staff often prioritize confidentiality and data protection, while TSMO operators prioritize system availability. Bridging this difference requires joint policies and shared metrics.
- **Incident response coordination:** Some agencies rely heavily on state IT departments, which may not understand OT systems. Clear division of responsibilities is essential.
- **Training gaps:** Participants called for standardized onboarding training for TMC and maintenance staff that includes cybersecurity awareness.
- **Vendor management:** Many incidents originate from weak vendor practices or third-party access. Several DOTs now require vendor log reviews or time-limited credentials.
- **Workforce challenges:** Hiring and retaining cybersecurity professionals remains difficult; agencies often cross-train operations engineers instead.

Emerging National Themes

Across DOTs, several national-level trends are emerging:

1. **Integration of Cybersecurity into TSMO Guidance:** Cybersecurity is becoming embedded within the broader resilience and operations frameworks developed by AASHTO and FHWA.
2. **CISA and AASHTO Collaboration:** The CISA tabletop templates have become a de facto standard for transportation cybersecurity exercises.
3. **Metrics and Self-Assessment:** Agencies are beginning to use maturity models to track progress year over year.
4. **Data Classification and Segmentation:** Some DOTs are segmenting networks by criticality (signal systems vs back-office data) to reduce exposure.
5. **Growing Emphasis on COOP and Resilience:** Continuity of Operations (COOP) planning is evolving to include cyber disruptions alongside natural disasters.

Closing Observations

Cybersecurity within TSMO is transitioning from an IT problem to an operational imperative. Agencies are taking measurable steps to integrate resilience into everyday practices.

The most effective agencies:

- Provide well-defined roles and responsibilities and procedures for IT and OT staff.
- Maintain accurate inventories of all connected assets.
- Conduct regular tabletop exercises that include both IT and operations staff.
- Embed cybersecurity expectations in procurement and vendor oversight.
- Document lessons learned through after-action reviews.

As one participant summarized,

"Cybersecurity is now as essential to safety as striping or signals—it keeps our systems alive."