NOCoE
National Operations Center of Excellence

Peer Exchange Report

TSMO and Information Technology

Overview

The National Operations Center of Excellence (NOCoE) hosted the TSMO and Information Technology Virtual Peer Exchange to share information between a cross section of agency leaders in the transportation operations and ITS function and the information technology function of their jurisdictions. Their experience in developing and implementing IT and TSMO plans, programs, technology, strategies, and policies in their organizations provided the basis for an exchange of ideas about methods to address the challenges and opportunities with operations technology applications.

The goal was to share successful real world strategic and tactical experience from agencies that are working through the process of collaboration between Information Technology (IT) and TSMO agency functions that have been historically separate. There was an emphasis on sharing successful approaches that can be adapted and applied to other peer organizations. There was recognition that agency staff are working to create new opportunities to work together in problem-solving, but it is still a work-in-progress in some regards.

The participants were encouraged to actively participate by sharing their questions, comments, and current practices among each other. The topics within each broad session were crowd-sourced by participants using a virtual white board then voted for the priority topics to discuss. Those not touched on are noted in Next Steps at the end of this report. Attendees were asked to consider the actions their agency may need to take to align desired goals and objectives between the TSMO and IT functions for their agencies to resolve the current and future challenges.

Participants are able to reach out to presenters for further information or assistance, and were asked how the NOCoE, its partner associations, and FHWA help them in their journey to improve collaboration between TSMO and IT.

Discussion Topics

Summary

Session 1 – Opportunities for TSMO and IT to Improve the Transportation System

Introduction to the Conversation

The session was introduced by the facilitator with an initial outline of the discussion touching on overarching challenges and opportunities for the transportation system management and operations (TSMO) and information technology (IT) functions for transportation systems created and prioritized with a virtual white board.

TSMO business units face a number of challenges identified through prior conversations with agencies, including:

- The 24/7 on-call operating environment of TSMO, which can strain IT agencies.
- Limited product options and vendors within intelligent transportation systems (ITS), some of which are sole source, which may not align with usual IT standards and procurement plans.
- The critical issue of coordinating maintenance and cybersecurity has become increasingly vital, amplified by recent national transportation news.
- TSMO faces hurdles due to the unique training and skill sets required.
- The prevalence of legacy operations technology (OT) equipment (some dating back 35 years).
- Decentralized organizational structures within state Dots, where regions often operate independently.
- Pride and ownership individuals have in the existing work and systems under their authority which can sometimes impede transition and/or new approaches.

In a similar manner TSMO business units see various opportunities looking forward:

- Potential to leverage cybersecurity expertise by collaborating with IT function/agencies.
- Standardization and easier lifecycle replacement of legacy systems.
- Benefits from the vast pool of IT resources not traditionally accessed by TSMO business units.
- Potential to leverage existing contracts, systems, resources from other agencies when standards, requirements, and specifications align.
- Collaborative development and deployment of new ITS, communications, and other systems, especially when considering vehicle-to-everything (V2X).
- The adoption of software-as-a-service (SaaS) and cloud-based solutions is a space where IT expertise is necessary rather than TSMO business units attempting these alone.
- Current TMC managers and ITS engineers are “quasi-IT professionals” due to historical organizational evolution of transportation operations functions to support OT. Future workforce challenges necessitate a focus on core traffic operations skills.

- Ability to recruit traffic operations professionals without requiring specific IT or OT experience since that would be provided through other staff with those credentials.

Moving to IT business units, there are challenges which in turn affect the application of technology in TSMO business units such as:

- Increasing project oversight and government accountability requirements from centralized groups controlling overall roadmaps.
- Increased procurement complexities for cloud-based solutions, which were historically less accepted.
- Understanding how software-as-a-service (SaaS) impacts program capital versus operating budgets.
- The rapid speed of change in the IT industry, along with associated process adjustment requirements.
- Overall lack of resources, including a significant workforce gap in available staff.
- Increasing stress to invest in replacement IT and OT to pay down technical debt.

Even with these challenges there are opportunities on the horizon for IT business units, including:

- Establishing strong collaborative relationships with TSMO business units.
- Ability to gain expertise and provide specialized support as an exciting break from routine tasks.
- Better alignment with overall IT (and OT) roadmaps for improved outcomes in the future.
- Improved backlog prioritization to reduce impact of workforce shortages that can hinder timely approvals.
- Ability to be more responsive to changing needs based on the collaboration.
- Ensuring a focused IT architect who understands TSMO is available to help lead the conversations when needed is beneficial and supportive of the end goal of getting right people involved and focused on the right part of the job.

Perspective from Both Sides – Oregon DOT

Galen McGill, Oregon DOT's State Management Operations Engineer, recounted the origins of the agency's ITS program, which began in 1998 with just one engineer and one IT person. This early structure fostered a foundational partnership, rooted in the understanding that ITS could not exist without IT. Rod Kamm, the Enterprise Business Applications Manager for Oregon DOT has been a long-standing partner in the ITS program. A newer layer of state agency IT oversight has added some complexity, but the core partnership remains strong.

The agency's current top two priorities are addressing the challenge of prioritizing limited resources amid the rapid pace of IT change and the need to address aging legacy equipment in the field. It has been difficult to convince people to invest in maintaining existing, outdated systems when the allure

of new projects is often stronger. They strive to maximize the lifespan of equipment, while constantly balancing maintenance of the old systems with adoption of the new. The partnership with IT is crucial to addressing the critical risks associated with older technologies such as supportability issues and security vulnerabilities. IT provides a different perspective on backend and central infrastructure needs. Immediate issues are replacement of outdated variable message signs and network equipment, as well as servers running unsupported operating systems that pose security risks. Their IT partners help ITS staff understand and address these backend assets, which operators might overlook while focusing on roadside equipment.

The IT organizational structure at Oregon DOT features application support teams built around specific business lines within the agency. Rod Kamm oversees six such groups, supporting various applications and attributes their successful partnership to embedding IT personnel in the same building as the ITS/TSMO team from day one. This close proximity fosters natural dialogue, shared program understanding, and institutional knowledge, ensuring everyone is "on the same general page."

Facing the same challenges of limited resources, there is constant need for IT teams to agree on how to allocate time and energy between new initiatives and addressing "technical debt" — the aging infrastructure and systems that require maintenance. The ITS domain has a unique set challenges involving numerous roadside technologies and the complex supporting network infrastructure. There is necessarily constant attention to these layers and the collaborative development of practical plans for both application support and network modernization. Over the years, this shared understanding between the ITS and IT staff within the agency has enabled them to continually progress by simultaneously addressing both the old and the new elements of the system.

The Oregon DOT representatives noted that they were not surprised by the high ranking of "increased procurement complexity" in the virtual white board. The agency retains its specific IT functions, including OT while there is a separate state IT oversight agency (under the Department of Administrative Services, Office of State CIO) that exists to oversee security and enterprise systems. This oversight agency, however, adds a review layer to all IT procurements which can significantly extend timelines.

There is inherent complexity of purchasing technology within a state procurement framework. Unlike traditional low-bid scenarios, software requires an RFP and best-value proposition. The challenge lies in making sound procurement decisions that secure the best product for long-term needs, especially within the constraints of state contracts, which typically last 5-10 years.

The feasibility of replacing software systems every few years due to contract expiry is questionable, particularly with the increasing shift towards Software as a Service (SaaS) and the high degree of integration in operations. Replacing interconnected systems frequently due to contract cycles is inefficient and disruptive. Navigating state contracting rules in Oregon alongside rapidly changing technology to achieve an efficient and effective systems, without constant changes, is a significant though unsurprising challenge.

The shift to a cloud-first strategy years ago brought external agency layers of oversight with vendor contracts being scrutinized for hosting options, with rules against international hosting. Now, with a heightened focus on cybersecurity, an external cybersecurity group reviews contract terms and conditions. In addition, the emergence of artificial intelligence (AI) introduces new concerns and laws, leading the Department of Administrative Services to issue specific AI policies and frameworks. All these layers translate to numerous checks and balances required to finalize any contract, even contract

amendments or modifications. They noted that standard contract terms and conditions that have not been updated in five years (a significant period in technology evolution) require review each time. This further slows down speed through the procurement system compared to a decade ago when such complexities were far fewer.

Perspective from Both Sides – New York State DOT

Sandra Clark, Deputy Commissioner for Technology with the Office of Information Technology Services (OITS) in New York state, explained that their IT department is an independent agency that consolidated all state agency IT departments in 2012. While they manage traditional IT functions like system development, they had not taken on OT support, leading to limited involvement in that area.

Robert Limoges, Director of Office of Traffic Safety and Mobility, from New York state DOT (NYSDOT) elaborated that agency began to evaluate its TSMO program four years ago. Historically, their signal program and legacy ITS programs were overseen by separate organizational entities. They made a strategic decision to combine these into a new TSMO bureau recognizing that signals are essentially ITS equipment and that technology would drive future business decisions. NYSDOT manages large and organically grown network(s) of OT: 10 transportation management centers, 6,500 traffic signals, and 10,000 field devices. Each region has historically used different methods for asset construction and developing procedures and software in their TMCs. This realization spurred the need for centralization and standardization.

These internal changes at NYSDOT started agency's journey towards collaboration and coincided with a statewide push from OITS to standardize and enforce stronger security protocols. Initially, these efforts led to some procedural and approval conflicts, prompting the realization that both agencies needed to collaborate.

Last year, both agencies came to the table initiating a "true collaboration" and held workshops bringing together experts from both DOT and OITS, including network services, cybersecurity, and regional and central office staff. The goal was to establish shared goals and project priorities. They are currently working on the fundamentals to define how they will work together, the team structure(s), and establishing governance. They are documenting the planning to build a strong foundation, recognizing they are still in the early stages of this collaborative effort. They acknowledge that while they have made significant progress in their collaborative continuum, they still have considerable work ahead.

The agency's top projects, like Oregon DOT, focus on foundational systems. While executives often desire "shiny new objects" like connected vehicles or AI, the agencies' priority is to maintain and rebuild core systems. Key projects include:

- Rebuilding their ATMS (Advanced Traffic Management System)
- Constructing a new 511 System
- A major effort to install communications at all traffic signals to ensure connectivity
- A significantly elevated focus on their cybersecurity program

Although these foundational projects, while crucial, may not be as stimulating as new technologies. Nevertheless, they are also trying to integrate innovative initiatives like V2X and AI to meet the agency's leadership priorities.

New York state staff noted that the top-ranked challenges and opportunities both related to cybersecurity, which was not shocking and resonated strongly with their current efforts. NYSDOT has experienced security incidents, including hacked modems and message boards, which have been disruptive and unpleasant. While NYSDOT has made significant strides in building an internal cybersecurity program, they also rely heavily on their partners at OITS.

To clarify roles and responsibilities between the two agencies, last year they developed together a RACI (Responsible, Accountable, Consulted, Informed) matrix based on the NIST cybersecurity framework. This matrix helps guide who has ownership of actions regarding cybersecurity for both OT and IT. Although still a work in progress, the agencies have found the exercise extremely helpful to avoid stepping in each other's way or missing crucial aspects of cybersecurity.

Another key takeaway for NYSDOT, when considering opportunities, is recognizing and then leveraging the extensive resources and skill set available through OITS, including software products, expertise, and procurement capabilities. Sandra Clark from OITS agreed NYSDOT's observation about cybersecurity being a top concern. The largest challenge in their RACI matrix effort stems from having cybersecurity professionals on both the OT and IT sides, making it crucial to define responsibilities clearly.

The IT challenge of "increasing project oversight and governance accountability requirements from outside entities" was surprising in its low-ranking. This challenge is highly tied to the procurement process. For New York State, multiple agencies participate in procurement oversight, including the Division of Budget (spending approval) and the State Comptroller's Office (contract approval above a certain cost threshold). This layered approval process is not agile nor quick. In the past NYSDOT traditionally managed its own procurements for major projects (e.g., software systems, ATMS, 511 system, etc.). However, the current state directive is that OITS will conduct these procurements on behalf of the department. This shift is happening in real-time, so NYSDOT is actively working through the procedural implications.

Discussion

Kyle Nelson from Michigan DOT's IT role reinforced the common frustration with procurement, but introduced another critical challenge: managing funding sources, particularly grants with tight schedules. He noted that regions often secure grants for innovative projects, but then IT faces the immediate challenge of supplying resources to ensure these vendor-developed solutions are secure.

Around 10-20 years ago, districts had more autonomy, akin to a "wild west" approach to deploying ITS devices. However, with rising maintenance and operations costs, leadership has initiated a push towards centralized decision-making. While they have formed an "alignment team" to aid this, districts can still independently apply for grant funding, and MDOT often has to accommodate these projects, creating a struggle. In addition, IT and system implementations require coordination with their state Department of Technology Management and Budget as a central control.

Galen McGill noted that Oregon DOT faces similar issues with project funding, not just grants. There are instances where creative solutions requiring backend software would come in unexpectedly, leaving IT scrambling to integrate them into an already full schedule. While not perfectly solved, Oregon has moved towards more centralized review for grants and new IT components. This allows for a checkpoint to assess if a project with an IT component can be accommodated by their IT resources, ideally before a grant's requirements force the issue.

As a result of several grants with a short implementation runway that came unexpectedly to IT creating

some chaos, the IT function has moved towards a planned model through Application Portfolio Management as a solution. This involves inventorying applications, assessing technical health, business value, and total cost of ownership, and then developing a roadmap. This approach facilitates proactive planning for end-of-life systems and helps avoid inefficient investments, such as having multiple asset management systems doing similar work. Planning discipline with this approach, tied to governance, will improve their IT maturity.

NYSDOT has had similar experience with grant opportunities creating "silos of excellence." There is a need for better coordination and governance from central office to guide innovation and system upgrades across the agency. Their new governance process with OITS, while untested, aims to provide better visibility and guidance.

Nicholas King of New Hampshire DOT (NHDOT) observed that the past "cowboy days" of ITS and TSMO purchases did not involve as much red tape and that can impede innovation. While oversight is a necessity the current level, driven by cybersecurity concerns and the growth of the ITS industry, is a challenge to acting nimbly. In New Hampshire there is a multi-layered approval process involving a cybersecurity committee, a Transportation Technology Innovation Committee, a data and systems workgroup, embedded IT department processes, Federal Highway approvals, and even governor and council meetings for purchases of ITS technology. TSMO business units can be bogged down by seemingly endless processes and new policies that are slowing down deployment and TSMO is becoming something different than what it was created to do.

In New York, external controls and internal processes are also increasing due to the magnified focus on security, with new privacy and risk reviews, and more recently, an AI review board for any project involving AI. While these add time and process steps, they are necessary due to increasing capabilities of bad actors and heightened risks, meaning they cannot be skipped.

Others concurred given that in government, accountability is paramount, especially given the front-page news generated by IT vulnerabilities. While some oversight may appear to go too far, there is value in governance models, particularly enterprise architecture. In Oregon, Rod Kamm shared that there are multiple asset management products across different DOT sections. He suggested that better enterprise architecture could consolidate these, leading to cost savings and more strategic investment. Without such overarching roles agencies can waste time and money.

Kyle Nelson from Michigan DOT reiterated that IT's primary goal is system security and availability. He shared the 2015 Target hack, which originated through an unpatched HVAC system connected to point-of-sale, as an example of how seemingly disconnected systems can pose significant risks. IT's concerns about cybersecurity, like a camera connected to a signal, then a central system, causing chaos,are rooted in ensuring operational availability. Michigan DOT's solution is an ITS cybersecurity task force that works closely with the ITS team, tackling one challenge at a time to achieve "1 percent better all the time," fostering both progress and stronger relationships.

WisDOT particularly sees the need for collaboration between traffic engineers, IT infrastructure, and security, whose interests do not always align. There remains a cultural perception that IT slows things down. However, there are reasons for IT's measured approach. By cautionary example from 2016 where an exploit in the state election system could have impacted WisDOT customer records, highlighting the danger of unknown system linkages and the importance of knowledge and collaboration for cybersecurity defense.

On the procurement side, WisDOT uses alternative methods through the National Association of Purchasing State Purchasing Officers (NASPO) and the federal General Services Administration (GSA), which, despite a small premium, bypass lengthy RFP processes for suitable products. Protested bids from the RFP process on major projects (e.g., a network operations center bid) can cause year or longer delays reinforcing the need for easier purchasing methods. Others noted cooperative purchasing agreements through MPO's.

In the early days of ITS rapid deployment was possible without much oversight in Oregon. However, the current increased scrutiny comes from mainstreaming of TSMO. As TSMO programs grow in size and utilize more significant agency resources, they naturally face more oversight. The resulting trade-off is increased complexity and risk aversion, often stemming from high-profile IT failures.

In NYSDOT early programs were built by innovators. While culturally they might still lean towards that, the reality is that everything is now connected, necessitating a focus on security. There remains a cultural resistance to new processes, but there is a clear need for transparency and nimble processes to navigate reviews, working closely with OITS.

In Michigan, while there are cultural differences between the TSMO and IT staff, open communication is critically important especially as individual trusted relationships are foundational to progress, including, for example, the creation of their ITS cybersecurity task force. Understanding each other's needs and establishing regular dialogue prevents either side from feeling like the other is slowing them down, fostering an understanding of why processes are in place. An emphasis on engaging "early and often" in the process is essential and bringing IT in earlier allows for necessary reviews to happen sooner, potentially preventing delays at the end.

Matt Sneed from TxDOT concurred with the points previously made, particularly the cultural shift needed as ITS, often perceived as "10 years behind," confronts basic cybersecurity practices like password management. The increased network complexity of moving to the cloud has exposed issues as well, (e.g., TxDOT's ATMS migration that revealed a lack of secondary network connections, leading to vulnerability during power outages).

Software as a Service (SaaS) presents challenges as does vendor compliance with state requirements like TxRAMP (similar to FedRAMP), often requiring education for ITS vendors, which extends procurement timelines. ITS vendors are improving their cybersecurity practices, but it is taking time. As a solution, their agency CIO established a Traffic Management Steering Committee, including leadership from various divisions, to foster collaboration and prevent "silos of excellence" from working independently.

Iowa DOT is transitioning to centralized IT and Chris Pelton reiterated the paramount importance of communication and building relationships between IT and TSMO teams to establish trust. Springing projects on IT or procurement at the last minute is unfair, so "early and often" communication allows for shared expectations. For TSMO staff the challenges of centralized IT can result in the potential loss of personal connections and easy access to expertise, but centralized IT brings added expertise.

DOTs nationwide are grappling with similar challenges at the intersection of IT and TSMO. The recurring themes of procurement complexity, cybersecurity, funding constraints, and the need for centralization

highlight a significant shift from the early innovator period of ITS deployments. Potential solutions revolve around:

- Establishing clear communication channels and fostering strong relationships: This was repeatedly emphasized as crucial for bridging the cultural divide between TSMO and IT, ensuring mutual understanding of needs and constraints.
- Early engagement of IT in ITS/TSMO project planning: Bringing IT in at the earliest stages of grant applications or project conceptualization allows for proactive identification of IT implications, security reviews, and resource planning, ultimately reducing delays.
- Developing robust governance models: Steering committees, alignment teams, and the implementation of Application Portfolio Management are methods to centralize decision-making, prioritize projects, and ensure strategic IT investments across the agency.
- Addressing cybersecurity proactively: Recognizing that the connected nature of modern ITS makes systems vulnerable, many DOTs are forming dedicated cybersecurity task forces and incorporating rigorous security reviews throughout the project lifecycle.
- Exploring alternative procurement methods: While state procurement processes remain a hurdle, some DOTs are finding success groups NASPO, GSA, or MPO's to expedite technology acquisitions.
- Investing in cultural change: Acknowledging that the transition from decentralized approaches to more centralized, secure, and integrated systems requires a shift in mindset across all levels of the organization(s).

Session 2 – Roles and Responsibilities

Introduction to the Conversation

This session focused on roles and responsibilities involving the people and policies aspects of IT and TSMO integration, as distinct from the management technology elements (e.g., hardware, software, communications, etc.) that will be covered later. An initial virtual white board was provided by WisDOT for the session that displayed pre-listed topic areas under successes and challenges. Participants added their input to these lists. Roles and responsibilities include:

- Approvals, agreements, and responsibilities
- Procurement practices
- Data sharing and governance
- Recruitment
- Consultant Management
- Internal vs support services
- Funding for staff and resources
- Training practices

Successes related to roles and responsibilities have included:

- IT-related issues shared earlier in the process
- NASPRO contract mechanisms can help expedite schedule and reduce costs of developing "full blown" RFP
- Project approval process to tap into IT resources formalized
- Hiring a Chief Data Officer
- ITS/TSMO can rely on IT to support business-related IT infrastructure
- Currently high demand for IT positions

Some of the unsolved organizational challenges include:

- Knowing the "triggers" of when to share issues with IT functions
- Lack of awareness of big purchases that require additional reporting outside of transportation agency
- Governance across IT and OT can be unclear
- Risk associated with having one long-term ITS maintenance contractor
- Challenge filling niche positions in TSMO/ITS
- Efforts underway to improve governance including internal CAV-related committee(s)
- More training needed across IT and OT agency divisions

Some ideas that could be built upon work already completed revolved primarily around recruiting strategies by using university relationships as a staffing resource as well as military, junior college, and/or apprentice pipelines.

Two key takeaways from the first session serve as starting points for this segment. First, the change in the role of TSMO from peripheral function to a mainstream role. The drive to mainstream TSMO in order to to gain funding, recognition, and integration into project development and capital improvement processes (even beyond technology) inherently brings more oversight; hence, oversight is the cost of mainstreaming TSMO. This increased role for TSMO, especially with its reliance on ITS technology and IT, necessitates clearer policy definitions and addressing recruitment challenges.

The second takeaway is to engage between IT and TSMO groups early and often. This principle is already reflected in agencies' successes noted by participants on the virtual white board that IT-related issues are shared earlier in the process indicating this proactive approach.

Perspective from Wisconsin DOT

Todd Szymkowski, the Statewide Traffic Systems Engineer at WisDOT highlighted their success in getting ahead of issues, primarily through solid communication, noting direct involvement of the head of the applications development support section (Shiva Kalyanaraman) in routine discussions with the Bureau of Traffic Operations (BTO). The opposing challenge is defining the triggers for engaging the IT organization which was clear (server or firewall issues) in the past, but the blurring lines between IT and

OT creates the need to address issues earlier.

The changing technology landscape, particularly the shift to Software as a Service (SaaS) complicates matters. In Wisconsin, any cloud vendor must undergo a cloud brokerage agreement with the state, regardless of the cloud service used. This involves rigorous checks on vendor certifications (like SOC), security posture, and data center location (must be in North America). This process, while a perceived "bottleneck," is crucial for security and compliance and inherently time-consuming.

There are monthly recurring meetings with the leadership team in BTO, a larger Division of Transportation System Development group meeting with a BTO representative, and frequent project-level meetings (potentially weekly) for active projects. Steve Schar (IT Supervisor for Cloud Services and Systems Engineering) added that a weekly change meeting run by the TMC is also attended by his team members.

Moving to procurement practices, WisDOT funding approval processes can vary in speed, impacting project timelines and budgets. The agency has been searching for acceptable methods to expedite purchasing and has had recent success with the NASPO list, which allows them to bypass the full RFP development process for a small markup. This approach has been used for their video management solution, video analytics, and specialized software licenses.

Using NASPO is crucial because Wisconsin policy dictates that they cannot do business with any cloud vendor that lacks a North American data center, necessitating thorough checks on data center location, practices, and security. Significant time is added by anything cloud-related (e.g., a project to equip state patrol vehicles with Haas Safety Cloud integration for broadcasting vehicle location when lights are on) which leads to an increase of six months to the overall process.

WisDOT has additional reporting requirements outside of the agency to their state IT organization, about which they are not always privy. State statutes require reporting to the legislature for any spending over one million dollars (which includes every TMC system). This involves twice-yearly reports on project status, budget adherence, and timelines, leading to intense scrutiny. Steve Schar noted that a newer procurement challenge is related to vendor price increases. For example, a recent VMware licensing renewal where Broadcom initially proposed a 700 percent price increase, which, with third-party assistance, was negotiated down to a still substantial 400 percent price increase (aligning with what other state agencies pay). This unexpected and significant cost jump created budget difficulties.

WisDOT is in the process of hiring a Chief Data Officer (CDO), who will be positioned in the agency's Division of Budget and Strategic Initiatives, to establish an enterprise-wide view of data and its governance. A lingering challenge in data governance is defining the line between IT and OT and how governance should transcend these domains. Some issues span both, while others are unique to each. Data is increasingly a compliance issue rather than solely an IT issue. The agency also has subcommittee under their department-wide connected and automated vehicles (CAV) initiative that focuses on data governance and cybersecurity. A project to develop a cybersecurity framework assessment for WisDOT was recently initiated, inspired by similar efforts in other states.

The emerging challenge of AI components is in new software procurements. The evaluation of AI's utility is still "up for grabs," and the state of Wisconsin is working on a statewide AI policy that all agencies must follow. This means a period of "gray" areas and unknowns until it is in place, as AI is increasingly integrated into every tool they procure, from small to full-fledged systems.

Discussion

The subsequent discussion focused on people and policies as distinct from management including defining the boundaries between OT and IT, engagement, and workforce development as key areas.

Defining IT/OT Boundaries and Organizational Structures

The fuzziness of the line between IT and OT is a major challenge in determining roles and responsibilities. In New York state their governance model aims to clarify this, moving from an "us vs. them" mentality to a co-managed approach for procurements, cybersecurity, and other issues. It is difficult to hire for IT job titles within DOT due to OITS approval requirements. OITS has proposed a solution to create a "middle" OT team comprising both DOT and IT staff, working in partnership. This is not the traditional way for government to work but appears to be the only path to full collaboration if executive leadership approves. This situation is unique to OT work that OITS did not receive in the 2012 consolidation of IT departments. NYSDOT and OITS need to jointly develop expertise to be successful in delivering ITS/TSMO solutions for the state. Others agreed in the discussion that the blurred line does not exist in the same way in any other business area, given the technical complexity of OT.

At Oregon DOT wireless communications (e.g., land mobile radio systems) is another area within the agency portfolio with blurred IT/OT lines, similar to TSMO. Past disagreements over IT standards (like Cisco for network gear) vs. traffic cabinet environmental standards, highlighting the need to resolve overlaps and adapt IT approaches to the unique operational needs like resilience and environmental conditions necessary for OT.

Christeen Pusch from TxDOT noted the increasing IT/OT overlap but emphasized data governance is broadly applicable to everyone and needs to be driven from higher levels. Asset management is an area where a single system supporting the entire organization (beyond just IT or OT) would be ideal. Her small team's challenge is preparing data for the entire organization during crowdsource data procurement, underscoring the need to understand everyone's data needs.

Fostering Early Engagement and Communication

WisDOT has made significant progress in IT-TMC collaboration over the last five to six years. The TMC staff now engage IT during the planning phase of projects, even before funding is secured. For example, they proactively sought IT security's help in reviewing networks. This is attributable to a growing understanding within TMC that IT can provide valuable assistance. The agency has processes in place to vet project ideas at different levels to determine the required IT involvement, from advisory to full leadership. This process often involves collaboratively filling out an IT request form to initiate early communication, to estimate resources, describe the project concept, and define IT's role.

Oregon DOT has been successful with development of their technology and data plan jointly between the agency's IT and OT groups. This 10-year plan outlines priorities for new technology and addressing technical debt. They hold quarterly portfolio management meetings to review active and upcoming projects, resource constraints, and collaboratively make intentional decisions on project prioritization. While they lack a formal workflow for all meetings, they've established clear "lanes" for representation. The IT application manager regularly coordinates with the OT team on operational issues and proactively addresses network modernization. Coordination occurs at multiple tiers, from tactical meetings to portfolio reviews with oversight partners. In addition, they use work item management process for standard maintenance

and support activities (e.g., adding cameras, website updates), ensuring prioritization even for small, day-to-day IT staff work.

From a cybersecurity perspective Michigan DOT's IT staff have had success in "shifting left" on security scanning of vulnerabilities through automation using continuous integration/continuous delivery (CI/CD) pipelines. This integrates security scans directly into the development workflow, catching vulnerabilities as early as code is committed, leading to greater efficiency and discipline. The risk associated with long-term ITS maintenance contractors is a topic that resonated with many participants.

The Pennsylvania Turnpike Commission has been using an IT ticketing system (ServiceNow) for project management since 2019. Pre-project ideas are tracked as "demands," giving the business visibility into both demands and active projects. This list is maintained by their PMO office and reviewed quarterly with the business relationship manager, ensuring ongoing relevance and identifying new needs. This is an evolution from their past reliance on whiteboards and spreadsheets.

Workforce Development: Recruitment and Training

WisDOT uses a combination of full-time employees and contractors, with contractors often sourced and funded by agency divisions. They have observed that there is a pendulum nature to IT hiring during tech booms and downturns. Currently it is a hiring manager's market for IT generalists, but specialized skill sets are harder to find. The current tech downturn offers more applicants for typical IT roles, for example, for a recent Java developer posting they received 95 applicants in one week, compared to 15-25 previously. For the first time since 2017 the IT teams (server, storage, cloud, network, web hosting) were fully staffed in December 2024.

However, filling OT-specific positions remains challenging. OT positions have taken months to fill and require refreshing advertisements. They have had success recruiting individuals with telecom or military experience. For training, the agency is looking for more cross-training and the availability of materials from ITS America and FHWA for OT cybersecurity.

The state government doesn't offer high salaries but provides stability, which is attractive, particularly in uncertain economic times. They have increased efforts in college job fairs for engineering roles and upcoming federal job fairs. There are some differences in hiring rules, e.g., full-time state employees must reside in Wisconsin, even if remote, while contractors have more location flexibility.

Michigan DOT IT has had success in hiring contractors who demonstrate quality work and then converting them to full-time employees, particularly for their cybersecurity team. The agency focuses on individuals with a great attitude and then provides training using resources from ITS America and FHWA to develop them into highly valuable personnel.

Iowa DOT IT staff are being reorganized under the Department of Management but are still assigned and funded by their original agencies, limiting resource sharing. This is expected to change in the next fiscal year, allowing for cross-training, but a hiring freeze currently impacts recruitment and training opportunities.

Texas has moved back to full-time in-office work which more recently may have had an impact on recruiting. TxDOT is working to utilize federal-level training resources more effectively.

Navigating Funding and Federal Requirements for IT/OT Integration

The discussion concluded with a thought-provoking point about the complexities of funding sources and federal requirements as they pertain to the integration of OT and IT. A key challenge highlighted is how to manage projects funded through diverse sources—be it state or regional transportation improvement program (TIP), FHWA funds, or various grant applications. These funding streams come with specific requirements, compliance criteria, and strict timelines.

To effectively navigate these processes across both the OT and IT domains often involves intricate conversations between state DOTs and their FHWA division offices to align with FHWA and USDOT's perspectives on architecture and other essential elements to ensure that projects submitted for federal approval meet all necessary standards. Many IT professionals may not be fully familiar with these federal funding and compliance intricacies, underscoring the need for greater cross-functional understanding and collaboration. A supplemental point is that regular Federal funding in certain categories is eligible for operations costs, including labor, subject to specific criteria. This offers the potential for leveraging existing federal funds for ongoing operational expenses related to integrated IT/OT systems crucial for long-term sustainability.

Session 3 – Practical Needs and Considerations

Introduction to the Conversation

This session revolves around practical needs and considerations categorized into planning, designing, operating, maintaining, and measuring processes. Representatives from New Hampshire DOT, Pennsylvania Turnpike, and Maricopa County shared their experiences as part of a round robin discussion.

Background and Applications

Nicholas King, the TSMO Bureau Administrator from NHDOT began by detailing the structure of their embedded Department of Information Technology (DOIT) staff, which includes two and a half full-time equivalents. Steve Lemire is their DOIT lead who manages the other two embedded staff, one at the TMC. This arrangement has been in place since 2007, coinciding with the opening of their TMC operations which is co-located with state police headquarters. The DOIT staff have dedicated space within the TMC, allowing for real-time awareness of outages and issues impacting services. A challenge for these embedded staff is the organizational reporting to both DOIT and DOT, leading to multiple bosses. The dual reporting structure, while frustrating, actually helps bridge the gap between different DOIT departments and the TSMO Bureau, allowing more effective communication of needs within DOIT.

The NHDOT TSMO Bureau was officially established in 2014, the realization quickly came that communication between various agencies was lacking. To address this, they formed a monthly meeting group called CODES (Communications, Operations, DOIT, Engineering, and Systems), which utilizes an ITS integration flowchart. This group discusses projects, streamlines efforts, and ensures no overlaps in effort and always concludes their meetings with action items.

Their biannual budget, capital expenditures, and $1.3 million federal money is dedicated to TMC operations and covers purchases related to the TMC. They also benefit from a streamlined process where 1.5 percent of every NHDOT project is allocated for TSMO use. This allows ITS or communication solutions

to be incorporated into projects and to secure supplemental funding.

The NHDOT ITS statewide architecture now includes regional planning commissions through a recent Memorandum of Agreement (MOA) which broadens their planning scope beyond just DOT purposes. In addition, the agency has an ITS lifecycle plan for making decisions on replacing aging equipment, such as portable boards with more permanent solutions.

NHDOT has a tri-state contract for their advanced transportation management system (ATMS) with Maine and Vermont, where all three states share costs. New Hampshire takes on the total cost and acts as the contract owner, covering the initial costs and is then reimbursed by the other states. Representatives from all states are present at contract meetings. However, Maine's DOIT can be reactive rather than proactive, occasionally disrupting processes, though New Hampshire tries to engage them consistently.

Brittany Piazza from Pennsylvania Turnpike explained that their Traffic Operations Center (TOC) selected their ATMS solution and continues to work closely on its implementation. An IT project manager is embedded in this process to keep IT informed of desired changes and enhancements. A significant success is their five-year plus ten-year contract for the ATMS, providing stability for 15 years before a new RFP would be necessary.

The Maricopa County DOT system interacts with two regional IT partner groups: a county-wide enterprise technology group and an internal departmental IT group. This dual support helps facilitate projects, with enterprise technology providing access to equipment and the internal IT group managing data movement. The enterprise group is largely "hands-off" the operational network, focusing on support and network building rather than taking over management, which is very helpful. As a long-standing group with many new people, they are actively building out processes, moving away from reliance on consultants to bringing expertise in-house.

Discussion

Standards, Requirements, and RFP Processes

For NHDOT the harmonization of standards and requirements among the three states involved in their tri-state ATMS is achieved through RFP development and regular meetings with IT support from each state. The systems engineering model, a requirement for most federal funding, serves as a baseline for procurement, integration, and operation of devices across all agencies. Reconciling operational differences between the three states during the requirements writing process was complex, requiring compromises to ensure the software accommodated varying state operations.

The Pennsylvania Turnpike Commission as a largely standalone entity and has minimal collaboration with PennDOT, primarily on specific projects like PA511 and work zone speed enforcement. In these joint efforts, the contract holder's rules generally prevail, with both parties contributing security requirements and participating in the RFP process to ensure all needs are met.

New York is moving towards a collaborative RFP model between NYSDOT and OITS, a shift from their past where DOT primarily drove requirements. They will be involving OITS from the beginning to embed all IT, security, and standardization requirements upfront, rather than trying to fit them in later. Previously independent TMCs are now beginning to align their contracts, which will be a challenging but necessary work in progress.

For Maricopa County their regional AZTEC group coordinates data sharing and discusses operational plans, fostering informal collaboration. The county consolidates and manages much of this data and the overall network, giving them control over
network involvement.

Design Process and Coordination

NHDOT coordinates ITS architecture with four MPOs with quarterly meetings through their planning division and monthly meetings of their Transportation Technology and Innovation Committee, where MPOs have a seat and a vote on projects. MPOs are now asking to be included in NHDOT's 10-year strategic plan, foregoing their individual plans. This gives them a significant voice in prioritization, design, and project selection, a level of influence they previously didn't have. NHDOT's ITS architecture design utilizes the FHWA Regional Architecture Development for Intelligent Transportation (RAD-IT) software application.

Operating Aspects: Third-Party Data Integration and Fiber Network

The Pennsylvania Turnpike Commission has seen early success integrating third-party data from an operational and IT perspective, particularly with Waze and Google data providing alerts before traditional calls, significantly aiding safety, and early notification. They also integrate HAAS Alert data to push safety alerts to third-party apps. Beyond consuming data, there's a significant push to share their own data with these entities and others through an enterprise data management project.

A major initiative is connecting devices previously on cellular networks to a statewide fiber network. They are future-proofing cabinets to allow for easy expansion and addition of more cameras and devices. The Commission discovered a significant design detail/specification challenge where the standard backfill practices in contract work often crush conduit, requiring rework. They are revising standards to use sand or protective sleeves for conduit to prevent this issue. Consistency in fiber placement is also crucial for protecting it from future road work.

Maricopa County has similar concerns, noting a recent incident where a contractor hit their fiber optic cable, revealing they lacked an on-call contractor for such repairs. This highlighted the importance of planning for fiber protection during construction.

There is common simplified perception that fiber solely brings successes, while IT oversees all issues. The operations function often believes devices can just be plugged in with fiber, which is not always the case, though they are working towards that ease of integration. The NOCoE has touched on this subject in a prior peer exchange on digital infrastructure, where the idea of just throwing devices up onto fiber received pushback from individuals with practical experience.

Cybersecurity and Standards Requirements

At the Pennsylvania Turnpike Commission all IT-related deployments adhere to standard security requirements, which generally work well. While they sometimes need exceptions (e.g., for data not remaining in the United States), they strive to maintain open communication and work through these issues during the onboarding process.

A common challenge that Michigan DOT sees is vendors who often don't fully read or understand security requirements in RFPs. This leads to post-selection discussions where vendors are surprised by the

full scope of compliance needed. He notes that while vendors can request internal policy changes before bidding, they rarely do.

When NYSDOT solicits contracts, OITS provides a "technical package" attached to the RFP, outlining compliance requirements for technical security, risk, privacy, and AI. Vendors must review these policies and respond in their proposals about compliance, gaps, and how they will achieve compliance. This includes accessibility guidelines and specific hosting options within New York State's governed cloud tenants (Microsoft, Google, Amazon AWS) or their private cloud/DR site. This robust collaboration between NYSDOT and OITS occurs upfront in the RFP crafting process and continues during proposal evaluation, ensuring both business and technical/security needs are met.

Oregon DOT also sees vendors not fully grasping IT and security requirements. Vendors have taken a handwave approach where RFPs broadly state compliance with statewide standards, but the practical implications are often unclear. This results in security being addressed after the fact where IT's 90-page controls document is used as a cudgel during design. A more concise, big-picture one-page brief outlining key security expectations and what doesn't meet their bar, along with a clear security strategy for the entire ITS environment is needed, to make the RFP process more effective.

Day-to-Day Operations and Staffing Models

Participants shared about their day-to-day operations and co-location/embedded staff in TMCs. The Pennsylvania Turnpike Commission has a network control team, which functions as their 24/7 Network Operations Center. Though no longer physically in the same room as the TOC due to COVID, they are in an adjacent room. They monitor dashboards for device issues, proactively enter tickets, and serve as the first point of contact for the TOC for break-fix issues, escalating to vendors as needed. The Commission also has a small internal staff that provides directed response for TOC technology, handling updates to prevent outages. The network control team comprises agency personnel, while ITS maintenance and fiber contracts are managed by external contractor teams.

New York is decentralized, relying heavily on contract staff for systems engineers and other technical roles to maintain and operate networks and equipment in each TMC. They are working towards a more integrated team model with OITS agency partners, contractors, and DOT staff.

Some TxDOT staff work in TMCs, and in some locations, police also work in the same room. Maricopa County is currently hiring a part-time Enterprise Technology, part-time TSMO ITS technology person responsible for security, with expectations that this will be very helpful.

Oregon DOT uses a tiered, hybrid model. Traffic system technicians support field equipment and fiber outside buildings, while a centralized network team manages the network. A TSMO application support team serves as the first line of support for system issues, escalating up to agency security, network, and server teams. They also leverage agency-wide personal computer support for desktops in TOCs but do not have dedicated staff physically in the TOCs.

Iowa DOT uses contracted staff in their TMCs. When their ITS maintenance vendor RFP was renewed, they changed the vendor's responsibilities. Previously, the vendor was responsible for the entire ITS network, including servers, but Iowa DOT realized vendors might not always prioritize the agency's best interests, especially concerning cybersecurity, and may lack expertise. Now, the contractor is primarily responsible for Layer 1 infrastructure, specifically fiber.

Session 4 – Cybersecurity

Introduction to Conversation

This session looked at the intersection of TSMO and IT cybersecurity challenges. Cybersecurity-related themes that are a core concern for both IT and TSMO staff from the prior sessions past two days, include:

- Cybersecurity is a top organizational priority, driven by high-profile incidents and leadership concerns.
- Cybersecurity serves as a driver for interagency and regional collaboration.
- Cybersecurity is a core factor in procurement and governance, including discussions on processes, contract compliance, and cloud vendors.
- Cybersecurity is a focus area for task forces, governance groups, and technical teams.
- Cybersecurity frames discussions around legacy system management, workforce coordination, procurement complexity, and evolving oversight structures.

Again, advance responses from TxDOT and Iowa DOT, and the virtual white board were used to crowd-source answers to a set of questions, in this session directed toward cybersecurity. The first question asked about the single biggest cybersecurity challenge my division/agency is facing right now is:

INFORMATION TECHNOLOGY PERSPECTIVE:	BUSINESS UNIT/ TSMO PERSPECTIVE:
• Integration of cybersecurity with TSMO • IT, ITS, and OT network detection • Meeting IT cybersecurity requirements for TSMO solutions • Network visibility • 3rd party information and systems • Advanced threat detection • TMC engineers expected to having IT and security skills but many do not • Lack of STIX/TAXII feeds • Lack of overall security architecture • Getting hacked and being able to detect it • Public-Private partnership • Keeping devices current in regard to firmware and patching • Change management • Security logging • Internal users of our systems • Vendor indifference to keeping devices/systems patched • Working through the processes for procurement • Every TMC is different including approach to security (*within agency*)	• Where to draw the line between IT and OT • Identity access management • Evolving threat landscape • Taking care of the basics – field equipment, logins, locks, port security • Lack of understanding • Disruptions to systems/devices during large scale incidents • SD-WAN, 5G,and 6G network connectivity • Centralized management • Keeping up with the changing risk environment • Vendor compliance with good security practices • Regulatory compliance • Privileged access management • Security and IT audit • Key Performance Indicators (KPIs) • API integration • DOT collaboration in incidents and threats

What is a cybersecurity and TSMO-related win for your agency? What creative or noteworthy practices have been implemented?

- Coordinated development cycles, gathered regional input, and consolidated into a single statewide plan annually
- Effective Incident Response Plan
- RACI for as-is IT and OT
- SD-WAN
- CISCO Catalyst center and ISE development
- Coordinated Cyber Response. However, not yet clear on triage and mitigation roles and responsibilities
- Security audit for ITS systems
- Establishing regular Microsoft patching for Windows systems
- Pilot testing passive network monitoring system built for OT
- Partnering with IT agency has helped us further our cyber posture
- Implemented Clarity to monitor anything connected to our network
- Standardization of firewalls
- Network Consolidation
- Hiring an agency Chief Information Security Officer who is very well versed cyber matters
- ITS Security Task Force
- Planning shared admin and management platforms for firewalls and field devices
- Implemented multi factor authorization and secure remote access
- Consensus decision to standardize routers and firewalls
- Planning extending fiber connectivity for signals and field devices

Discussion questions for peers:

- How often do you audit your ITS devices for security compliance?
- What are people doing for threat detection and response?
- Curious how organizations broke down the walls between cyber and IT/OT to reach a collaborative relationship.
- How do you manage vulnerability mitigation at scale?
- How do you move past mitigation to secure by design?

- How do you ensure and track asset preventative maintenance/ patching particularly when performed by a vendor?
- Who is monitoring your systems for threats? Is there a systems operations center?
- Have you started to transition to digital locks?
- How do you approach securing technology that was never designed for security in mind?

The question and topics were polled for the highest interest topics and the session began a facilitated discussion.

Aggregating this information, many topics overlap, and a high level summary includes:

- TSMO network locations and field equipment: How interactions happen with field devices.
- Technical debt and legacy systems: Challenges of long-term planning and vulnerabilities.
- Vulnerabilities (broadly defined).
- Third-party information and systems: Including third-party data (e.g., probe data) and compliance with vendors/contractors.
- IT and TSMO realignment and structure: Discussions around RACI charts, embedded IT professionals, and organizational structures.
- Data governance rules: General data management and specific models supporting cybersecurity.
- Culture around cybersecurity: Leadership and executive buy-in.
- Dedicated groups or task forces for cybersecurity.
- Internal processes and reviews.
- Privacy, risk, AI.
- Redundancy and resiliency efforts due to security.
- Security strategy for the whole IT environment and strategic planning.
- Roles and responsibilities for IT versus OT
- Operational practices that support security emphasizing the inherent security within daily operations, distinct from culture or roles.
- Regarding legacy systems – security devices and equipment that ignore security – highlighting that some necessary operational equipment lacks security as a priority.

The discussion summary follows on the highest ranking topics. Topics not discussed will be added for consideration to a future NOCoE cybersecurity peer exchange.

Addressing Technical Debt and Legacy Systems

Matt Sneed from TxDOT discussed their evolving approach to managing OT networks and ITS/TSMO devices. They have the challenge of having "one foot in the future, one foot in the past," with the past being particularly difficult to move away from due to the traditional mindset of keeping things until they break. This approach has been partly driven by the logistical difficulties of replacing devices that require significant traffic disruption.

However, this mindset is changing as TxDOT is now prioritizing upgrades based on whether devices have reached their end-of-life, largely due to cybersecurity concerns. End-of-life equipment cannot be adequately supported, patched, or protected against vulnerabilities. This shift has required not only a cultural change but also adjustments to budgeting and lifecycle planning.

TxDOT has begun a legacy device replacement initiative, prioritizing equipment most critical to their traffic networks, specifically:

- Firewalls: Replaced all traffic network firewalls with newer models, deploying them in high-availability pairs to prevent widespread outages affecting cameras, traffic signals, and dynamic message signs.
- Core Switches: Currently upgrading core switches and plan to move to field switches next year.

The agency has had significant growth in cellular routers, which are crucial for connecting traffic signals, cameras, and various sensors. They have leveraged statewide competitive pricing for quick procurement and reasonable service packages, enabling them to expand from 2,000 to 4,000 connected signals in just a few years, now reaching approximately 5,000 statewide. A key challenge, however, was addressing the technical debt associated with these routers. They were initially deployed with disparate operating systems, configurations, and SIM cards, lacking standardization. TxDOT had to standardize the configuration and management of these routers before they could effectively scale their deployment. TxDOT is not currently using the Cisco SD-WAN platform to manage these field routers but it is on their roadmap.

Iowa DOT has had challenges of getting buy-in for upgrades to address technical debt. Chris Pelton shared the example of a critical standalone server used for ITS maintenance that lacked redundancy. The proposal to virtualize and update its operating system met resistance from users accustomed to the existing setup. Creating understanding with the user community starts with communicating the benefits of such changes to users, stressing the risks of relying on a single point of failure, and how an outage would impact their daily operations. Gaining user buy-in is a common struggle when addressing technical debt.

The security implications of technical debt, particularly for operational technology (OT) stems from many legacy devices were designed without security in mind, often only support older, less secure protocols like SNMP v1. A more subtle issue is how the robustness of traditional business applications, which can tolerate latency, differs from the "fragility" of network services and devices in the ITS realm. Advanced traffic controllers, for instance, may be sensitive to latency, making it challenging to implement secure tunneling or other layering techniques without negatively impacting their performance. This adds another dimension to the technical debt of devices not built with security considerations, as they prioritize real-time operations over network robustness.

There is an overwhelming amount of change currently underway in New York. OITS is consolidating 10 individual TMCs into a single enterprise system to leverage statewide contracts, pricing, and maintenance. This involves replacing 20-year-old traffic signal controllers, integrating TMC and traffic signal management into a new ATMS system, launching a new 511, and adding modems to all traffic signals. The situation as being "underwater" with technical debt. OITS's approach is to take small steps focusing on one issue at a time due to the sheer scale of the challenge.

Cloud vs. On-Premise Servers

TxDOT is encouraged to use state cloud services despite challenges. Iowa DOT confirmed they use a mixture of cloud and virtual on-premise servers. NYSDOT anticipates using a hybrid approach for their new ATMS system, which they are trying to put in the New York State governed cloud, but they will still need on-premise video servers at the TMCs.

Oregon DOT prefers virtualizing existing physical servers on-premise rather than simply "lifting and shifting" them to the cloud. They bias towards cloud solutions for Software-as-a-Service (SaaS) or when cloud-native services can be leveraged, but not for traditional server deployments that still require patching and management in the cloud. Michigan DOT shares a similar perspective to Oregon DOT, indicating they are moving away from a "cloud-first" to a "cloud-smart" approach, leveraging cloud solutions when it truly makes sense, particularly for SaaS. Many of their ATMS-based systems remain on-premise.

NH DOT, representing a smaller state, notes that their ATMS is hosted on AWS for all three participating states, but their video systems are on-premise due to the complexities of pushing all video streams to the cloud.

Roadside Detectors and Third-Party Data

WisDOT raised a question about scaling back installation of roadside detectors given the availability of robust data from third-party sources like INRIX and TomTom. WisDOT is being pressured to deploy RSUs roadside units (RSUs) everywhere but questions the necessity of traditional speed detectors between interchanges, suggesting they might be an unnecessary investment compared to available probe data.

Oregon DOT has scaled back and removed all Bluetooth sensors used for travel time measurement and stopped deploying pure speed detection devices, relying instead on their INRIX contract for data portal access, which they use to measure delay in work zones. They have been reducing their roadside infrastructure footprint where virtual solutions suffice.

Securing Inherently Insecure Technology

The group discussed approaches to securing technology that was never designed for security in mind, which has become a common struggle. At Michigan DOT, their primary IT strategy is defense in depth, focusing on solid network design and minimizing the attack surface when devices cannot be patched or replaced. This involves stringent firewall rules and perimeter zones to segment the network and protect more vulnerable devices. The agency performs application scans from an insider threat perspective, assuming network penetration to evaluate for privilege escalations, reinforcing that security isn't just about the outer shell.

Oregon DOT IT uses the defense in depth approach as well, but that has tension with the modern

security concept of “zero trust.” While network segmentation creates a hard outer shell, zero trust principles dictate that internal network presence alone shouldn’t grant broad access. There is a need to reconcile these approaches when dealing with inherently insecure legacy OT which suggests that focusing on the hard outer shell puts a greater onus on secure operational practices and access control.

There are also very practical physical security issues including the widespread use of common keys (aka the #2 key problem) for ITS cabinets, allowing access across multiple jurisdictions. NHDOT has an unapproved grant proposal to update ITS cabinets with secure access measures. Michigan DOT noted the difficulty of protecting against a crowbar but adds that at least a camera would show someone breaking in. NYSDOT confirmed they experience many physical break-ins but are more concerned with digital access than physical.

Michigan DOT sees that full zero trust might be impossible and their approach includes testing applications from an insider threat perspective to identify vulnerabilities even if the network is breached. A question was raised about agencies’ experience using the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) or private companies for red-teaming and penetration testing on their systems on a wider scale. NHDOT worked with CISA for penetration testing on their systems, network, and physical location. The resulting report highlighted vulnerabilities and was used to secure leadership buy-in for cybersecurity initiatives, including the development of an RFP for a managed safety security provider. The CISA testing was free of charge but difficult to schedule, taking several months. CISA also provides follow-up evaluations.

An agency is in the early stages of implementing a hut security system for their fiber connection points. This system uses an alert system controlled by their network operations center, requiring authentication before granting access. This is intended to mitigate security threats at these critical network access points, as cameras are seen more for monitoring than prevention.

It was observed that insider threats are real, citing an instance of city agency personnel intentionally disrupting traffic management systems. Many city agencies have used Urban Area Security Initiative (UASI) grants from DHS to install keypad access and upgraded locks on traffic signal and ITS cabinets, especially along evacuation routes. This provides knowledge of who accessed the cabinets (staff, police, third-party maintenance personnel, etc.).

Roles and Responsibilities for IT vs. OT Cybersecurity

Iowa DOT noted a win in their organization by standardizing their firewall platform on Palo Alto software. This eliminated the need for IT staff to be experts on multiple firewall brands (e.g., Fortinet, Checkpoint) and streamlined support, leading to more efficient issue resolution.

TxDOT uses an approach to clarifying roles by creating a matrix for each device type (firewalls, core switches, field switches, racks, fiber patch panels, etc.). This matrix delineates responsibilities for initial purchase, minor enhancements, monitoring, physical hands-on work, and maintenance. He explains that it took six versions and extensive collaboration with IT, perimeter groups, network teams, and TMC staff to reach a consensus, ensuring no questions about who is responsible for what, even including specific vendor names.

The TxDOT exercise to create the RACI matrix began with a simple, “crayon-style” network diagram showing typical district network deployments from firewalls to field devices (point-to-point radios, cellular routers). Each device was numbered and mapped to a table detailing the specific group or

vendor responsible for purchasing, maintenance, monitoring, and incident remediation. Vendor names were confirmed to eliminate ambiguity. Other agencies expressed an interest in more detail on how TxDOT structured the conversations to delineate roles, especially given the IT agency's potential lack of OT experts.

Next Steps

Gaps and Future Actions

This peer exchange encompassed a broad exchange of ideas on current challenges and successes with TSMO and Information Technology from the participation of various agencies across the country. NOCoE will meet the AASHTO, ITE, ITS America, and FHWA representatives to review the peer exchange findings and work on next steps as well as potential products.

Undiscussed questions from the cybersecurity session will serve as a starting point for an upcoming cybersecurity peer exchange. Based on participants' feedback, it is anticipated that the following priority topics and questions need to be further explored.

Topics for consideration of resource development:

- Revisit and refresh the TSMO workforce definitions to explicitly address how to integrate with partner agencies, especially IT support agencies, as current definitions might be too standalone within the DOT context. Address how to build deep specialization on the IT side for a transportation systems specialization.
- Models for deploying software-as-a-service, cloud computing and hybrid/cloud service.
- Tools to establish joint IT/OT roadmaps for enterprise architecture matching with ITS architecture requirements.
- To find a home for this IT/OT community of practice within AASHTO, perhaps through a subcommittee in CTSO or in some other manner.
- Share insights from the IT/OT convergence that could benefit the ITS Standards program with the lead SDOs, AASHTO, ITE, and NEMA.
- Tools to identify and prioritize technical debt and impacts on other aspects such as budget, training, and workforce as well as mechanisms to maintain while replacement is sought
- Case study or best practice report on OT and IT coordination using RACI matrix. Follow up with Matt Sneed (TxDOT) on clean version of their RACI matrix as an example.
- Case studies or best practice report on defining IT/OT boundaries, organizational structures, and processes.
- Information for IT on CAV implementation and implications for IT of RSU installations.
- Case studies or best practice report on approaches for agile joint IT/OT processes for procurement, deployment, and/or system maintenance of TSMO technologies.

In initial feedback from participants, they expressed feeling less isolated after realizing other organizations face similar challenges, emphasizing the value of the new network of contacts. This work, though sometimes thankless, significantly benefits their agencies and the public. They are part of the greater picture. NOCoE and its partners are willing to connect participants with peers facing similar issues.

Resources

Federal Highway Administration

Coordination of Information Technology and TSMO web page has links to multiple resources:

- *Coordination of Information Technology and TSMO* primary landing page with links to resources.
- *Coordination of IT and TSMO* fact sheet

TSMO funding eligibility information:

- *Transportation Systems Management & Operations: Operating Cost Eligibility Under the Federal-Aid Highway Program*

NOCoE

- Model TSMO Position Descriptions

ITE

- Links to ITS Standards (ATC, CAV/CI, Cybersecurity, NTCOP, TCIP)

New York state

New York State DOT

- Request for Proposals for Contract, Attachment XX – Ongoing System Support, Maintenance and Enhancement Requirements
- Request for Proposals for Contract, Attachment XX – NYS Information Technology Services (ITS) Requirements
- ITS / DOT Quality Assurance/Quality Control and Release and Deployment Process for DOT Vendor Contract Solutions

New York State Office of Information Technology Services Standard

- ITS Standard: Service Oriented Architecture