Coordination of IT and TSMO

U.S. Department of Transportation
Federal Highway Administration

Project Executive Summary

COMMON UNDERSTANDING

Agency Successes

Staffing Practices

Cybersecurity Practices

This is one of five fliers that highlight aspects of coordination between Information Technology (IT) and Transportation Systems Management and Operations (TSMO) in transportation agencies. Each flier draws from *Principles and Strategies for Effective Coordination of IT and TSMO, a Reference Document* (https://ops.fhwa.dot.gov/publications/fhwahop21008/index/htm).

The role of IT is becoming increasingly central to TSMO. Leading edge TSMO strategies involve increasingly complex and interrelated systems, organizations, and institutions. Real-time and predictive tactics, such as active traffic management, integrated corridor management, and vehicle-to-infrastructure systems, are characterized by high levels of complexity and a dependence on integrating with IT. A principle objective of the FHWA IT-TSMO project was to identify common IT-related challenges experienced by TSMO staff and effective practices that have been implemented to resolve those challenges.

COMMON CHALLENGES

The project identified the following IT-TSMO coordination challenges:

Institutional	Business and Technical Processes
Cultural	Strategic Planning
Staff and Financial Resources	Procurement
Organizational	Systems and Technology
Policy	Risk/Security

EFFECTIVE PRACTICES

Many agencies have had success in overcoming their IT-TSMO coordination challenges by employing practices in the following categories:

☑ **Collaboration**

☑ **Program Delivery**

☑ **Staffing**

☑ **Equipment/Systems**

☑ **Planning and Programming**

Enhancing Common Understanding Between TSMO and IT Staff

TSMO and IT groups bring distinct perspectives, roles, and practices in seeking to improve business processes for which they are responsible. Often, these two groups may not have extensive exposure to each other's mission or operational responsibilities. Focus areas for targeting improved understanding between the two groups are explained below and summarized in the table that follows.

Governing Principles

Governing principles reflect the values of an organization and are of primary importance in day-to-day activities. For TSMO professionals, those principles are focused on safe and efficient operations. Technology-based systems must be available whenever they are needed, regardless of the time of day or day of week. It is important for IT staff to understand the urgency that TSMO staff view uptime of TSMO assets, and to structure their support to respond accordingly. For IT professionals, those principals are based on ensuring reliable delivery of services, including maximizing uptime and operating IT systems 24/7. They are also focused on protecting IT assets, especially from cybersecurity threats.

Domains Components

Domains include the devices and assets that comprise the networks of interest. For TSMO, the domains consist of field devices and data sources, operations center servers, and communication components that link them. The domain for IT is quite large and can include data centers, databases, back office systems, and the internal and external network communications that links them. Most of the domain is located within office environments. Security is essential. It is important for TSMO staff to understand the IT environment and the desire for consistency across large enterprise networks and systems.

Risk Management

Within TSMO, the most important risks relate to the safety of the transportation system. TSMO elements need to fail safe or "fail soft." The risks are often greatest when these elements are needed most, such as during peak traffic periods, traffic incidents, or emergency situations. Within IT, the biggest risks involve system integrity, and protecting the IT network and other IT assets from unauthorized intrusion. Malicious intrusions can compromise the entire enterprise network, including financial systems and private data.

As a risk management technique, the Michigan DOT (MDOT) invited the Michigan Department of Technology, Management and Budget (DTMB) to help identify vulnerabilities in its ITS communications network. The DTMB cyber security group analyzed MDOT networks, identified cyber risks, and informed MDOT about the vulnerabilities, which MDOT was then able to address.

Standards and Architecture

Core TSMO standards and development models relate to system engineering, ITS Architecture, and ITS devices. It is important for IT staff to understand the background of these standards and the public-facing nature that they serve. IT standards typically revolve around security, technology compatibility, and a variety of hardware and software standards. In addition, IT systems often need to comply with State legislated or Chief Information Officer mandated standards and policies that serve the full range of IT services provided to all their client agencies.

Asset Management

Managing TSMO assets emphasizes the needs and requirements for maintaining and repairing specific devices at specific (often field) locations. TSMO assets generally last longer than most IT assets because of their hardened nature. The result is often a mix of equipment that requires a broad range of troubleshooting and repair skills. Managing IT assets emphasizes strict adherence to asset maintenance levels. IT assets generally have a shorter lifecycle than TSMO assets. Software and technology asset licenses must also be managed to protect against financial or performance risk.

Future Technologies

Future technology trends for both TSMO and IT will likely center around new functionality and increased efficiency. Practitioners expect TSMO systems and processes to utilize expanded data sources, larger quantities of data, and more automation. Newer technologies may include support for connected and automated vehicles, smart cities, mobility on demand, and other emerging concepts. Future technologies that will be incorporated within IT will be driven by evolving business needs across the agency or throughout a centralized IT management approach. Trends include movement toward more cloud storage and cloud computing, mobile access, and reliance on increasingly sophisticated web services.

The Pennsylvania Turnpike runs a large tolling operation that relies on both TSMO and IT staff to operate a safe, reliable, customer-valued toll road system. The Turnpike makes a concerted effort to integrate IT staff into the operation's business to encourage better understanding and collaboration between the two groups. From a leadership perspective, the IT group is aligned with the Turnpike's mission and was included in the operations strategic plan. The IT group has also been included in major efforts, such as the TSMO Capability Maturity Model (CMM) workshop.

Category	What IT professionals need to know about TSMO	What TSMO professionals need to know about IT
GOVERNING PRINCIPALS	Ensuring safe and efficient day-to-day operations through: ▪ Maximizing system "uptime," especially during critical demand. ▪ Operating systems whenever conditions dictate, 24/7. ▪ Interfacing with outside parties to share information and control.	Ensuring reliable business-focused delivery of services through: ▪ Maximizing IT system "uptime," especially during peak use. ▪ Operating IT systems and networks according to business demands 24/7. ▪ Ensuring cybersecurity.
DOMAIN COMPONENTS	Multiple domains that must work together: ▪ Traffic operations center/data center. ▪ Data sources from third parties and field devices. ▪ Communications to link centers and data sources.	Multiple domains that must work together: ▪ Data center/back office. ▪ Database. ▪ Security. ▪ Internal and external network communications.
RISK MANAGEMENT	Considered from transportation system operations perspective: ▪ Transportation systems are operational 24/7. ▪ Systems need to fail safe or fail soft. ▪ Troubleshooting should occur with minimal impact to system operation.	Considered from software/hardware and network resilience perspective: ▪ System outages can affect enterprise-wide business continuity. ▪ Unauthorized intrusions can jeopardize network wide operations. ▪ Inconsistent systems and applications can increase repair time and cost.
STANDARDS AND ARCHITECTURE	The range of standard practices include: ▪ Systems engineering and ITS architecture. ▪ ITS device standards. ▪ Hardened equipment (maximum availability).	The range of standard practices include: ▪ Enterprise architecture. ▪ Technology compatibility standards. ▪ Hardware/software standards.
ASSET MANAGEMENT	Managing TSMO assets emphasizes: ▪ Needs/requirements for maintaining and repairing traffic management specific devices at specific locations. ▪ Relatively longer lifecycle than IT assets. ▪ Highly reliable legacy devices with limited capabilities.	Managing IT assets emphasizes: ▪ Strict adherence to current maintenance levels. ▪ Relatively shorter life cycle than TSMO assets. ▪ Technology asset and license management. ▪ Newer devices with greater flexibility.
FUTURE TECHNOLOGIES	Technology considerations include: ▪ Using emerging technologies and data sources are critical to meet growing transportation needs and challenges. ▪ Many of the new technology are market-related and come out of the private sector.	Technology considerations include: ▪ Managing ever evolving advances in hardware/software with business needs. ▪ Movement toward more cloud computing and web services.

For More Information:

Jim Hunt, FHWA Task Manager ☎ 202.680.2679 @ jim.hunt@dot.gov

U.S. Department of Transportation
Federal Highway Administration