Coordination of IT and TSMO

U.S. Department of Transportation
Federal Highway Administration

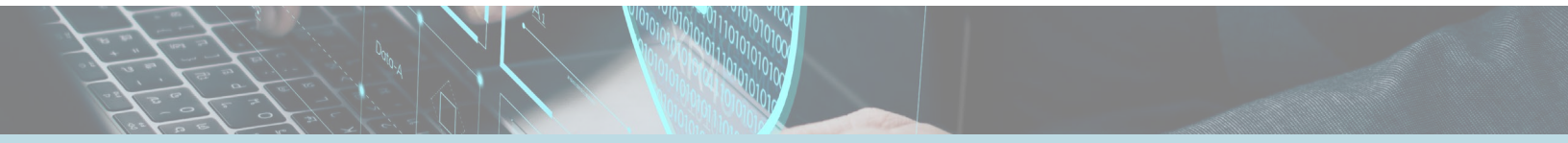
Source: Getty Images

CYBERSECURITY PRACTICES

This factsheet, one of five in a series, focuses on cybersecurity and highlights transportation agency coordination between Information Technology (IT) and Transportation Systems Management and Operations (TSMO). Each factsheet draws from Principles and Strategies for Effective Coordination of IT and TSMO, a Reference Document.

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.

The reference linked above identifies a range of IT-related challenges facing TSMO organizations and practices for addressing those challenges. One of the challenges discussed in the Reference Document relates to cybersecurity vulnerabilities that threaten TSMO and other agency IT systems and networks.



Practices to Address Cybersecurity Vulnerabilities

The technology infrastructure used to support TSMO can be a source of cybersecurity vulnerability. Agencies have used the following practices to foster improved coordination and cooperation between TSMO and IT for the purpose of strengthening the cybersecurity aspects of their TSMO programs.

Michigan Department of Transportation (MDOT) Integrates IT Staff within TSMO

MDOT integrated IT staff into the TSMO organization with the goal of enhancing collaboration and understanding of their respective missions. IT staff and TSMO staff work collaboratively to analyze cybersecurity risks and recommend approaches to eliminate or mitigate vulnerabilities, while ensuring that mission-critical TSMO functions are not disrupted.

California Department of Transportation (Caltrans) Created Policies to Require and Encourage Coordination

Caltrans created internal policies and procedures that require mandatory “touch points” or coordination efforts with the California Department of Technology. IT staff involved early in the process help develop the vision for a project, assist in procurement strategies, and assess future IT maintenance and support needs. Caltrans believes that all have viewed the mandatory "touch points" positively and, as a result, IT staff regard for transportation systems has increased, particularly with the standardization of security practices that both agencies have deemed critically important.

New Hampshire Department of Transportation (NHDOT) Leveraged External Organizations to Assess Cyber Vulnerabilities

NHDOT took part in a National Guard cyber-training exercise known as “Cyber Yankee,” in which NHDOT built a virtual network simulating its Intelligent Transportation System (ITS) network. National Guard cybersecurity specialists probed the virtual network and the physical assets connected to it to find vulnerabilities. They were able to uncover the password to hack into it and post a message to a dynamic message sign. NHDOT used this experience to work with IT staff to close vulnerabilities in its network.

Pennsylvania Turnpike Commission Incorporates IT Staff in Systems Engineering Process

The Pennsylvania Turnpike Commission includes its IT staff in TSMO project development. IT staff are involved early and throughout the systems engineering process to reduce risk and speed the process. The commission has found that inclusion of IT staff adds value through their expertise in identifying and addressing potential security issues early in project planning and project development.

Maricopa County and AZTech Defined and Coordinated Data Sharing and Access Agreements

Transportation systems often involve sharing data and, at times, sharing functions such as controlling closed caption TV cameras with outside agencies. Maricopa County, Arizona, formalized access to data and device control though written agreements within a consortium of transportation agencies know as AZTech. These agreements clarify access rights, restrictions, and security protocols. IT staff provided the expertise both parties believed were needed to assess vulnerabilities and proposed ways to provide access to data and systems control while minimizing vulnerabilities and intrusion risks.

Florida Department of Transportation (FDOT) Created a Data Governance and Management Plan

Technology systems that generate a significant amount of data present data governance and management challenges. FDOT worked with its IT partners to develop a Data Governance and Management Plan to ensure appropriate data access, ownership, integrity, quality, and control. Data governance includes methods, technologies, and behaviors that promote proper management of data to address security and privacy, integrity, usability, integration, compliance, availability, roles and responsibilities, and overall management of the internal and external data flows within an organization. The Data Governance and Management Plan also identified how data is collected, organized, stored, and archived. IT staff were involved from the outset of the process to determine appropriate data formats, storage location, and security protocols.

In summary, the technology and data platforms underpinning TSMO applications introduce security risks. It is important for TSMO and IT to jointly work on solutions to ensure that best security practices are implemented in ways that will meet TSMO business needs. The reference and the other IT-TSMO factsheets are available at:
https://ops.fhwa.dot.gov/plan4ops/focus_areas/integrating/it.htm

For More Information:

Jim Hunt, FHWA Office of Operations | 202.680.2679 | jim.hunt@dot.gov

U.S. Department of Transportation
Federal Highway Administration