Photo source: U.S. DOT

Cybersecurity is a serious and ongoing challenge for the transportation sector. Cyber threats to transportation systems can impact national security, public safety, and the national economy. The Cybersecurity for ITS research area was developed in response to the urgent need to protect intelligent transportation systems (ITS) from cyber-attacks.

CYBERSECURITY FOR ITS

The biggest challenge to the ITS ecosystem is a result of the increased value of ITS data and connectivity. Concerns about cybersecurity for ITS and traffic management deployments are related to both current technologies as well as legacy systems, coupled with the growing trend to integrate ITS deployments with other networks. This combination has introduced new threats that have not been previously encountered in this domain.

Cybersecurity Research at the ITS Joint Program Office (JPO)

The U.S. DOT's ITS JPO is uniquely positioned to work across the Department modes and with their modal partners to develop and coordinate multimodal projects central to cybersecurity research. This work includes convening and facilitating the transportation ecosystem around shared priorities, facilitating the development of related policies, identifying and addressing cross-modal issues, and sharing best practices and information while eliminating activities that may hinder cooperation across teams.

The ITS JPO also offers leadership, information, and resources to state and local agencies that cross modal boundaries and ensure risk management across all of the transportation enterprise technology components. State, Local, Tribal, and Territorial (SLTT) agencies do not necessarily have access to the type of expertise or the resources needed to pursue research initiatives to improve their daily operational mission and cyber hygiene. Further, needs that cross jurisdictional boundaries and apply nationally can be efficiently addressed via ITS JPO leadership and coordination.

Cybersecurity Research Objectives

Achieving the proposed vision is a sizable challenge. But as our understanding of ITS risks evolves, so too have the methods used in other sectors and industries to measure, assess, and manage risk. The following four strategies are offered as a logical path forward for industry, government, and academia to realize and sustain the vision.

Adapt and Implement Protective Measures to Reduce Risk Preferentially. *Next-generation ITS architectures provide "defense in depth" and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber-incident.*

- The National ITS Architecture Reference incorporates Confidentiality, Integrity, and Availability (CIA) analysis for all the data flows in the ITS Architecture. CIA analysis is a basic best practice for all organizations trying to secure their communications, and state and local agencies can use this as a starting point when analyzing their own architectures.

ITS JPO High-Priority Research Areas

- Automation
- Data Access and Exchanges
- Emerging and Enabling Technologies
- Cybersecurity for ITS
- ITS4US Deployment
- Accelerating ITS Deployment

Alignment with U.S. DOT Strategic Goals

Safety

Economic Strength and Global Competitiveness

Equity

Climate and Sustainability

Transformation

Organizational Excellence

U.S. DOT | Cybersecurity Reseach Partners

Private Sector Firms

Non-Federal Public-Sector Organizations

Federal Organizations

NIST

U.S. Department of Transportation
Federal Highway Administration

U.S. Department of Transportation
Federal Motor Carrier Safety Administration

U.S. Department of Transportation
Federal Transit Administration

NHTSA

Transformative Goal:

ITS will be cyber-resilient. The vulnerabilities that ITS deployments create in the transportation system will be continually and systematically assessed at all levels so that risks associated with malfunction or malfeasance are mitigated to an acceptable level and resiliency plans exist.

- ITS Standards activities are underway to identify implementation guidance and best practices that can be added to key ITS infrastructure standards.
- The U.S. DOT partnered with the National Institute of Standards and Technology (NIST) to tailor the NIST Cybersecurity Framework to address connected vehicle systems.

Assess and Monitor Risk. *Continuous cyber risk monitoring of all ITS architecture levels and across cyber-physical domains is conducted by transportation sector asset owners and operators.*

- The U.S. DOT sponsored a penetration test of a state and local agency to demonstrate the value of and provide guidance on conducting this type of testing and identify best practices based on the findings of the testing itself.

Manage Incidents. *Transportation sector stakeholders are able to mitigate a cyber-incident as it unfolds, sustain critical operations during the incident, return to normal operations quickly, and derive lessons learned from incidents and changes in the ITS environment.*

- The U.S. DOT sponsored the development of the Secure Credential Management System Proof of Concept, which secures vehicle-to-vehicle and vehicle-to-infrastructure communications.
- The U.S. DOT developed a Transportation Cybersecurity Incident Response and Management Framework that improves communication and information sharing with transportation roadway stakeholders when detecting and responding to a cyber-attack or vulnerability that spans across devices or other sectors.

Creating an Organizational Culture of Security. *Cybersecurity practices are reflexive and expected among all transportation sector stakeholders.*

- The U.S. DOT is developing training through the ITS Professional Capability Building program on specific cybersecurity topics.

Partnering to Address Challenges, Leverage Lessons Learned, and Ensure Success

The distributed ownership, operation, and oversight of the transportation system among federal, state, and local governments as well as the private sector imposes complexities for implementing cybersecurity solutions and information sharing in this ecosystem. However, a wealth of knowledge and resources has been developed in other sectors that the U.S. DOT can leverage and adapt for the ITS ecosystem.

To leverage this expertise, the Department is partnering in cybersecurity research with private sector firms and non-federal public-sector organizations, as well as the following federal organizations:

- National Institute of Standards and Technology
- Department of Homeland Security
- Department of Defense
- Department of Energy
- Federal Highway Administration
- Federal Motor Carrier Safety Administration
- Federal Transit Administration
- National Highway Traffic Safety Administration.

The Presidential Executive Order 14028 Improving the Nation's Cybersecurity (issued May 12, 2021) holds Departments accountable for managing cybersecurity risks of their ecosystem, and further encourages Departments to work with stakeholders to adopt the NIST Cybersecurity Framework.

The ITS JPO has partnered with the Connected Vehicle Pilot sites to adapt the NIST Cybersecurity Framework for connected vehicle environments. They have provided expertise from public and private firms on user requirements and countermeasures that are critical to establishing Cybersecurity Framework guidance for the connected vehicle environment. An effort to apply the Cybersecurity Framework to the much more complex and diverse ITS infrastructure environment began in 2022 and will continue through 2023.

To learn more about this program, contact:

Steve Sill, ITS Architecture, Standards and Cybersecurity Program Manager
U.S. DOT ITS Joint Program Office
(202) 366-1603 | *Steve.Sill@dot.gov*