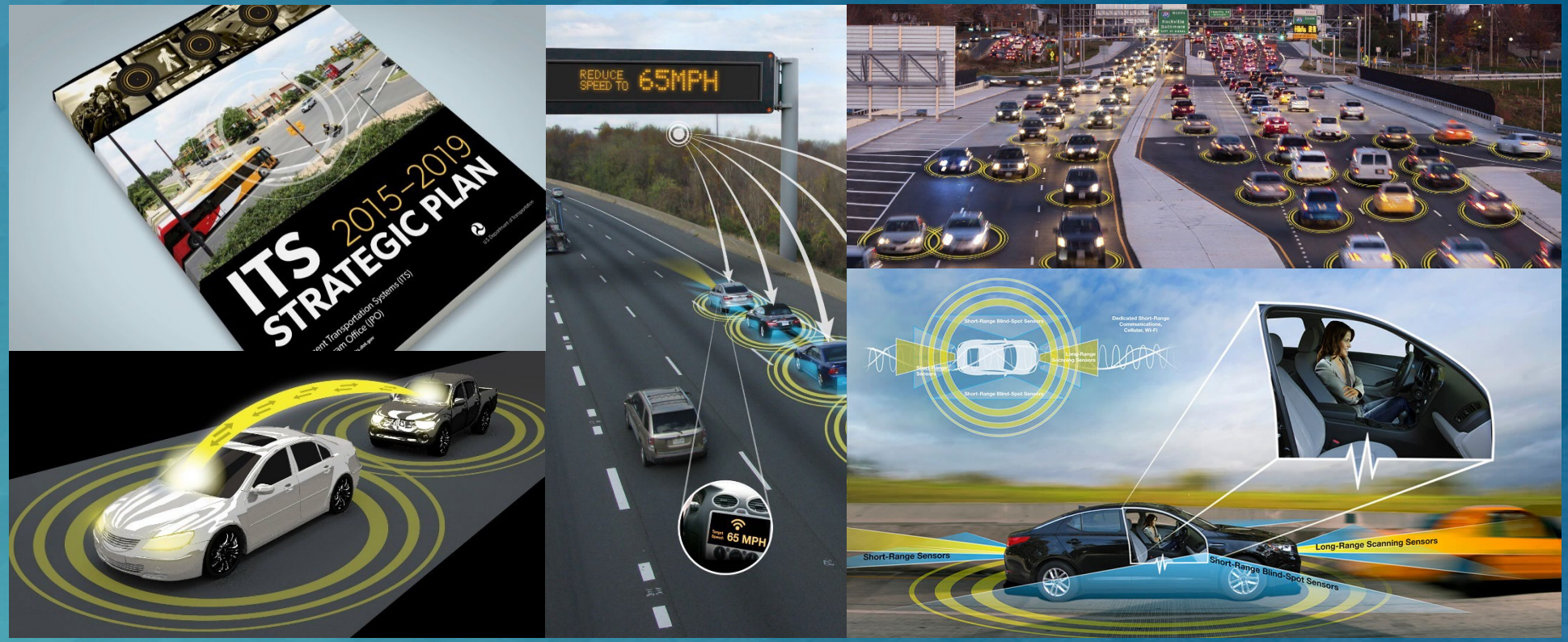
U.S. Department of Transportation



INTELLIGENT TRANSPORTATION SYSTEMS (ITS) CYBERSECURITY ACTIVITIES
US DOT ITS JOINT PROGRAM OFFICE (JPO)

JANUARY, 2020

ITS INFRASTRUCTURE CYBERSECURITY CHALLENGES

- ITS Infrastructure systems employ a wide diversity of devices, many never designed with security in mind
  - ITS infrastructure devices can be decades old
  - ITS infrastructure security was predicated on the idea that ITS networks were completely private
- ITS networks vary widely between states and localities
  - Diverse network are architectures and types/mix
  - No “one size fits all” solutions

HOW TO ADDRESS ITS INFRASTRUCTURE CHALLENGES

- Focus on areas where nation-wide interoperability is critical to success, and provide detailed security guidance
  - Likely a small number of information flows within the ITS reference architecture
  - Would likely include: Probe Data collection; Signal, Phase and Timing (SPaT) dissemination; V2V and V2I safety message exchange; Signal Priority
- Evolve the security guidance supporting these flows in the architecture reference
- Specify appropriate ITS Standards to support nationwide interoperability
- Where most beneficial, develop and maintain Reference Implementations (RI)
  - Ease interoperable deployments

ITS JPO SUPPORTED CYBERSECURITY PROJECTS

Ongoing
1. Application of the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF) to the Connected Vehicle Environment
2. Assessment of selected State DOT cyber infrastructure against Federal IT standards
3. Develop a Transportation Cybersecurity Incident Response and Management Framework
4. NIST Cybersecurity Profile for the ITS Ecosystem

Completed
1. Distributed Ledger Application for Transportation (Blockchain)
2. ITS Infrastructure Penetration Testing
3. Cybersecurity of Traffic Management Systems/Centers
4. Roadway Transportation System Cybersecurity Framework and Tools

APPLICATION OF THE NIST CYBERSECURITY FRAMEWORK TO THE CONNECTED VEHICLE ENVIRONMENT

Purpose

- Establish a candidate Cybersecurity Framework Profile and Privacy Guidance that will help state, local and regional organizations apply the principles and best practice of risk management to improve the cybersecurity and resilience of critical transportation infrastructure. The CSF Profile is implemented to understand their baseline cybersecurity posture and develop an understanding of the priority measures they should take to improve it.

Tools & Products:

- Connected Vehicle Environment Profile
- Implementation Guidance
- Privacy Risk Assessment

ASSESSMENT OF STATE DOT CYBER INFRASTRUCTURE

Purpose

- This project is assessing State transportation organizations against cybersecurity requirements for *Federal* systems to apply risk-based methodology in identifying gaps in need of remediation.
- Focus on how state transportation agencies are securing their ITS deployments rather than on enterprise, “back-end” systems.

Expected Results

- Information on how to apply existing Federal regulations, standards and practices

DEVELOP A TRANSPORTATION CYBERSECURITY INCIDENT RESPONSE AND MANAGEMENT FRAMEWORK

Purpose

- Develop a framework for 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.

Tools

- Develop Strategies to Establish Consistent Usage of Cybersecurity Terminology (Common Glossary)
- Identify Information Sharing Organization(s) and Define Transportation Infrastructure ISAC Requirements
- Develop/Adapt Cybersecurity Incident Communication Protocols

NIST CYBERSECURITY PROFILE FOR THE ITS ECOSYSTEM*

Purpose

- Development of a NIST CSF specific to the ITS ecosystem, along with guidance for State and Local agencies to adapt the profile for their environment. The CSF Profile is implemented to understand their baseline cybersecurity posture and develop an understanding of the priority measures they should take to improve it.

Expected Results

- Candidate ITS Environment Profile
- Implementation Information and Model Templates

*To be initiated in FY2020

DISTRIBUTED LEDGER APPLICATION FOR TRANSPORTATION (BLOCKCHAIN)

Purpose

- Analyze the potential application of Distributed Ledger Technology (DLT) within the Intelligent Transportation System domain.
- Evaluate the ITS architecture framework as a whole and outlined service packages that would be likely candidates to benefit from a DLT solution.
- Conduct an analysis of the application of DLT within these service packages and evaluated the potential advantages and disadvantages of this technology.

Results

- Case study on the Application of a Distributed Ledger solution for the ITS service packages TM01 Infrastructure-Based Traffic Surveillance and TM03 Traffic Signal Control.

ITS INFRASTRUCTURE PENETRATION TESTING

- Planned and conducted a full penetration test in cooperation with an infrastructure owner operator (IOO)
  - Looked at multiple areas of the transportation infrastructure including field devices such as the advanced transportation controllers (ATC) and ITS cabinets as well as the traffic management center (TMC) and backhaul networks
- Multiple critical vulnerabilities were found and exploited during testing
- Detailed report was delivered to the participating IOO (identity of IOO is not being revealed while they address vulnerabilities)
- A best practices document was developed providing general recommendations for how to plan and conduct a penetration test for ITS infrastructure which includes general security best practices based off the detailed findings
  - This document can be found at: https://rosap.ntl.bts.gov/view/dot/42461

CYBERSECURITY OF TRAFFIC MANAGEMENT SYSTEMS

Sponsored by the National Cooperative Highway Research Program (NCHRP)

Project Team: Southwest Research Institute (SwRI) and Praetorian

Purpose

- This program aimed to guide transportation agencies in assessing their Traffic Management Systems' risk, gaining an understanding of its current cyber-security standing, and taking steps to improve their security posture.

Products/Tools

- Cybersecurity Risk Assessment Web Guidance Tool
- Risk Assessment of Typical Traffic Management System Design
- Cybersecurity and Privacy Primer for Deployment of Connected/Automated Vehicle Technologies

ESTABLISHING A ROADWAY TRANSPORTATION SYSTEM CYBERSECURITY FRAMEWORK AND TOOLS

Sponsored by the Federal Highway Administration (FHWA) and ITS JPO

Project Team: *Institute of Transportation Engineers (ITE), American Association of State Highway and Transportation Officials (AASHTO), ITS America, National Electrical Manufacturers Association (NEMA), and the National Association of City Transportation Officials (NACTO)*

Purpose

- Provide a means of rapid, secure communication of relevant cybersecurity challenges among trusted stakeholders.
- Provide a common means whereby all stakeholder classes may communicate as equals to discuss and develop guidance to address cybersecurity challenges.
- Develop response options that may be implemented as cybersecurity threats materialize.

Products & Tools to be available via National Operations Center of Excellence (NOCoE) website https://transportationops.org/cyberfmwk

- Cyber Transportation Systems Framework
- Toolkit for Creating or Reviewing Your Cyber Resiliency Plan

STAY CONNECTED

Websites:

www.its.dot.gov

standards.its.dot.gov

www.arc-it.net

Steve Sill, PE
ITS Architecture, Standards and Cybersecurity Program Manager
ITS Joint Program Office
US Department of Transportation
steve.sill@dot.gov