U.S. Department of Transportation
Federal Highway Administration

July 2024

FHWA/USDOT
Transportation Cybersecurity Resources

NHI Training

(High-Level and Basic) NHI 137055 - Transportation Cybersecurity
Available at: https://www.nhi.fhwa.dot.gov/course-search?tab=0&key=137055&sf=0&course_no=137055
The FHWA National Highway Institute offers an online course to introduce transportation professionals to cybersecurity challenges. It covers topics such as cyber threats, vulnerabilities, and tools for enhancing resilience in transportation systems.

Technical Reports, Online Resources, and Tools

(Informational) USDOT Intelligent Transportation Systems Cybersecurity Research Program
Available at: https://www.its.dot.gov/research_areas/cybersecurity

This website provides the latest USDOT research and tools in transportation cybersecurity.

(Basic) Transportation Cybersecurity Wargaming Exercise Guide
Available at: https://rosap.ntl.bts.gov/view/dot/75259
This guide assists State, local, tribal, and territorial (SLTT) highway agencies in conducting simple self-paced cybersecurity wargaming exercises. It covers planning steps and example scenarios to enhance cyber readiness without external assistance.

(Basic) Transportation Cybersecurity Glossary
Available at: https://www.standards.its.dot.gov/DeploymentResources/CyberGlossary
This glossary provides a list of common and standardized terminology for the transportation and cybersecurity community to improve communication across disciplines. It includes definitions of cybersecurity and transportation terms along with illustrative examples. Visitors to the website can download an Excel version of the glossary to use as a local reference.

(Intermediate) Transportation Cybersecurity Incident Response and Management Framework
Available at: https://rosap.ntl.bts.gov/view/dot/57007
Incident Exercise Summary Report: https://rosap.ntl.bts.gov/view/dot/57311
Outlines a communication framework for transportation stakeholders to detect and respond to cyber-attacks or report discovered vulnerabilities across devices. The framework supports a cyber incident response exercise similar to a Department of Homeland Security “Cyber-Storm” exercise. The summary report presents proposed procedures and data collected from completed incidents, including participant actions evaluated against rubrics in the incident exercise plan.

(Intermediate) Cybersecurity Language for the Procurement of Intelligent Transportation System Equipment
Available at: https://rosap.ntl.bts.gov/view/dot/73792
This report provides example cybersecurity language that can be developed and inserted into contracts when procuring intelligent transportation systems (ITS). It identifies security principles such as software updates/patches, cybersecurity maintenance, vulnerability disclosure policies, breach notification, and initial device or system configurations.

(Intermediate to Advance) ITS Cybersecurity Penetration Testing Guide
Available at: https://rosap.ntl.bts.gov/view/dot/42461
Titled "Cybersecurity and Intelligent Transportation Systems: Best Practice Guide," this report details the methodology for an operating agency to scope a penetration test for ITS operational technologies.

(Intermediate to Advance) Transportation Management Center Information Technology Security
Available at: https://ops.fhwa.dot.gov/publications/fhwahop19059
This report is focused on best practices from NIST and the Center for Internet Security to reduce vulnerabilities of transportation management centers (TMCs). This is intended for use by TMC managers working and information support professionals to reduce vulnerabilities.

(Advance) Intelligent Transportation Systems (ITS) Cybersecurity Framework Profile
Available at:
1. ITS Cybersecurity Framework Profile: https://rosap.ntl.bts.gov/view/dot/72769
2. Template and Instructions: https://rosap.ntl.bts.gov/view/dot/72781
3. Procedures for Developing Security Control Sets: https://rosap.ntl.bts.gov/view/dot/72784
4. Control Set for Traffic Signal Controllers: https://rosap.ntl.bts.gov/view/dot/72772

These documents contain a profile for ITS devices for use with the NIST Cybersecurity Framework version 1.2. They are intended to help organizations prioritize cybersecurity capabilities and inform their cybersecurity decisions. A control set for traffic signal controllers was also developed and will be expanded to cover other ITS devices and updated to be consistent with the current version of the NIST framework.

(Operators and Vendors) ITS Security Configuration Application Functional Prototype
Available at:
https://github.com/usdot-fhwa-OPS/ITS-Secure-Prototype-App
https://github.com/usdot-fhwa-OPS/ITS-Secure-Prototype-Frontend
https://github.com/usdot-fhwa-OPS/ITS-Secure-Prototype-Backend
This is a functional prototype to demonstrate how a portable application can be a valuable tool for field technicians to reduce cybersecurity vulnerabilities of field equipment. The tool also demonstrates to equipment vendors how sensitive and proprietary information can be protected. Open source code for the functional prototype will be available for vendors to further develop or use as a model to deliver production software.

Research

NCHRP Web Document 355: Cybersecurity Issues and Protection Strategies for State Transportation Agency CEOs
Volume 1, Project Summary Report available at: https://www.trb.org/Publications/Blurbs/182976.aspx Volume 2, Transportation Cyber Risk Guide available at: https://www.trb.org/main/blurbs/182986.aspx

NCHRP 03-127: Cybersecurity of Traffic Management Systems
The project website is available at:
https://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=4179

NCHRP Report 930: Security 101: A Physical Security and Cybersecurity Primer for Transportation Agencies (2020)
Available at: https://www.trb.org/Publications/Blurbs/179516.aspx

Non-Binding Contents

Except for the statutes and regulations cited, the contents of this document do not have the force and effect of law and are not meant to bind the States or the public in any way. This document is intended only to provide information regarding existing requirements under the law or agency policies.