FHWA's Transportation Cybersecurity Strategic Plan

This plan is intended to serve as a starting point for a collaborative process with Federal Highway Administration (FHWA) Office of Operations stakeholders that will result in a roadmap for achieving cybersecurity for critical assets on the highway system. This plan could ultimately guide decisionmaking about the policies, standards, research, market development, and procurement required to minimize transportation disruptions due to a cyber incident. This is in response to the urgent need to protect these assets from cyberattack and align sectorwide resources to meet that need. The plan recognizes that protecting against every potential intrusion is impossible and focuses on building an infrastructure that could continue critical operations in the face of a cyber incident. This plan accounts for the activities and noteworthy practices that already exist or are under development.

One item of note is the use of the terms "cybersecurity" and "cyber resiliency." The distinction here is "security" focuses on not allowing the attackers in the system, while "resiliency" is much broader and also includes response and recovery should an attack occur. This document will use the term cybersecurity, the accepted term in the transportation community. However, the intent is to shift the conversation toward the use of cyber resiliency.

The Vision

A strategic plan is needed for the highway community that addresses the cybersecurity concerns of today's systems while preparing for the needs of tomorrow. The following vision statement describes what success could look like for transportation professionals in a 5-plus-year timeframe:

A TRANSPORTATION SYSTEM THAT IS RESILIENT TOWARD CYBERATTACKS

Strategic Cyber-Resiliency Goals

Achieving the proposed vision is a sizable challenge. But, as our understanding of risks evolve, so too have the methods used in other sectors and industries to measure, assess, and manage risk. The following three goals offer a logical path forward for industry, government, and academia to realize and sustain the vision:

1. Senior leadership and other units understand why they should care about cybersecurity and what roles and responsibilities they have.
2. FHWA, State, and local staff have sufficient cybersecurity knowledge, skills, and abilities and have protocols in place to defend, respond to, and recover from cyberattacks.
3. Stakeholders are able to identify, mitigate, and report cyberthreats and vulnerabilities.

Strategies

The following strategies align with the goals:

1. Create a culture that supports transportation cybersecurity for FHWA, State, and local stakeholders.
2. Increase cybersecurity capabilities for FHWA, State, and local personnel necessary for their duties.
3. Identify and integrate national standards and policies to support State and local cybersecurity activities.

The strategies form the core of the strategic plan, which is laid out in table 1. First, each strategy is mapped to the relevant dimension of capability from transportation systems management and operations (TSMO), so that this plan is consistent with the strategy the community already uses. Each strategy is tied to distinct milestones and timeframes. Finally, table 2 maps specific projects to the outcomes and timeframes from table 1.

Nonbinding 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.

TABLE 1. STRATEGIC PLAN WITH MILESTONES MAPPED TO GOALS.

Vision	**A transportation system that is resilient toward cyberattacks**		
Goals	**1. Senior leadership and other units understand why they should care about cybersecurity and what roles and responsibilities they have.**	**2. FHWA, State, and local staff have sufficient cybersecurity knowledge, skills, and abilities and have protocols in place to defend, respond to, and recover from cyberattacks.**	**3. Stakeholders are able to identify, mitigate, and report cyberthreats and vulnerabilities.**
Strategies	**1. Create a culture that supports transportation cybersecurity for FHWA, State, and local stakeholders.**	**2. Increase cybersecurity capabilities for FHWA, State, and local personnel necessary for their duties.**	**3. Identify and integrate national standards and policies to support State and local cybersecurity activities.**
TSMO Dimensions	**Culture, Organization and Workforce, Business Processes, Collaboration**	**Systems and Technology, Organization and Workforce, Business Processes**	**Performance Measurement, Collaboration, Systems and Technology, Business Processes**
Near-term Outcomes (0–3 years)	1.1 Executive engagement and support of cybersecurity and cyber-resiliency efforts are standard practices 1.2 Cyberthreats, vulnerability, mitigation strategies, and incidents are shared in a timely manner among appropriate sector stakeholders 1.3 The transportation sector understands their role in accordance with accepted cybersecurity sector cyber-resiliency definitions. The greater resiliency community of stakeholders collaboratively define and accept the role for cybersecurity and cyber resiliency. 1.4 Stakeholders internal to FHWA, modal partners, and State and local organizations are engaged and support cybersecurity and cyber-resiliency efforts 1.5 Lessons learned from cyber incidents are shared and implemented throughout the transportation sector	2.1 Common terms and measures specific to each transportation subsector are available for baselining a security posture in operational settings 2.2 The transportation sector leverages commercially available capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes 2.3 Transportation-tailored cybersecurity training content is available, and current cyber-event detection tools that evolve with the dynamic threat landscape are commercially available 2.4 Tools to support and implement cyberattack response decisionmaking for the human operator are commercially available 2.5 Support other FHWA efforts to incorporate cyber-resiliency considerations where needed	3.1 An Intelligent Transportation System (ITS)-specific National Institute of Standards and Technology (NIST) Cybersecurity Framework Profile exists with applicable control sets 3.2 Tools to identify cyber events across all levels of ITS system networks are commercially available 3.3 Each transportation subsector accepts and implements incident reporting guidelines 3.4 The majority of asset owners baseline their security posture using subsector-specific metrics 3.5 Field-proven noteworthy practices for ITS security are widely employed 3.6 Vendor systems and components using secure coding and software assurance practices are widely available and provide noteworthy practices for risk monitoring
Mid-term Outcomes (3–5 years)	1.6 Transportation-sector leadership understands the compelling business case for investment in transportation cybersecurity 1.7 Collaborative environments, mechanisms, and resources for connecting security and operations researchers, vendors, and asset owners are widely used	2.6 Tools for real-time security-state monitoring and risk assessment of all ITS system architecture levels and across cyber-physical domains are commercially available	3.7 Continuous risk assessment monitoring is in standard use across an ITS enterprise
Long-term Outcomes (5+ years)	1.8 Cyber-performance measures are collected	2.7 The industry employs significantly more workers skilled in ITS, information systems, and cybersecurity; capabilities for automated response to cyber incidents, including noteworthy practices for implementing these capabilities, are available	3.8 Mature, proactive processes to rapidly share threats, vulnerabilities, and mitigation strategies are implemented throughout the transportation sector 3.9 Security solutions enable transportation mission-critical operation to continue during a cyberattack

TABLE 2. STRATEGIC PLAN WITH PROJECTS MAPPED TO GOALS.

Vision	**A transportation system that is resilient toward cyberattacks**		
Goals	**1. Senior leadership and other units understand why they should care about cybersecurity and what roles and responsibilities they have.**	**2. FHWA, State, and local staff have sufficient cybersecurity knowledge, skills, and abilities and have protocols in place to defend, respond to, and recover from cyberattacks.**	**3. Stakeholders are able to identify, mitigate, and report cyberthreats and vulnerabilities.**
Strategies	**1. Create a culture that supports transportation cybersecurity for FHWA, State, and local stakeholders.**	**2. Increase cybersecurity capabilities for FHWA, State, and local personnel necessary for their duties.**	**3. Identify and integrate national standards and policies to support State and local cybersecurity activities.**
TSMO Dimensions	**Culture, Organization and Workforce, Business Processes, Collaboration**	**Systems and Technology, Organization and Workforce, Business Processes**	**Performance Measurement, Collaboration, Systems and Technology, Business Processes**
Completed	National Cooperative Highway Research Program (NCHRP) 23-03 Guidelines for State Transportation Agency Chief Executive Officers on Cybersecurity Issues and Protection Strategies	NCHRP Project 03-127 Cybersecurity of Traffic Management Systems	Apply NIST Cybersecurity Framework to Connected Vehicle (CV) Environment
			Establish a Roadway Transportation System Cybersecurity Framework and Tools
		Transportation Management Center Information Technology Security	Develop a Transportation Cybersecurity Incident Response and Management Framework
			Service Specific Permissions (SSP) and Security Guidelines for CV Applications (SAE J2945/5)
	National Institute of Standards and Technology (NIST) Cybersecurity Profile for the Intelligent Transportation System (ITS) Ecosystem	Transportation Cybersecurity Incident Response and Management Framework	Sensor-based Misbehavior Detection (MBD) for a CV environment
			NIST Cybersecurity Profile for the ITS Ecosystem
		Surface Transportation Infrastructure Penetration Testing	National Transportation Communications for ITS Protocol (NTCIP)
			9014 Infrastructure Standards Security Assessment (ISSA)
			Minimum Viable Product (MVP) MBD
In-Progress	*No data	ITS Cybersecurity Professional Capacity Building	Develop a roadmap for improving cybersecurity across NTCIP family of standards (ITS Standards)
		NTCIP 9014 ISSA	
		Develop Sample Cybersecurity Procurement Language	Initiate Analysis of Cybersecurity for Transportation System Users
			NTCIP 1218 Roadside Units (RSU) center to field control of RSUs
		Update National Highway Institute (NHI) Training Content	SAE J2945/5 SSP and Security Guidelines for CV Applications
		ITS Assessment Tool	Small Business Innovation Research 21-FH4: Reference Hardware for Infrastructure Global Positioning Systems (GPS) Abnormality Detector for Connected and Automated Vehicle Applications
		Wargaming exercise framework for State, Local, Tribal, and Territorial agencies	
Planned start —under 4 years	Conduct outreach with resiliency community	Create NHI training on the ITS Cybersecurity Profile	Develop additional control sets to the NIST Cybersecurity Profile for the ITS Ecosystem
	Coordinate this cyber strategy with internal FHWA stakeholders, U.S. Department of Transportation modal administrations, and other Federal agencies	Support CyberStorm exercise	
Planned start — 4+ years	Development of programmatic cyber-performance measures	*No data	Collect and analyze cyber-incident information to assess program impact
Planned start based on event trigger	*No data	Develop Reference Architecture for Intersection Radio Monitoring Unit, Trigger: stability with the spectrum situation with vehicle safety communication	Cyber-Performance Measures, Trigger: maturity of transportation system penetration testing methods