Transportation Systems Cybersecurity and Cyber Resilience Whitepaper

Michelle J Barnes
Assistant Research Scientist
Texas A&M Transportation Institute
The Texas A&M University System
# TABLE OF CONTENTS

**Abstract** ........................................................................................................................................... 3

**Background on Cybersecurity and Transportation** ........................................................................... 4
  Why is it important? ................................................................................................................................. 4
  What are the risks to transportation providers? .................................................................................... 4
  What are the risks to the public? ........................................................................................................... 7

**Description of State of the Practice and Knowledge Gaps** ............................................................ 8
  How are cybersecurity threats and cyber resiliency being addressed now? ........................................ 8
  What are the stated research needs? .................................................................................................... 11
  Where are there noticeable gaps? ........................................................................................................ 14

**Conclusion** ........................................................................................................................................ 16

**Acknowledgments** ......................................................................................................................... 16

**List of Figures**

<table>
<thead>
<tr>
<th>Figure 1. Workforce Need.</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>15</td>
</tr>
</tbody>
</table>

**List of Tables**

<table>
<thead>
<tr>
<th>Table 1. DOT Computing Milestones</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2. DOT Cyber Functions</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6</td>
</tr>
</tbody>
</table>
ABSTRACT

This white paper explores cybersecurity and cyber resiliency in transportation systems. Cyber issues are dynamic and increasingly more integrated as transportation technology and communication rapidly grow.

Potential risks for transportation providers from cyber attacks include financial losses, disruption of service, theft of data, reputational damage, and potential security impacts. For the public, associated risks range from a minor inconvenience to a catastrophic safety consequence to the masses. Users expect confidential, consistent, and safe operations.

Transportation systems need to prepare their security for information technology and operational technology devices to minimize cyber vulnerabilities, defend against attacks, and plan for when cyber-attacks happen to ensure their resiliency. There are many resources and available tools for transportation providers to address cyber risk; however, there are also remaining knowledge gaps. The research needs for cybersecurity and cyber resilience as related to transportation systems will continue to grow as cyber elements in transportation accelerate.

The Texas A&M Transportation Institute (TTI) is poised to be an important link in filling the research needs and gaps by providing its unique transportation subject matter experts in partnership with the cybersecurity experts within The Texas A&M University System.

The objectives of this paper are to:

- Provide a basic background of cybersecurity and cyber resilience;
- Explore the cyber risks to transportation providers and users;
- Identify the available tools for transportation providers to address cyber risk; and
- Identify knowledge gaps and future research needs for cybersecurity and cyber resilience.
Background on Cybersecurity and Transportation

Why is it important?

Modern transportation systems are very integrated and more dependent on cyber communication and information technologies. This will likely only increase in the future. Core transportation functions such as positioning, navigation, tracking, shipment routing, industrial systems controls, access controls, signaling, communications, and data and business management extensively use cyber technologies.¹ When technology is compromised there are many potential repercussions: jeopardized public and employee safety, adverse effects on agency reputation and user confidence, loss of proprietary information, release of personally identifiable information or confidential data, economic loss, and impact on national security. Transportation agencies across the country are challenged to learn more about the cybersecurity of their systems, develop, and implement cybersecurity programs to reduce and or mitigate cybersecurity vulnerabilities.² Furthermore, revolutionary technologies are being developed for the future of transportation such as unmanned aircraft systems or drones and connected and automated vehicles (CAV). Their integration into existing systems are still being developed.

Complementary to cybersecurity is cyber resiliency. An organization’s cybersecurity strategy is a way to reduce the possibility of an attack being successful; however, a cyber resilience strategy is also necessary to assure our transportation systems continue to perform in an acceptable fashion even when under attack. Cyber resiliency is a combination of political, strategic, and operations decisions made by elected officials and senior agency managers and embedded in agency business policies, plans, processes, and workflows.³ Cyber threats require constant management, and agencies must realize they are never completely capable of preventing all threats.

What are the risks to transportation providers?

Over the years as adoption of technology has rapidly increased, the agency’s vulnerability has also increased. It is a real challenge for the agencies to keep up with evolving systems and related risks. Transportation agencies are realizing that they cannot plan, build, or operate their respective infrastructures to achieve and maintain the degree of reliable and resilient service expected by society and its elected representatives using the approaches, technologies, and mindsets of the past.⁴

The initial use of in-house computing devices by departments of transportation (DOTs) kept the agencies relatively isolated from threats. The first generation of digital devices and systems remained more isolated, less connected, and therefore less at risk to cyber attacks. However, in more recent years as cloud or network computing connects all the increasingly sophisticated components, not only are single components at greater risk but so are entire systems.\(^5\)

Table 1 illustrates how DOTs have embraced and implemented technology while simultaneously decreasing their control over technology.\(^1\)

<table>
<thead>
<tr>
<th>Cyber Milestone</th>
<th>Year Introduced</th>
<th>Units (worldwide)</th>
<th>Degree of DOT Control</th>
<th>Degree of Cyber Attack Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOT Computing</td>
<td>1953</td>
<td>NA</td>
<td>Very High</td>
<td>Very Low</td>
</tr>
<tr>
<td>Mainframes</td>
<td>1965</td>
<td>10 K</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Personal Computers</td>
<td>1983</td>
<td>2 B</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Web Browsers</td>
<td>1994</td>
<td>2-3 B</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Smartphones</td>
<td>2007</td>
<td>2.7 B</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Internet of Things</td>
<td>2010</td>
<td>12.5 B</td>
<td>Very Low</td>
<td>Very High</td>
</tr>
</tbody>
</table>

Note: NA = not applicable.

Transportation systems are cyber-dependent in three domains:

- informational technology (IT);
- operational technology (OT), also referred to as industrial control systems; and
- consumer technology (CT).

The IT systems collect and process the data and information with an emphasis on protecting the confidentiality, availability, and integrity. IT also includes sensitive employee and customer information. IT is usually the responsibility of the IT professionals. OT is hardware or software that monitors and controls the physical devices. The OT systems are usually the responsibility of the engineers and operators, and safety and reliability is emphasized. Historically, IT and OT were separate; however, more recently these systems are converging as the data storage and data monitoring for OT transitions to online storage and processing. CT in modern transportation systems allows employees, travelers, shippers, and almost everyone else to have access to and

interact with DOT services using a variety of apps, platforms, and social media. Users expect to be provided accurate and immediate information on their phones. Table 2 below provides examples of IT, OT, and CT as relating to transportation operations system management.

Table 2. DOT Cyber Functions

<table>
<thead>
<tr>
<th>System Type</th>
<th>Category</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Technology: Traditionally the responsibility of the IT professionals.</td>
<td>Engineering</td>
<td>Surveying, CADD, GIS, electronic bidding</td>
</tr>
<tr>
<td></td>
<td>Business management</td>
<td>Accounting, human resources, fleet and fuel management, resource planning, email systems, archives</td>
</tr>
<tr>
<td></td>
<td>Asset management</td>
<td>Highway and bridge inventory and inspection</td>
</tr>
<tr>
<td></td>
<td>Point of sale</td>
<td>Licensing, titling, registration</td>
</tr>
<tr>
<td>Operational Technology: Traditionally the responsibility of the transportation engineers and operators.</td>
<td>Control systems</td>
<td>Advanced traffic management system, train or bus control systems</td>
</tr>
<tr>
<td></td>
<td>Supervisory Control and Data Acquisition (SCADA)</td>
<td>Road/weather systems, traffic monitoring and surveillance, railroad crossings, the Global Positioning System (GPS), traction power, emergency ventilation system monitoring (pumps, alarms)</td>
</tr>
<tr>
<td></td>
<td>Signaling</td>
<td>Highway signals, train signals, signal priority systems</td>
</tr>
<tr>
<td></td>
<td>Passive Communications</td>
<td>Advance traveler information systems, highway advisory radio, dynamic/variable message signs</td>
</tr>
<tr>
<td></td>
<td>Mobile Communications</td>
<td>Security Credentials Management System for CAV, FirstNet messaging, Highway Emergency Link Platform alerts</td>
</tr>
<tr>
<td></td>
<td>Fare collection</td>
<td>Electronic toll collection, transit entry/exit gates, ticket vending, fare boxes, fare validators, ticket encoding</td>
</tr>
<tr>
<td></td>
<td>Building management</td>
<td>HVAC, building or property access, tunnel ventilation, fire detection and suppression</td>
</tr>
<tr>
<td>Consumer Technology</td>
<td>Social media</td>
<td>Traveler information</td>
</tr>
<tr>
<td></td>
<td>Mobile</td>
<td>Applications</td>
</tr>
<tr>
<td></td>
<td>Employee access by personal device</td>
<td>Email on phone</td>
</tr>
</tbody>
</table>

When IT data, OT controls, and CT privacy are not provided consistently, transportation providers risk:

- financial losses to the providers (ransomware payment, disruptions increase costs and impact revenue);
- disruption of services or halting of operations affect public and employee safety, movement of goods and people;
- theft of operations system, proprietary information, confidential data, or consumer data;
- reputational damage to the providers and decrease user confidence; and
- potential impact on national security.

Cyberattackers range from individual hackers, hacktivists, international criminal enterprises, terrorist groups, and major nation-states. These adversaries can target vulnerabilities at any point in the cyber supply chain from OT hardware to end users. The threat increases in sophistication as well as in magnitude but all have unifying goals of either taking control, stealing information, and/or disrupting service. The Industrial Control Systems Cyber Emergency Response Team has broadly created three groups of “Threat Agents” distinguished by degree of motivation, level of talent, financial support, and extent of available resources.

- Group 1 – anyone with the requisite technical knowledge. For example, reprogramming of portable dynamic message signs for “fun and notoriety” among peers.
- Group 2 – organized crime syndicates, activist groups, insiders, disgruntled employees, and hacktivist groups. Ransomware or malware are an example of Group 2 threats.
- Group 3 – terrorist and nation-states engaged in cyber warfare.

Conversations are necessary in transportation agencies to understand their cyber risks and the consequences of the loss of products and services for their system and its users. Cyberattacks are inevitable, and constant effort must be taken to improve the security and resilience of the transportation systems.

**What are the risks to the public?**

As vital and extensive as modern transportation systems are, they mostly escape notice until they do not function for the public. Users expect a system that is confidential, has continuity of operations, and provides consistent information. There is a risk associated with wrong information and loss of confidence in our transportation systems. Disruptions result in increased costs, lack of faith, reduced usage, and privacy and safety concerns. There are many reported cyber incidents in transportation that result in a wide range of disruptions from changing messages on roadside signs to halting public transportation. These can be just an inconvenience to a few or cause catastrophic consequences to community safety.

For example, in May 2016, a Cedar Park, Texas, man hacked and changed a highway sign to say “Drive Crazy Yall” as a prank. The culprit was identified, arrested, and charged with criminal mischief. The perpetrator admitted to guessing the login credentials for the sign, deleting the original message to warn traffic of upcoming construction, and typing the prank message for humorous purposes. The changes caused a loss of $100,000 to the sign owner. The internet is full of pictures of previous highway sign hacks, and it is easy to find “how to” descriptions and videos.
In March 2018, a ransomware attack on Atlanta’s municipal government infrastructure shut down many functions for several days, and manual workarounds continued for weeks. These were inconveniences such as: residents could not pay bills online, police had to file reports manually, court dates were rescheduled, and much more. Baltimore was also hit in March 2018 with a ransomware attack shutting down emergency dispatching for 17 hours. The Colorado DOT was hit twice in a month with ransomware attacks in 2018 shutting down 2,000 computers. And Mecklenburg County, North Carolina, (containing the city of Charlotte) had to rebuild its entire IT system after a ransomware attack that began with a phishing email. It took over 60 days for operations to return to normal.\(^\text{10}\) The Texas Department of Transportation (TxDOT) experienced a security breach and some employees’ personal information was altered and compromised in February 2017.\(^\text{11}\) TxDOT experienced a ransomware event in May 2020. An article published by GovTech.com estimates that this event cost TxDOT over $10 million to identify and minimize disruptions to operations. These costs may be reimbursed by TxDOT’s cyber insurance policy purchased in 2019 for protection for toll revenue bondholders.\(^\text{12}\) Senator Cesar Blanco filed SB 1908 (HB 3390) for additional funding for a second cybersecurity insurance policy for TxDOT. This bill passed both houses and was signed by the governor in May 2021.\(^\text{13}\) The ransomware incident at TxDOT followed another ransomware attack on over 20 local Texas governments.\(^\text{14}\)

More recently in September 2021, the Port of Houston was breached by a Chinese advanced persistent threat actor. The actor took advantage of a zero-day vulnerability (a flaw in security software) in less than eight seconds.\(^\text{15}\) The goal of the attacker is unknown.

Users need consistency in information and service. Transportation providers need tools and guidance to help them best navigate the quickly changing cyber elements of the systems they manage. What is being done to address these needs?

**Description of State of the Practice and Knowledge Gaps**

**How are cybersecurity threats and cyber resiliency being addressed now?**

There are several publications and resources available to help transportation agencies assess their cyber risk, evaluate their assets, and prepare to be more resilient. Every organization has a unique structure and unique components, and there is no program, technology, or training that fits every agency. Each of these items is discussed below.


To help organizations manage cybersecurity risk, the National Institute of Standards and Technology (NIST) Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity was developed after an executive order in 2013 (EO 13636) called for its development to manage cybersecurity risks for those processes, information, and systems directly involved in the delivery of critical infrastructure services. This cybersecurity framework provides a set of industry standards, methodologies, procedures, and processes that align policy, business, and technological approaches. The core functions are to: identify risks, protect services, detect cyber security events, respond appropriately, and recover services. The framework includes the importance of business confidentiality and protection of individual privacy and civil liberties.16

The NIST Framework, developed in 2014 and updated in 2018, is important because the national and economic security of the United States depends on the reliable functioning of critical infrastructure; however, it is general and included many more critical infrastructure sectors. A more specific plan for the transportation systems sector (TSS) was needed to best manage cybersecurity risk for the TSS seven subsectors: aviation, highway and motor carrier, maritime transportation system, mass transit and passenger rail, pipeline systems, freight rail, and postal and shipping. The Transportation Security Administration (TSA), United States Department of Transportation (USDOTr), United States Coast Guard, and TSS stakeholders created an implementation guide with more relevance to the TSS with the mission to continuously improve the security and resilience posture of the nation’s transportation infrastructure in order to ensure the safety and security of people and goods throughout the country and overseas. The Transportation Systems Sector-Specific Plan also updates the cybersecurity efforts to align with cyber threats, consequences, and advances initiatives in EO 13636 by helping agencies self-assess their current practices; identify areas of improvement; learn about existing tools, standards, and guidelines; and communicate their risk to stakeholders.1 The NIST Framework and more specific TSS Plan is voluntary and is intended to help organizations at any level of cybersecurity readiness.

Similar to the framework, the National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience is a result of EO 13636. The National Plan integrates the cyber and physical security and resilience of critical infrastructure assets, systems, and networks in an effort to manage risk and secure infrastructure from ever-evolving cyber threats.17

As a part of Department of Homeland Security (DHS), the nation’s Cybersecurity and Infrastructure Security Agency (CISA) was established in 2018 as the national coordinator for critical infrastructure security and resiliency. CISA works with industry and government to defend against cyber and physical threats to critical infrastructure.18

CISA partnered with the Computer Emergency Response Team Division of Carnegie Mellon University’s Software Engineering Institute to create the Cyber Resilience Review (CCR) for critical

---

infrastructure owners and operators. This program was established by CISA as a means to enable secure voluntary information sharing between critical infrastructure and the government. The CCR is a free and voluntary assessment to evaluate an organization’s operational resilience and cybersecurity practices and can be a self-assessment or facilitated on-site by a DHS representative.\(^\text{19}\)

In 2018, the National Cooperative Highway Research Program (NCHRP) 20-59(51) updated the original 2009 Security Primer with two documents: NCHRP Web-Only Document 266: Developing a Physical and Cyber Security Primer for Transportation Agencies (2020)\(^\text{20}\) and NCHRP Research Report 930: Update of Security 101: A Physical Security and Cybersecurity Primer for Transportation Agencies.\(^\text{21}\) These documents are designed for transportation personnel without a security background and address the evolving threats and hazards to the systems. The primer was updated with the current approaches, resources, and available tools for all transportation modes under state control or influence.

To support DOTs and others incorporating resilience concepts throughout their organizations, a resilience guide and self-assessment tool was developed in NCHRP 20-117, Deploying Transportation Resilience Practices in State DOTs. Another product of this research was a Resilience Innovations Summit and Exchange in 2018, where best practices for resilience among state DOTS and others was shared.\(^\text{22}\)

NCHRP Research Report 970 offers a self-assessment tool and framework to help transportation agencies incorporate resilience into their decision-making and support processes with the 2021 document, Mainstreaming System Resilience Concepts into Transportation Agencies: A Guide.\(^\text{23}\) This report was the feature of a May 2021 Transportation Research Board (TRB) webinar, Enhancing the Capacity for Transportation System Resilience, that presented how agency staff can self-assess their transportation resiliency.

NCHRP 03-127 developed a software application with the purpose of helping state and local transportation agencies mitigate cyber-attack risks in their traffic management system field network called TRB Risk Assessment Web Guidance Tool.\(^\text{24}\) The online software tool addresses the vulnerability of field devices, field communication networks, and field-to-center communications.

National Information Sharing and Analysis Centers (ISACs) are sector-based information sharing communities. ISACs help critical infrastructure owners and operators protect their facilities, personnel, and customers by sharing cyber and physical threats, vulnerabilities, and solutions with


their members. They help their members improve situational awareness, mitigate risks, and enhance resiliency.25

Further research focused on how the ISACs were used to produce a framework for improved cybersecurity communication and incident information sharing in the Federal Highway Administration report titled, *Transportation Cybersecurity Incident Response and Management Framework.*26

There are programs around the country such as the Colorado Emergency Preparedness Partnership and the Texas A&M Engineering Extension Service Cyber Readiness Center that offer a variety of cyber security training, services, and advice. The training is funded through grants through DHS/Federal Emergency Management Agency and include a variety of topics for technical and non-technical audiences.

The Texas Department of Information Resources (DIR) is available for state and local government entities for security resources and services. It is their mission to “serve Texas government by leading the state’s technology strategy, protecting state technology infrastructure, and offering innovative and cost-effective solutions for all levels of government.” Texas DIR runs Risk and Authorization Management Program that helps certify cloud-computing services for state agencies and institutions of higher education as required by the Texas Legislature SB 475.27

Even with the available tools and completed research to help secure cyber systems in transportation, there is a growing demand for cyber insurance to help transportation infrastructure systems recover from cyber incidents. However, uniformity in approach by insurers is lacking, and further research on cyber risk models, metrics, biases, and insurance is needed.28

**What are the stated research needs?**

A concerted effort was made to gather sources stating different research needs for cyber security and cyber resilience in transportation systems. Research focusing on finding the cyber issues, analyzing the risks in innovative ways, and creating resolutions for a quickly evolving cyber world is still needed.

The Presidential Policy Directive 21 in February 2013, directed DHS and other federal departments to create the *National Critical Infrastructure Security and Resilience Research and Development Plan* (National CISR R&D Plan) to guide research and design (R&D) requirements and influence investments.29

The National CISR R&D Plan priority areas are:

- Developing an understanding of critical infrastructure systems and their dynamics;
- Developing an approach for integrated and scalable risk assessment and management;
- Developing integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure;

---

27 Texas Department of Information Resources (DIR). [https://dir.texas.gov/about-dir](https://dir.texas.gov/about-dir).
28 *Cyber risk and insurance for transportation infrastructure.* July 2019. Transport Policy, Volume 79.
• Implementing data sciences to create unified, integrated situation awareness and to understand consequences of action; and
• Developing a culture of collaboration for CISR R&D.

The National Plan\textsuperscript{17} recognizes the overall important role of the academic and research communities in creating critical infrastructure security and resilience by in general:

• Establishing centers of excellence (e.g., university-based partnerships or federally funded R&D centers) to provide independent analysis;
• Supporting the research, development, testing, evaluation, and deployment of technologies;
• Supporting development and implementation of concepts, architectures, and technical strategies associated with critical infrastructure;
• Analyzing, developing, and sharing best practices related to critical infrastructure prioritization, security, and resilience efforts;
• Researching the behavioral aspects of terrorism and criminal activity;
• Preparing or disseminating guidelines and descriptions of best practices for physical and cyber security;
• Developing and providing all-hazards risk analysis and risk management courses;
• Establishing undergraduate and graduate curricula and degree programs;
• Conducting research to identify new technologies and analytical methods;
• Participating in the review and validation of risk analysis and management approaches; and
• Engaging and serving as a resource to local communities for efforts to enhance the security and resilience of physical and cyber critical infrastructure.

NCHRP 03-127, \textit{Cybersecurity of Traffic Management Systems}, states that cybersecurity efforts by state and local agencies is an area for future research. Documentation of programs, ongoing research, or any implemented frameworks is needed.\textsuperscript{30}

In 2019 the TRB Executive Committee published \textit{Critical Issues in Transportation 2019}, identifying several questions for the next 10 to 20 years that need to be addressed during the next 5 to 10 years through research. Several topics mention cybersecurity and cyber resilience and the need to identify vulnerabilities and how to overcome or manage them. Topics include:

• Automated vehicles, vessels, and aircraft and smart infrastructure are vulnerable in ways that failure would threaten public safety and confidence. Systems for managing vehicle flow and data with personal information are a concern.
• GPS is integrated through all transportation modes for guidance and navigation. A national or regional backup is needed should GPS systems fail.
• Trip data ownership needs to be determined as well as how to manage the volume of data, how to protect personal privacy, how to protect proprietary information, and how to best share data with transportation providers.

Mileage-based user fees data would need privacy protection to gain public and political acceptance before becoming an acceptable approach to funding highway infrastructure.3

USDOT’s Intelligence Transportation Systems (ITS) Joint Program Office (JPO) develops and coordinates multimodal projects central to cybersecurity research. The JPO has four strategies as its path forward for industry, government, and academia:

- Adapt and implement protective measures to reduce risk preferentially,
- Assess and monitor risk,
- Manage incidents, and
- Create an organizational culture of security.31

The 2021 Transportation System Resilience: Research Roadmap and White Papers looks at knowledge gaps within the American Association of State Highway and Transportation Officials and state DOTs and recommends a five-year research plan to guide efforts. Research needs that relate to cyber and transportation system management are:

- Cyber Risk Transfer Strategies. Exploring elements of cyber resilience when IT is outsourced.
- Maintaining Resilience in a Multi-modal Transportation System. Understanding the interdependencies between transportation modes and other critical infrastructure.
- Assessing Resilience Frameworks. Collecting and analyzing frameworks and developing tools and guidance for transportation agencies to help them select what to use.
- Assessing the Resilience of GPS-Based Applications in Transportation. Documenting transportation vulnerabilities to GPS failure.
- Deploying the NIST Cybersecurity Framework in State DOTs. Taking the NIST framework and adapting it to specific needs for state DOTs.4

Standing committees for TRB are formed with the purpose of identifying research needs as well as providing information to the transportation community. TRB has several standing committees related to cyber issues in transportation systems, including:

- Emerging Technology Law;
- Critical Transportation Infrastructure Protection;
- Systems, Enterprise, and Cyber Resilience;
- Aviation Safety, Security, and Emergency Management;
- Aviation Security and Emergency Management;
- Cybersecurity of Traffic Signals and Related ITS Equipment;
- Protection of Transportation Infrastructure from Cyber Attacks;
- Targeted Guidance and Information Support to State DOT CEOs on Cybersecurity Issues and Protection Strategies;

• Cyber Security in Transit Systems;
• Transit Safety and Security;
• Logistics of Disaster Response and Business Continuity; and
• Transformational Technologies in Transportation.\textsuperscript{32}

USDOT’s ITS Program has several research initiatives recently completed or in progress titled:

• Infrastructure Cybersecurity. Research efforts focusing on strategies and technology options to protect against threats and vulnerabilities to our nation’s roadside equipment, devices, and systems.
• Security Credential Management Systems. Tool developed for secure connected vehicle communication.

\textbf{Where are there noticeable gaps?}

\textbf{There is a gap in the workforce.} Control systems are the responsibility of the transportation engineer or operator; cybersecurity is often the responsibility of the IT personnel. Communication and teamwork between the two roles is critical. There is an increasing need to overlap and have transportation cyber specialist.\textsuperscript{34} Very few transportation agencies have the knowledge and skills to respond to the potential variety of cyber attacks.\textsuperscript{5} It is important to understand agency ability and when outside help is needed.

\textsuperscript{33} ITS Cybersecurity Research Program. U.S. Department of Transportation. Intelligent Transportation Systems Joint Program Office (ITS JPO) \url{https://its.dot.gov/research_areas/cybersecurity/research.htm}.
Transportation agencies can consult the DHS Cybersecurity Workforce Development Toolkit for guidance about preparing, planning, building, and advancing cyber security staff.\textsuperscript{34}

There is a gap in knowledge between the current best practices to protect IT systems and the threat of tomorrow’s attackers. The Committee on Improving Cybersecurity Research in the United States was established by the National Research Council of the National Academies with the financial support of National Science Foundation, Defense Advanced Research Projects Agency, NIST, DHS, the National Academy of Engineering, and F. Thomas and Bonnie Berger Leighton. The basic premise underlying the committee’s task is to produce a research agenda. Their report, Toward a Safer and More Secure Cyberspace, states that closing this gap of knowledge will require traditional and unorthodox approaches to research.\textsuperscript{6}

Another issue will be a continuous need to improve security and resiliency. Cyber technologies are always growing and evolving, and it is difficult to stay a step ahead; IT and OT require active evaluation and maintenance to reduce cyber risk and the impact of inevitable incidents.\textsuperscript{5}

There is a gap between the knowledge of transportation system resilience and security and how state DOT officials and regional transportation planning organizations can make a business case for investing in resilience strategies and communicate the importance to the public and stakeholders. The objective of NCHRP 20-127, active and scheduled for completion in 2022, is to develop a resource to help state DOTs and other transportation organizations explain the value of investing in resilience throughout the life cycle of planning, engineering, design, operations, construction, and maintenance.\textsuperscript{36}

The joint Surface Transportation Systems R&D working group is the primary means of identifying capability gaps in the surface mode. The identified capability gaps are a basis for developing the R&D project requirements that the funding organization (e.g., DHS Office of Science and


Technology [S&T], TSA, or USDOT) will consider. S&T conducts and supports research of advanced cybersecurity technologies to secure the nation’s current and future cyber and critical infrastructures.

**CONCLUSION**

Cyber issues are dynamic and increasingly more integrated as transportation technology and communication rapidly grows.

Transportation systems need to prepare their security for IT and OT devices to minimize cyber vulnerabilities, defend against attacks, and plan for when cyber-attacks happen to ensure their resiliency. There are many resources and available tools for transportation providers to address cyber risk; however, there are also remaining knowledge gaps. The research needs for cybersecurity and cyber resilience as related to transportation systems will continue to grow as cyber elements in transportation accelerate.

It is important for transportation agencies to identify their current cyber posture, prioritize areas for improvement, and progress towards a more secure and resilient transportation system.

**ACKNOWLEDGMENTS**

The author gratefully acknowledges the TTI researchers that contributed their time with participation in interviews: Kevin Balke, David Bierling, Jolanda Prozzi, Jim Kruse, Swapnil Samant, and Shawn Turner. Additional TTI researchers that contributed their time and feedback: Ginger Goodin, Bill Stockton, Greg Winfree, Mike Vickich, Srini Sunkari, David Sweeney, Karen Dixon, Joe Zietsman, Matt Miller, and Jim Cline.

---