STATEMENT OF

SHAILEN P. BHATT

PRESIDENT AND CEO

INTELLIGENT TRANSPORTATION SOCIETY OF AMERICA

ON

“ADDRESSING CYBERSECURITY VULNERABILITIES

FACING OUR NATION’S PHYSICAL INFRASTRUCTURE”

SUBMITTED TO THE

UNITED STATES SENATE

COMMITTEE ON ENVIRONMENT AND PUBLIC WORKS

JULY 21, 2021

Chairman Carper, Ranking Member Capito, and Members of the Committee on Environment and Public Works, thank you for the opportunity to provide the Intelligent Transportation Society of America's (ITS America) perspective on "Addressing Cybersecurity Vulnerabilities Facing Our Nation's Physical Infrastructure."

My name is Shailen P. Bhatt, and I am the President and CEO of the Intelligent Transportation Society of America (ITS America). I am honored to be here today – I appreciate the opportunity to talk about addressing cybersecurity vulnerabilities related to road and bridge infrastructure.

Before becoming ITS America's President and CEO in 2018, I served as Executive Director for the Colorado Department of Transportation. During that time, I also served as the national Chair of the Vehicle-to-Infrastructure Deployment Coalition and the Chair of the National Operations Center of Excellence. Before the Colorado Department of Transportation, I served as Cabinet Secretary with the Delaware Department of Transportation and Deputy Executive Director of the Kentucky Transportation Cabinet. I also served as an Associate Administrator at the Federal Highway Administration under U.S. Department of Transportation Secretary Ray H. LaHood.

ABOUT ITS AMERICA

ITS America is the nation's leading advocate for the technological modernization of our transportation system by focusing on advancing research and deployment of intelligent transportation technology.[1] Founded as an official advisory board on road technology to the U.S. Department of Transportation, ITS America represents state and city departments of transportation, transit agencies, metropolitan planning organizations, automotive manufacturers, technology companies, engineering firms, automotive suppliers, insurance companies, and research and academic universities.[2] Our members come to one table – ITS America – to shape the next generation of transportation and infrastructure driven by intelligent transportation technologies.

[1] Find out more information about ITS America here: https://itsa.org/

[2] The ITS America Board is represented by the following organizations: AAA, AECOM, Amazon Web Services, Arizona Department of Transportation, California PATH University of California Berkeley, California State Transportation Agency, Central Ohio Transit Authority, Cisco, Cubic, Econolite, Florida Department of Transportation, Ford Motor Company, General Motors, Google, PrePass Safety Alliance, HNTB, Iteris, Los Angeles Department of Transportation, MCity, Michael Baker International, Michelin, Michigan Department of Transportation, National Renewable Energy Lab, New York City Department of Transportation, Panasonic North America, Qualcomm, San Francisco Bay Area Metropolitan Transportation Commission, San Francisco County Transportation Authority, State Farm Insurance, Texas Department of Transportation, Texas Transportation Institute, Toyota, Virginia Department of Transportation, and Washington State Department of Transportation

ITS America's mission is to advance the research, development, and deployment of intelligent transportation technologies and solutions to save lives, improve mobility, promote sustainability, expand equity, and increase efficiency and productivity. Our focus is policy that accelerates the deployment of seamless mobility technology, connected and automated vehicle technologies, and smart infrastructure; policy that breathes new life into our transportation system by expanding investments in technologies that support smart communities; policy that encourages new models and modes of transportation, including micro-transit and Mobility on Demand, including ridesourcing, carshare, bikeshare, micro-mobility, and unmanned systems; and policy that does all of this while making our transportation system safer, greener, and smarter. Investments in these technologies should also address issues of transportation equity, so everyone gains access to mobility and opportunity, and the valid concerns of the transportation workforce.

As ITS America noted in our recently-released technology blueprint, enacting policies that deploy intelligent transportation technologies will ensure a safer, greener, smarter, and more equitable transportation system.[3]

My remarks will focus on three key areas.

- First, how intelligent transportation technologies have transformed transportation and are defining the way people, goods, services, and information move in the 21st century.
- Second, why cyber-attacks on transportation are a growing concern worldwide.
- Finally, much like Vision Zero, in regard to the national strategy to make our streets and physical infrastructure safer, ITS America calls on Congress and the Biden Administration to work with the United States Department of Transportation and other stakeholders to adopt a more robust national transportation cybersecurity strategy to make the digital layer of our transportation system safer.

INTRODUCTION

On behalf of ITS America members working to secure critical transportation assets, including road and bridge infrastructure, thank you for recognizing the growing risk and making cybersecurity explicitly eligible, for the first time, under federal highway formula programs in the Committee on Environment and Public Works approved Surface Transportation Reauthorization (STRA) Act of 2021.[4i]

[3] Find out more information about ITS here: https://www.transportation.gov/new-and-emerging-technologies

[4] STRA made cybersecurity explicitly eligible, for the first time, under the following federal highway formula programs: Sec. 1105. National Highway Performance Program. Makes eligible measures to protect

As vehicles and infrastructure become more connected, our nation's transportation system faces increasing cybersecurity risks. Given the ability to cause loss of life and inflict significant economic damage in a highly visible manner, cybersecurity attacks directed at those producing or operating technologies travelling over or connected to U.S. roadways will intensify. Infrastructure with Intelligent Transportation Systems (ITS) leverages modern communications systems to support transportation management and operations. As a result, intelligent transportation technologies no longer function as closed systems, thus exposing transportation facilities and infrastructure to cyber threats due to their connectivity.[5]

ITS support the U.S. economy and state and local economies by making our transportation system safer and more efficient. They allow U.S. cities to compete globally with cities in Asia and Europe in a technology-driven 21st century economy. But - we must manage the vulnerabilities that come with a more complex and connected transportation system. We need to stop thinking of cybersecurity as something to add to our infrastructure. We need to fully integrate cybersecurity as part of our infrastructure and make intelligent transportation systems secure by design.[6]

DEFINING THE WAY PEOPLE, GOODS, SERVICES, AND INFORMATION MOVE

For the past 100 years, road and bridge infrastructure has primarily consisted of individual, independent vehicles traveling on asphalt – in other words, cars and trucks moving on and over roads and bridges without the benefit of intelligent transportation technologies.

Twenty years ago, in addition to the tragic loss of life on 9/11, the attack was a wake-up call that focused our attention on the vulnerabilities of U.S. infrastructure. While I served as Deputy Executive Director of the Kentucky Transportation Cabinet in 2005, we had deployed CCTV and sensors to monitor roads and bridges. At that point, data was still largely siloed and fragmented, but over time these transportation data systems converged. Cybersecurity weaknesses in one system could jeopardize the safety of other systems in the converged data system. Shortly after that, connected vehicles communicating with the Internet, with transportation infrastructure, and with each other also created risks of those vehicles' systems being attacked by hackers trying to steal data, learn their locations, or take control of the vehicles' operations.

Around the same time, state and local transportation agencies began to introduce Information Technology (IT), including networked communications, and connect it to new and existing

segments of the National Highway System from cybersecurity threats. Sec. 1109. Surface Transportation Block Grant Program. Makes measures to protect a transportation facility otherwise eligible for assistance under this section from cybersecurity threats.

[5] Federal Highway Administration Office of Operations Guide on Transportation Management Center Information Technology Security, https://www.itskrs.its.dot.gov/sites/default/files/docs/fhwahop19059.pdf

[6] https://www.missionsecure.com/

Operational Technology (OT) such as traffic signals, cameras, and sensors. This created a new digital layer of road, bridge, and tunnel infrastructure overlaying their physical infrastructure. The state and local transportation agencies began to use real-time data and predictive analytics now available over their communication networks to operate their transportation systems with more precision, efficiency, and functionality, which led to safer roads. These agencies could respond to urgent events more quickly, change traffic signals in real time to reduce congestion, and even detect freezing and potentially dangerous road surfaces such as was done during and after my time in Colorado as executive director of the state's Department of Transportation.

Today we are on the cusp of digital transformation in transportation as dramatic as the period when the car supplanted the horse and buggy. The Internet of Things (IoT), autonomous and automated technologies, artificial intelligence and machine learning, electric vehicles, Mobility on Demand, advanced air mobility, and many other technologies have the potential to save lives, and make surface transportation safer, greener, smarter, and more equitable.

Let me give you an example of the critical role technology plays in supporting our economy. Think about a truck delivering freight from South Carolina's port of Charleston to West Virginia's capital city of Charleston. Traffic management software efficiently guides traffic movement, so the truck moves through the city traffic more efficiently. Automated enforcement allows inspections to happen at 30 miles per hour instead of the driver pulling over and remaining idle during the inspection. Smart truck parking helps the driver find a place to rest and maximizes their hours of service. Electronic devices log hours of service. GPS technology adjusts routing based on weather and traffic information.

It is important to speak about multi-purpose evolution when discussing technology – some things designed for singular purposes often produce additional applications. For example, with trucks, ITS America member WSP points out that electronic logging technology in the previous example also creates data that can be further analyzed and combined with vehicle sensors to flag unusual patterns or unexpected events for further security investigation or action. This is similar to how electronic toll collection data can also identify traffic congestion, an additional benefit realized through interconnected systems.

ITS is transforming how we maintain and build new roads and bridges by integrating technology into the infrastructure, including sensors and advanced monitoring systems that can track roadway and bridge conditions, which will alert state and local transportation agencies of any disruptions or extreme weather conditions.

An example of this is the Star City Bridge in West Virginia. The Star City Bridge is outfitted with more than 700 sensors that monitor measurements on the triaxial state of strains on the concrete, concrete crack initiation and growth, opening of joints at the bridge edges, steel girder bending/stresses, axial forces on the bracing members, and the angles and inclination of abutments. The bridge sensors also collect data on traffic weight, dynamic strain, temperature profiles of the bridge and climate data. West Virginia University, located near the bridge, uses the

bridge as a teaching tool, particularly in regard to the data on "deflection," the stresses placed on it at various locations and how loads, such as two trucks approaching each other from opposite directions, affect it.

The Indian River Inlet Bridge in Delaware is another example of a bridge instrumented with smart technology. It is equipped with 119 fiber optic sensors built into the pylons and support cables. The sensors measure stress on structural components, wind-related movement, and the penetration of road salt into the concrete. Each sensor has its own wavelength that will change due to stressors and alert the Delaware Department of Transportation, allowing it to make changes to traffic patterns or make targeted repairs to alleviate stress. This bridge was the first in the country to utilize this technology.

While advancements in technology have made the transportation system more connected than ever, this connectivity brings increased cyber risk – and these risks have the potential to threaten the system, the economy, and people's lives.

CYBER ATTACKS ON TRANSPORTATION

The nation's transportation assets and infrastructure are now as vulnerable to cyber threats as are other connected systems. Cybercriminals may have the opportunity to disrupt the American economy by targeting transportation systems and infrastructure due to these vulnerabilities.

U.S. Transportation Secretary Pete Buttigieg described the Colonial Pipeline attack as a "wake up call" that highlighted significant vulnerabilities in U.S. critical infrastructure. The Department of Homeland Security considers the Transportation Systems Sector to be one of 16 critical infrastructure sectors whose "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." The cybersecurity threat landscape is constantly evolving, and new vulnerabilities are discovered every day.[7]

Cyber threats are becoming increasingly sophisticated and target transportation's interconnected data systems, monitoring physical and digital networks. As cyber technology becomes more sophisticated, the threat from attack is moving from data breaches to interrupting physical critical infrastructure, exposing transportation operators to economic and reputational damage.[8] More important than these harms or damage to infrastructure is the potential harm to the nation's

[7] Federal Highway Administration Office of Operations Guide on Transportation Management Center Information Technology Security, https://www.itskrs.its.dot.gov/sites/default/files/docs/fhwahop19059.pdf
[8] https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20in%20the%20Transportation%20Industry-03-2015.pdf

transportation system. The figure here illustrates common cyber incidents within the transportation sector.

According to ITS America member Mission Secure, in the last three years alone, the United States has seen a 900 percent increase in attacks focused on Operational Technology used in traffic management signaling systems. ITS America member Southwest Research Institute (SwRI) notes that phishing emails, malware, and Denial-of-Service, as well as ransomware, are some publicly known and heavily used cyberattacks against state and local transportation agencies. Compromised Dynamic Message signs displaying various messages (e.g., "Zombies Ahead," "Hacked by Sun Hacker") have targeted state transportation agencies. As state and local transportation agencies migrate systems to the cloud, more vigilance is needed. More prevalent cloud attacks include stolen credentials, typically via phishing, exploitation of cloud misconfigurations, and vulnerable cloud application hacking.

ITS America member AECOM notes that the use of GPS to adjust routing based on weather and traffic information might have an associated threat of being spoofed via a cyberattack. If a related vulnerability were successfully exploited, a simple denial of service attack could be performed on a wide scale, causing delays to shipments and traffic flow on the highway. This could also be used as a targeted means of causing valuable freight to be re-routed to a specific road where police protection, traffic volume, and CCTV camera coverage are not as prevalent as on the main route. Sensors and monitoring systems on roads and bridges could be susceptible to similar attacks, with a malicious actor intentionally hiding the fact that a structural problem exists. Other vectors of attack could be the interception of transmitted sensor information (e.g., if weak or no encryption existed) or having stored diagnostic data leaked from compromised monitoring system databases. In the worst case, if not properly secured, this sort of information could get into the hands of a

malicious actor who is actively planning physical attacks on U.S. infrastructure and assessing potential targets.

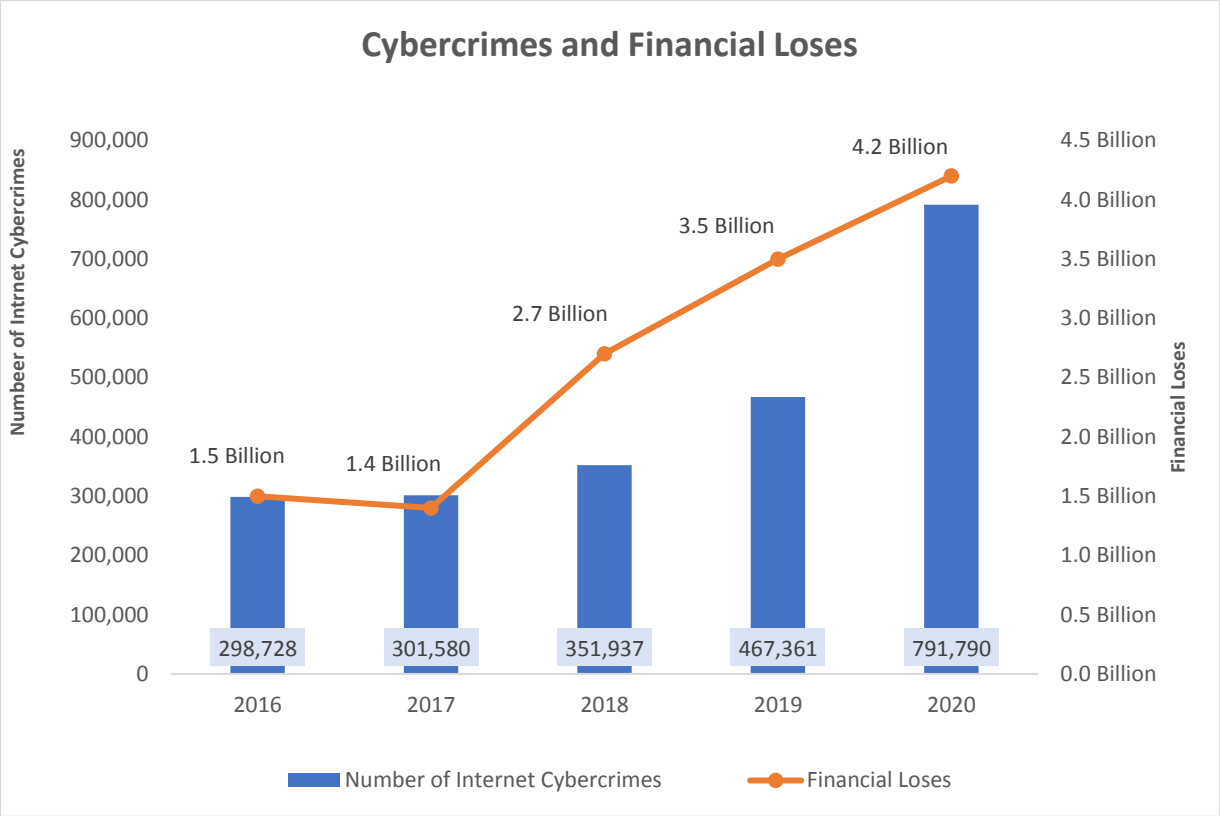
The number of attacks made on public and private organizations is growing at an alarming rate and becoming more sophisticated, notes ITS America member C. Douglass Couto, Senior Fellow, Center for Digital Government, and chair of the Transportation Research Board Cybersecurity Subcommittee. There are estimates in the millions per day. "We can defend against them day after day, but it only takes one vulnerability exploited to create havoc. The use of artificial intelligence thwarts these attacks," notes Couto. Investments in research to identify the next generation of cyber tools to defend against attacks is critical. The word cloud below from Couto illustrates the numerous cybersecurity concerns for transportation agencies and government leaders at all levels.

The COVID-19 public health emergency forced many organizations, including state and local transportation agencies, to rely more heavily on technology as people worked from home. More

than a third of U.S. households reported working from home more frequently than before the pandemic.[9]

Based on a report released by the Palo Alto Networks threat intelligence team Unit 42, organizations expanded their cloud workload deployments following the onset of the pandemic, but they also saw more cloud security incidents. Such incidents in the retail, manufacturing, and government industries rose by 402%, 230%, and 205%, respectively. These industries were among those facing the greatest pressures to adapt and scale in the face of the pandemic – retailers for basic necessities and manufacturing and government for COVID-19 supplies and aid.[10]

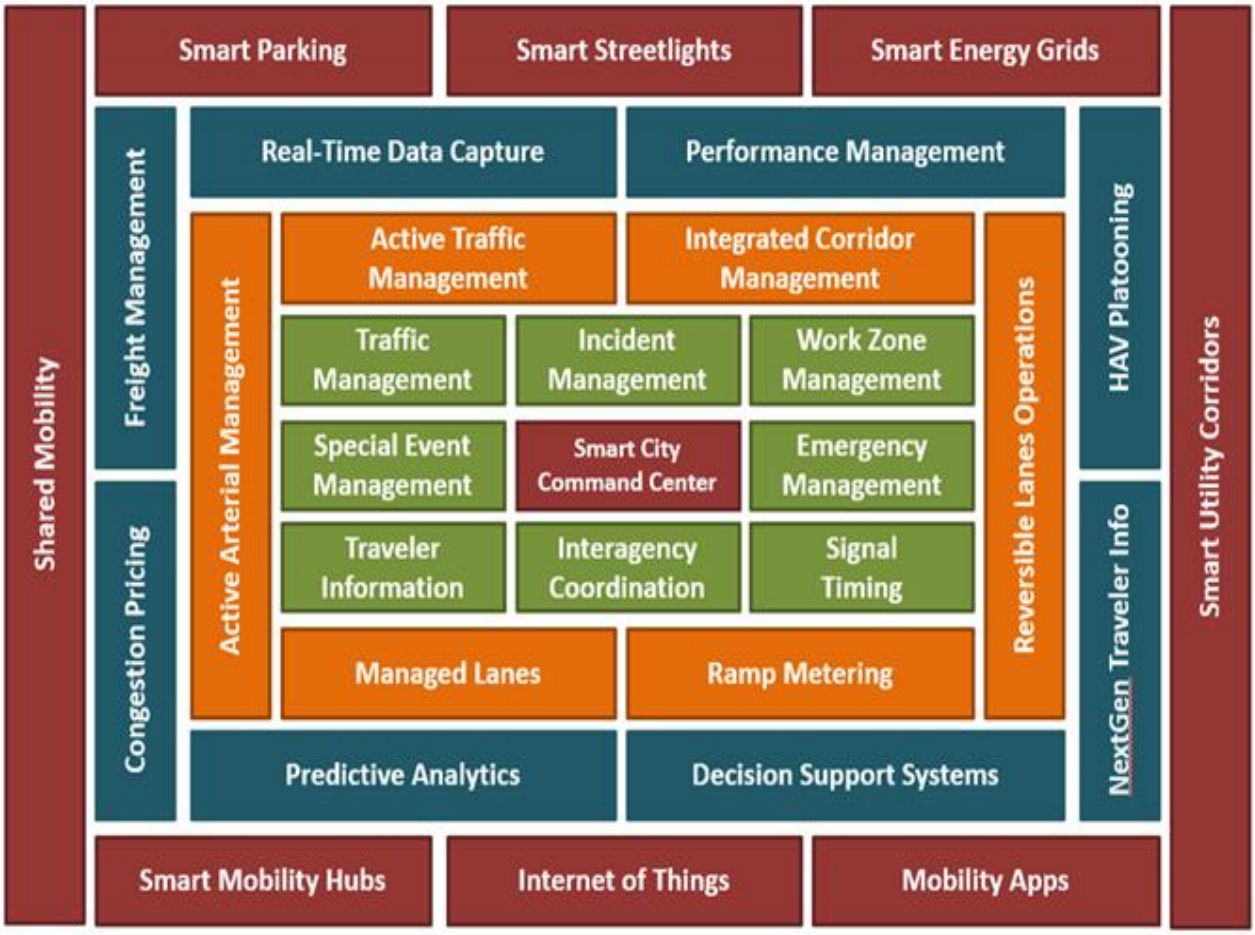
The chart below, based on the FBI 2020 Internet Crime Report data, illustrates a record number of cyber incidents in 2020 exceeding $4.1 billion in financial losses, which represents a 69% increase from 2019.



The following chart from AECOM illustrates all the functions and interfaces that need to be secured to protect transportation, and its users, from cyber threats. To reduce transportation's susceptibility to cyber threats, the transportation sector needs to ensure security not just for each

[9] https://www.census.gov/library/stories/2021/03/working-from-home-during-the-pandemic.html
[10] https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research-1h21 Find out more information about how malicious cyber actors have exploited the COVID-19 here: https://us-cert.cisa.gov/ncas/alerts/aa20-099a

of these boxes on their own, but also interconnectedly for when these functions interface with each other or interface with a command center.



According to Mission Secure, the increasing prevalence of connected, autonomous, and automated assets in our systems further exacerbates this problem. For example, connected and autonomous vehicles will increasingly rely on real-time, accurate data from traffic controllers, interacting directly with the entire traffic system. Any potential compromise to the car or controller would have adverse impacts on safety.

ITS America member Texas Department of Transportation points to an integrated city in the not so distant future in which automated and autonomous vehicles, including Personal Delivery Devices (PDDs), connected bikes and scooters, and other systems not yet developed will be operating in the same areas – sidewalks, bike paths, roads, intersections. Directly above them will be drones delivering packages, and potentially people, along managed low-level air corridors. Future urban traffic management will incorporate all these elements and it is critial that the entire system integrates strong cybersecurity systems.

Intelligent transportation technologies are making our country safer and more efficient - by moving people, data, and freight, they support the U.S. economy. We must, however, manage the vulnerabilities that come with a more complex system by meeting cybersecurity benchmarks that

increase adoption of security best practices, including by employing a zero-trust security model, accelerating movement to secure cloud services, and consistently deploying foundational security tools such as multifactor authentication and encryption.[11] Outdated security models and unencrypted data have led to compromises of transportation assets and infrastructure. Any potential vulnerability could have adverse impacts on safety.

Just as we have underinvested in roads, bridges, and tunnels over the last two decades, the same is true for cybersecurity – we have not made the investments necessary to protect our transportation system. Developing a resilient system begins with cybersecurity. As a former DOT director for two states, I am well acquainted with making tough choices about spending scarce resources. State and local transportation agencies must analyze their systems to identify where the greatest risks and weaknesses exist. A risk management plan is used to determine courses of action to mitigate and manage those risks.[12] The transportation sector needs to secure network infrastructure devices[13] and enforce domain security.[14]

ITS America member Michigan Department of Transportation (MDOT) notes that cybersecurity crosses several governmental jurisdictions and can be justified as part of several department missions. These include state and local DOT's, law enforcement, and others such as the National Guard or anti-terrorism agencies. When these agencies work together, it is important that new cyber vulnerabilities are not created by lack of coordination.

MDOT also notes that cybersecurity for transportation interests and providers is more challenging because the consequences are public and immediately affect people regardless of whether they are connected to a system, business, or process. A hospital under a ransom attack is threatened, but that threat does not affect people who are not connected in some way. An attack on a bank concerns people with savings there, but not necessarily the general public. An attack on an ITS roadside network access point can affect the personal safety of nearby pedestrians and all vehicles and their passengers communicating with that network.

[11] https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/
[12] Federal Highway Administration Office of Operations Guide on Transportation Management Center Information Technology Security, https://www.itskrs.its.dot.gov/sites/default/files/docs/fhwahop19059.pdf
[13] https://us-cert.cisa.gov/ncas/tips/ST18-001
[14] https://www.circleid.com/posts/20210709-domains-a-critical-component-of-your-enterprise-risk-management/

A NATIONAL TRANSPORTATION CYBERSECURITY STRATEGY

ITS America and our members, in particular the New York City Department of Transportation, recommend a more robust national transportation cybersecurity strategy to make the digital layer of our transportation system safer, much like how Vision Zero strategies in New York City and elsewhere have saved lives and prevented serious injuries through engineering, education, and enforcement to make our streets and physical infrastructure safer.

Commercial aviation has long embraced a safe systems approach, and since 1997, the risk of a fatal crash has fallen 95 percent. In fact, in 2017, there were no passenger jet crash fatalities anywhere in the world – a previously unimaginable achievement. The same principles, applied to road traffic and focused on data-driven policy, have the potential to significantly reduce the burden in death, disability, and property damage from crashes in the United States

A more robust national transportation cybersecurity strategy should see all cyber attacks as defendable, provided we make the necessary investments before they occur. The strategy should include risk assessment, network security controls, and updated Information Technology – Operational Technology cyber-physical systems.

Adopting a national strategy can be achieved by ensuring that state and local transportation agencies and other transportation bodies adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework for cyber risk management and the Center for Internet Security (CIS) Critical Security Controls to improve their network cyber defenses as recommended in the Federal Highway Administration's Transportation Management Center Information Technology Security Final Report, September 2019. Specifically, we call on the federal governement to:

1. Provide state and local transportation agencies or other bodies funding at up to a 100% federal share, technical assistance, and best practices to modernize intelligent transportation systems, so they can adopt the NIST Cybersecurity Framework for risk management, CIS Critical Security Controls to improve network security, and upgrade or replace IT-OT cyber-physical devices and systems;

2. Establish a Department of Transportation grant program to provide grants to rural transportation agencies and areas of persistent poverty or income inequality to modernize intelligent transportation systems and adopt the NIST Cybersecurity Framework and CIS Critical Security Controls;

3. Reimburse state and local transportation agencies or other bodies that have been proactive and used state, local, or other funding sources to modernize intelligent transportation systems and improve cyber defenses according to the NIST Cybersecurity Framework for risk management and CIS Critical Security Controls; and

4. Allow flexibility in how transportation funds are used to invest in future cybersecurity workforce capacity. We see marked improvements in threat reduction when agencies hire full-time staff to manage their cybersecurity programs. However, there is a skyrocketing demand for cybersecurity-trained people making it harder to hire these skills across all sectors of our economy, including transportation.

Thank you again for the opportunity to testify today. I look forward to answering any questions you may have.

***

ITS America acknowledges the contributions of members AECOM, C. Douglass Couto, HNTB, New York City Department of Transportation, Michigan Department of Transportation, Mission Secure, Southwest Research Institute, Texas Department of Transportation, and WSP.

Please email ITS America's Vice President of Public Policy and Legislative Affairs Ron Thaniel at rthaniel@itsa.org with testimony questions or comments.

---

[i] **ITS America's FAST Act Reauthorization Platform Moving People, Data, Freight: Safer. Greener. Smarter. Cybersecurity Policy**

1. POLICY: SAFEGUARD CRITICAL TRANSPORTATION INFRASTRUCTURE FROM CYBERSECURITY THREATS

As vehicles and infrastructure become more connected, our nation's transportation system faces increasing cybersecurity risks. Given the ability to cause loss of life and inflict significant economic damage in a highly visible manner, cybersecurity attacks directed at those producing or operating technologies travelling over or connected to U.S. roadways will intensify.

ITS America Recommendation

- Support policy that would provide states and localities funding and technical assistance to safeguard critical transportation systems that are more reliant than ever on connectivity to communicate and exchange data from cybersecurity threats.
- Amend 23 U.S. Code § 119 National Highway Performance Program, 133 Surface Transportation Block Grant, 167 National Highway Freight Program, and 148 Highway Safety Improvement Program to explicitly authorize that funds made available may be used to implement measures to protect highways, roads, bridges, and tunnels against cybersecurity threats to transportation infrastructure by allowing system access only as authorized and preventing malicious activity.
- Amend 49 USC Chapter 53 of Subtitle III Public Transit to protect public transportation systems from cybersecurity threats – Amend § 5302 definitions to explicitly include measures to protect against cybersecurity threats under the definition of Capital Project to allow system access only as authorized and prevent malicious activity.

- Amend 23 USC § 503(c)(4)(E) Advanced Transportation and Congestion Management Technologies Deployment Program to explicitly include measures to protect against cybersecurity threats as an eligible use of grants.
- Explicitly provide funding for risk assessments and planning services; developing best practices supporting cyber protection of legacy infrastructure, software and hardware solutions; implementing active and predictive threat monitoring services; deploying continuous monitoring and attack mitigation cyber security technologies and devices to harden traffic management systems and operations centers, creating Security Operations Centers (SOCs); and providing cybersecurity training to cybersecurity staff and other staff.
- Eligible activities include operating Intelligent Transportation System networks (ITS Networks) that enable infrastructure owner-operators to actively manage and protect transportation system such as secure traffic signal and sensor networks; secure wireless, wired, and fiber-optic networks; toll lane devices and systems; secure devices and systems to provide reliable and authoritative traveler information (VMS, websites, handheld device applications, in-vehicle information systems, etc.); active traffic management systems (lane use signals, variable speed limits); camera networks; weather-incident management systems; rock fall, flood, and avalanche detection systems; seismic detection systems; connected vehicle systems (Vehicle-to-Everything: infrastructure, other vehicles, people, cyclists, etc.); and Security Credential Management System (SCMS) that ensures connected vehicle technologies operate in a safe, secure, and privacy-protective manner.