Information on Current and Future States of Cybersecurity in the Digital Economy

Request for Information / FHWA Response

The following questions cover the major areas about which the Commission seeks comment. They are not intended to limit the topics that may be addressed. Responses may include information related to or recommendations for other areas the Commission should consider.

For each topic area, the Commission solicits information on current and future challenges, promising and innovative approaches to address those challenges, recommendations, and references to inform the work of the Commission. The Commission is specifically seeking input on the topic areas below:

Topic Area Challenges and Approaches	1. Current and future trends and challenges in the selected topic area:
Critical Infrastructure Cybersecurity	Intelligent Transportation System (ITS), traffic management systems, and traffic operations centers have become more dependent on the internet. More ITS, transportation management systems, and the imminent deployment of connected vehicles are increasingly connected to the internet, interconnected to new devices, between information technology systems and networks, online services, and transportation operations partner agencies. There is now a heightened risk of cyber attacks and intrusion to the States Department of Transportation (DOT) ITS and transportation management systems. Unexpected cyber attacks has the potential to cause serious traffic disruption and can potentially diminish the trust of the ITS and traffic management system services to the motoring public. ITS and traffic management systems historically have not been adequately secure to withstand cyber security attacks.
Cybersecurity Insurance	N/A. (Most of highway transportation system are owned and operated by state agencies, local public organizations, or Public Private Partnership authorities.)
Cybersecurity Research and Development	N/A. (As part of the ongoing Connected Vehicle program, the Federal Highway Administration (FHWA) has been conducting research and development on this topic. No final guidance, standards or policies have been issued regarding cybersecurity.)
Cybersecurity Workforce	The States DOT has not implemented a comprehensive cyber security awareness program for their staffs. They need to promote a culture within their ITS Programs to visibly support and champion cyber security awareness. The States DOT Commissioner, Transportation Systems Management and Operations (TSM&O) Managers, ITS Engineers, and traffic operations operators will eventually face an increased level of complexity in managing the security of their ITS infrastructure and traffic management systems and preventing cyber security attacks that will surely increase in sophistication if a cyber security awareness program is not developed and implemented. The skill sets for cyber security tend to focus on the IT Enterprise core competency. It is not reflected in the skill sets of the States DOT ITS and traffic operation staffs specific to Industrial Control Systems (ICS). A TSM&O workforce development training opportunities

	specializing in transportation system cyber security needs to be tailored for States DOT traffic operations and ITS staffs.
Federal Governance	Internally, FHWA staff are require to take webinar training on cybersecurity awareness on computer access, safe guarding, and securing electronic information (the IT Enterprise-side). Recent NIST's Framework on CS has provided a great framework for commerce and industry but fall short on addressing CS on Highway Transportation. Due to financial and technical challenges, most state transportation agencies rely on guidance and standards issued by the federal government.
Identity and Access Management	
International Markets	Collaboration with international governments and agencies would help prevent and defend cybercrime.
Internet of Things	As more state and federal agencies start using cloud-based transportation management services, securing the internet from cyber-attack/incident will be very challenging for traffic operations and highway safety.
Public Awareness and Education	FHWA has been strong advocate and brought awareness to transportation cybersecurity via inter-agencies meetings, training, and forums. We have subcommittee working on topics of cybersecurity for presentation and best practice sharing experiences at the annual Transportation Research Board (TRB) Meeting.
State and Local Government Cybersecurity	FHWA provided technical and financial support to state and local governments via Federal Aid Highway Program.

Topic Area Challenges and Approaches	2. Progress being made to address the challenges:
Critical Infrastructure Cybersecurity	States DOT can take an initial step (starting point) to protect their ITS infrastructure and traffic management systems by utilizing their States Dept. of IT information security policies, procedures, and documented best practices to applied completely and effectively protect their ITS system environment.
Cybersecurity Insurance	
Cybersecurity Research and Development	
Cybersecurity Workforce	
Federal Governance	

Identity and Access Management	
International Markets	
Internet of Things	
Public Awareness and Education	
State and Local Government Cybersecurity	States DOTs should utilize the NIST Cybersecurity Framework to adopt existing cyber security standards and best practices. By implementing a set of cyber security best practices that allows for a broader range of controls, the States DOT will elevate the importance of cyber security risk management within their Department and ensuring they meet applicable federal regulatory compliance.

Topic Area Challenges and Approaches	3. The most promising approaches to addressing the challenges:
Critical Infrastructure Cybersecurity	
Cybersecurity Insurance	
Cybersecurity Research and Development	
Cybersecurity Workforce	
Federal Governance	
Identity and Access Management	
International Markets	
Internet of Things	

Public Awareness and Education	
State and Local Government Cybersecurity	

Topic Area Challenges and Approaches	4. What can or should be done now or within the next 1-2 years to better address the challenges:
Critical Infrastructure Cybersecurity	
Cybersecurity Insurance	
Cybersecurity Research and Development	
Cybersecurity Workforce	The role of the States DOT ITS Programs is to improve the day to day performance (safety and mobility) of the transportation system which includes managing unplanned incidents, identifying and mitigating incidents, managing the traffic signal operations, and managing and operating the ITS. Monitoring the performance of the ITS and traffic management systems for cyber attacks and cyber security is not considered a day to day operations activities. Duties of monitoring the performance of the ITS and traffic management systems for cyber attacks must be incorporated into the day to day duties of the ITS personnel and traffic operations centers operators.
Federal Governance	
Identity and Access Management	
International Markets	
Internet of Things	
Public Awareness and Education	
State and Local Government Cybersecurity	States DOT should perform a risk assessment and develop cyber security plans for their ITS and traffic management systems. A risk assessment provides an opportunity for the States DOT to currently assess their current cyber security state of practice, identified best practices, challenges, areas for improvement, and developing an action plan to address those deficiencies.

	States DOT can learn about IT security best practices to applied it to their ITS and traffic management systems. It will also save the States DOT in time and personnel resources to streamlined and incorporate those identified best practices within their standard operating procedures in the areas of ITS infrastructure and networking of ITS devices. Such as developing and implementing a new internet protocol (IP) address scheme for their ITS network to allow for seamless connectivity of the States DOT ITS ethernet network to the States Department of IT network for data sharing and traffic monitoring purposes. Conduct a cyber security audit to evaluate the States DOT ITS network ability to protect itself against common threats both external and internal to States DOT network. Used industry best practices from the Energy and Communication sectors to implement security measures on all devices in the traffic signal and ITS networks. As States DOT developed a Statewide TSM&O Plan or ITS Strategic Deployment Plan to sustain their TSM&O or ITS Programs, goals and objectives for transportation system cyber security should be articulated including describing the tactical activities to sustain the transportation cyber security program within their overall TSM&O or ITS Programs. Consider requiring cyber resilience as a review criterion for access to Federal Aid funds on transportation projects.

Topic Area Challenges and Approaches	5. What should be done over the next decade to better address the challenges:
Critical Infrastructure Cybersecurity	See item 2 in R&D
Cybersecurity Insurance	
Cybersecurity Research and Development	There is an opportunity for the States DOT to established an ITS Resource Center (i.e. funded with FHWA SP&R Federal aid funds) through a partnership and collaboration with the State's research institution/university to focus not only ITS research but also other emerging TSM&O areas and transportation system cyber security and training. Fundamental R&D in several areas will be critical and collaboration opportunities should be fully explored. These are cyber security industry wide issues and Federal participation can benefit from coordinated collaboration: 1 – Create a repeatable, technology agnostic, performance based cyber security metric 2 – Assess if and how Artificial Intelligence and Machine Learning technologies can help to improve security and resilience of legacy systems.
Cybersecurity Workforce	See item 2 in R&D

Federal Governance	
Identity and Access Management	
International Markets	
Internet of Things	
Public Awareness and Education	
State and Local Government Cybersecurity	See item 2 in R&D

Topic Area Challenges and Approaches	6. Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges:
Critical Infrastructure Cybersecurity	
Cybersecurity Insurance	
Cybersecurity Research and Development	
Cybersecurity Workforce	
Federal Governance	
Identity and Access Management	
International Markets	
Internet of Things	

Public Awareness and Education	
State and Local Government Cybersecurity	The States DOT must allocate the appropriate resources to identify, evaluate, and mitigate cyber risk for their ITS infrastructure and traffic management systems. For many without the cyber security knowledge and expertise, it may require the States DOT to utilize and procure professional/consulting service contracts in order to conduct network architecture reviews, security vulnerability assessments, penetration testing, and networking monitoring.