ITS AMERICA

ITS AMERICA'S CYBERSECURITY EXECUTIVE FORUM WRAP-UP: August 5, 2019

At ITS America's recent "Securing the Transportation Network" executive forum, cybersecurity experts from the public and private sectors convened to discuss the numerous challenges related to cyber threats facing transportation stakeholders. These high-level producers and managers of intelligent mobility technologies traveling over or connected to U.S. roadways met to discuss the adoption of a robust, layered approach to cybersecurity. This conversation centered on the best ways to mitigate cybersecurity risks to our nation's transportation system, which have grown as vehicles and infrastructure become more connected.

Participants highlighted the challenge of balancing the need for vigorous cybersecurity measures with inadequate dedicated funding and outlined a series of best practices to employ when managing cybersecurity. In talking about how to secure transportation resources, common themes emerged – prioritizing strategic decision-making, focusing on workforce development, and sharing successful cybersecurity practices. Some recommendations and highlights include:

· As vehicles and infrastructure become increasingly connected, the vulnerabilities facing our transportation network continue to grow. Users and operators must often defend against these vulnerabilities with limited funding, while ensuring their security posture does not become too rigorous for the transportation technology to function. Balancing these considerations requires critical classification of threats to a given transportation system based on likelihood and potential risk, allowing limited cybersecurity resources to be focused on the most threatening possibilities.

· These potential risks vary from one system and organization to another, so there is no "one size fits all" approach to cybersecurity. Stakeholders, however, can implement best practices to mitigate their exposure to risk. Before new security techniques can be executed, current vulnerabilities must be identified. Often, dated software contains exploitable vulnerabilities, as it would not be updated as frequently with security patches. The sunsetting of this old software in favor of more up-to-date technology can help support cybersecurity infrastructure, as it is very difficult to retrograde security.

· When developing new cybersecurity practices, ensure that security infrastructure is scalable and expandable. New cyber threats are constantly being developed, so the defenses must be forward compatible with future updates and adaptations. There is no silver bullet solution to security, but a proper cyber infrastructure can provide industry and agencies alike the ability to respond to emerging threats.

· After initial security measures are put in place, participants emphasized the importance of cyber hygiene to maintain readiness. They recommended using live-threat detection to be alerted to risks on a real-time basis. Additionally, even with software that has been previously secured, be wary of adding new programs that have not been checked for security vulnerabilities.

- One of the most pressing challenges articulated at this forum was the need for cyber workforce development in the public sector. Numerous participants expressed concern about the lack of cybersecurity-focused staff within public sector agencies, as private companies are often able to offer more lucrative positions to job-seekers with cybersecurity backgrounds. Many automakers, technology companies, and agencies, however, have developed programs to boost cybersecurity training. Panelists emphasized the importance of these programs, as well as programs where cybersecurity professionals mentor aspiring professionals. Participants also advised that ideally all staff working on potentially targeted systems should undergo a common cybersecurity proficiency certification, ensuring a basic standard of security literacy among users of connected systems.

While there is still much to be done to prepare for emerging cybersecurity threats to both public and private sector transportation stakeholders, the strategies discussed throughout the event offer a blueprint for increased readiness. Collaboration between industry and agency leaders through sharing these insights continues to be an effective tactic in securing our increasingly connected transportation network. ITS America is proud to host these important conversations and will continue working with our task force on this critical issue.