SAE NHTSA Vehicle Cybersecurity Workshop Remarks

Ann Carlson, NHTSA Acting Administrator

Tuesday, January 17, 2023

Washington, D.C.

AS PREPARED FOR DELIVERY

Good afternoon, and thank you for attending today’s SAE NHTSA Vehicle Cybersecurity Workshop. We’re glad you’re here. Marc LeDuc, thank you for that kind introduction.

SAE’s Government/Industry Meeting has been an important event on everyone’s calendar now for more than 30 years, because it brings us together to discuss policies, regulations, technology, and the future of transportation. And, every year since 2016, we have added a vehicle cybersecurity workshop, usually the day before the SAE Government/Industry Meetings. Today’s workshop is a product of the strong partnership between NHTSA and SAE International, and I’d like to thank them for their collaboration with us on this event.

I’d also like to recognize NHTSA’s staff for their efforts. They were instrumental in organizing today’s panels and will be presenting at several sessions throughout the week. I encourage you to attend if they aren’t already on your schedule.

Technology is evolving rapidly, changing how we live, work and drive. Vehicles are increasingly intricate and today, software and electronics control nearly every aspect of a modern vehicle. And they will only become more complex in the years to come.

That’s why cybersecurity needs to be a priority for everyone. We can never overstate the fact that a chain is only as strong as its weakest link, and no one in the chain should find comfort in thinking that cybersecurity is someone else’s responsibility. It should matter to everyone because an attack may put lives at risk.

The Biden-Harris Administration is prioritizing cybersecurity and has issued some principles to further the conversation. The fundamentals of the White House’s approach are incredibly relevant to everyone here today, and I’d like to touch on a few of them.

First, improving the cybersecurity of our critical infrastructure is essential. Vehicles play critical roles in transporting people and goods. We saw an example of that during the pandemic, where truck drivers kept our store shelves stocked. A successful attack exploiting vehicle software vulnerabilities could have very serious consequences that could impact safety as well as the smooth running of our everyday lives.

Second, we must ensure new infrastructure is smart and secure. After all, technology evolves daily, and so do cybersecurity threats. That is why our approach to improving the cybersecurity posture of newer vehicles must remain nimble and adaptive.

And as we ensure the cyber-resiliency of the newer fleet, we certainly cannot forget about the 275 million vehicles already on the road, with an average age of 12 years old. The management of existing vehicles presents a specific challenge as well, and one that needs to be a priority too.

Third, we must guard against ransomware attacks to protect Americans online. We've heard a lot in the news about recent ransomware attacks on businesses, municipalities, schools and hospitals. But ransomware attacks are also a threat for motor vehicles. Many of you participated in a recent CyberStorm exercise focusing on just this scenario. Locking people out of using their vehicles could have dire consequences for all, specifically for first responders, law enforcement, and other critical service providers.

Fourth, working with allies and partners to deliver a more secure cyberspace is critical. That's exactly why we're all here, and why NHTSA helped to stand up Auto-ISAC.

NHTSA collaborates with all stakeholders, including our international colleagues, to promote a culture of collaboration. Information sharing is vital to get ahead of cybersecurity risks and vulnerabilities.

And finally, building the nation's cyber workforce and strengthening cyber education is key. Having the right people with the right skills is vital to the nation's cybersecurity readiness.

This is one reason why NHTSA is collaborating with Auto-ISAC on the Automotive Cybersecurity Training, or ACT, program. I know many of you are participating in this pilot, and I thank you for doing your part. We are keenly interested in establishing robust curricula in vehicle cybersecurity and making those available to the broader stakeholder community.

These principles all have one thing in common – cybersecurity is everyone's responsibility.

NHTSA is committed to supporting you to establish a strong, resilient cybersecurity posture. We have an ongoing research project, Cybersecurity Characterization of Vehicle Electronics and Electrical Architectures, which will provide insight into the direction of cybersecurity and cyber resilience within the automotive industry. We are studying architectures on a cross-section of makes and models to better understand them, as well as how architectures are changing over time.

Last fall, NHTSA published an updated version of our Cybersecurity Best Practices for the Safety of Motor Vehicles.

This update is a substantive update to our 2016 guidance, and it was crafted after receiving extensive feedback from industry and other stakeholders. Our Federal Register notice provides a summary of the comments we received, as well as how we addressed them in the drafting process. We appreciate everyone's input and support for this important project. While this document is non-binding, it contains important guidance and tools for industry to apply to your work.

These best practices leverage research, industry best standards, and learning from the motor vehicle cybersecurity issues discovered by researchers over the past several years. They reflect NHTSA's continued cybersecurity research findings, including over-the-air updates, formal verification methods, and static code analysis.

In addition to general best practices on organizational processes, this document provides recommendations on education. It also considers aftermarket devices, serviceability, and contemporary technical approaches to securing vehicle systems.

This is for anyone involved in designing, developing, manufacturing, and assembling a vehicle and its electronic systems and software. Cybersecurity isn't the sole domain of OEMs – anyone involved in components and software has a role to play.

For example, one best practice is to "know the software you are using." This principle is the same across industries and components. This concept is known as the software bill of materials, or SBOM.

The Biden-Harris Administration recommends this principle to federal agencies, and it's included in our cybersecurity best practices for the same reason.

It's key to software security and supply chain risk management. Software bill of materials involves creating and maintaining a list of software components, as well as a log of version updates. This helps identify which components within a vehicle or system may have been affected when a new vulnerability is identified.

NHTSA recommends that manufacturers, including component and aftermarket manufacturers, use software bill of materials to strengthen cybersecurity. After all, a crisis is the worst time to find out you are unprepared, disorganized, or relying on outdated information. Preparation ensures a strong cyber defense.

I spoke earlier about the rapid evolution of vehicle technology. Perhaps nowhere is that more evident than in electrification.

Electric vehicles are claiming a larger share of the marketplace, and automakers recognize that the future is electric. I expect that the volatile gas prices we saw last year, new investments and incentives contained in the Inflation Reduction Act, and major OEM investments will only increase the interest and demand for electric vehicles.

NHTSA has been researching the cybersecurity of battery management systems. Our ongoing EV study looks at cybersecurity and resiliency issues with different battery management systems and designs.

For example, there's movement toward wireless battery management systems, which would reduce weight and improve fuel economy. However, these potentially add another attack vector or point of vulnerability. NHTSA is expanding our ongoing research on potential cybersecurity and resiliency issues to include wireless battery management systems.

We are also evaluating potential mitigation strategies and the resiliency of current systems in the face of a cybersecurity attack. We look forward to sharing our results with you when complete.

It should be noted that our research is limited to the cyber protections implemented on the vehicles themselves; the cybersecurity of EV charging infrastructure falls under the purview of the U.S. Department of Energy.

Cybersecurity may sound like a daunting task, but it need not be. Preparation can strengthen cybersecurity and help us all respond quickly should a vulnerability be identified. Just as this administration has prioritized cybersecurity, so should each and every one of you. A prepared organization is a resilient organization.

I encourage you to continue to engage with others to share best practices, alert each other to vulnerabilities, and conduct exercises. Please also seek out resources to help you, such as NHTSA's cybersecurity best practices and other research.

I also want to remind you that the Enhanced Safety of Vehicles conference that NHTSA co-organizes is right around the corner. This is the 27th ESV conference, and it will be held in April in Yokohama, Japan. We'll have a special panel discussion focused on vehicle cybersecurity, and we hope to see you there to continue the conversation.

Together, we can make a stronger, more secure, and safer future. Thank you so much for your time today and your interest in this incredibly important area of transportation safety.