Auto-ISAC Cybersecurity Summit Keynote

Ann Carlson, NHTSA Chief Counsel

Wednesday, September 07, 2022 |

Dearborn, Michigan

AS PREPARED FOR DELIVERY

I'm pleased to be with you in person for this sixth-annual Auto-ISAC Cybersecurity Summit.

Events like these don't come together on their own. This summit is the result of many people's hard work. Thank you for bringing us together to discuss this critical topic. The Auto-ISAC Summit is a fixture on NHTSA's calendar, and several of our staff have made the trip to Dearborn to present and participate. I hope you'll attend their sessions.

I also want to take a moment to remember our former colleague, Art Carter, who passed away unexpectedly last week. While I did not have the pleasure to work with Art directly, I understand that many of you have, and you remember him fondly.

I know from our staff that Art was one of our experts who frequently tackled the most challenging problems during his long and decorated tenure at NHTSA. He took over as the vehicle cybersecurity research program lead in 2012, a role he carried out passionately until his well-deserved retirement a few years ago. I hope you'll keep his family in your thoughts as we carry on his cybersecurity legacy.

The collaboration and conversations you'll have over the next few days are why Auto-ISAC was created. NHTSA worked with the industry to stand up this organization because collaboration and information sharing are vital – and not an intuitive practice. After all, it's a competitive industry, and working with one's rivals doesn't come naturally. But, for all of our sakes – and to fulfill the responsibility we all have to protect the American public – it is critical that we work together to ensure cybersecurity is a priority every step of the way.

That is what Auto-ISAC was established to do, and what it continues to do every day.

NHTSA and Auto-ISAC have a history of close cooperation to advance cybersecurity. Today, one of the industry's challenges is training and developing an experienced, agile workforce.

NHTSA and Auto-ISAC have a cooperative agreement to develop a pilot training curriculum for vehicle cybersecurity professionals. We are all excited to see this pilot's results and learn how we can train the next generation of frontline cyber experts dedicated to keeping the traveling public safe.

Last year, NHTSA Administrator Steven Cliff offered a keynote at the Auto-ISAC Cybersecurity Summit, and I am honored to speak to you about our priorities and progress.

Speaking of leadership … this week is Administrator Cliff's last at the agency, and we're very sorry to see him leave.

I have served as NHTSA's Chief Counsel since January 2021, and starting next week, I will be NHTSA's Acting Administrator. It is an honor to be called to serve, and you have my word that our priorities and work will continue unabated.

As for those priorities, safety is always No. 1 at NHTSA. It's at the heart of everything we do.

We address safety in many ways – from vehicle design to vulnerable road users, public education to vehicle defects, risky driving behaviors to EMS and 9-1-1 services. And we address public health and energy security in the work we do on fuel economy standards. At the heart of our work is our focus on saving lives on our roads. Cybersecurity plays a vital role in that goal.

The theme of this year's summit is "Driving a Secure Future." It seems clear that a secure future is a safer future. Ensuring the public's trust in vehicle technologies is paramount to their adoption. As automation and innovation progress, the industry must stand ready to combat any cyber threats that could endanger the public. It only takes one attack to shatter confidence, trust, and safety.

NHTSA stands ready to help you in your quest to strengthen vehicle cybersecurity. I am pleased to share that today we published our updated Cybersecurity Best Practices for the Safety of Motor Vehicles.

These updated best practices will provide the industry with important tools to protect against cybersecurity risks.

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 voluntary standards, and learnings 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 also 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 in the sole domain of OEMs – anyone involved in components and software has a role to play.

Every single company, and every single person, is a link in a chain. We cannot be strong against cyber threats if there is a weak spot in that long chain.

Technology is evolving rapidly, changing how we live, work and drive. Vehicles are increasingly complex and, of course, vary by manufacturer. Today, software and electronics control nearly every aspect of a modern vehicle.

Since the 1970s, cars, trucks and SUVs have become arguably the most complex, software-driven products consumers own today. In June, we published a research report, "Foundations of Automotive Software," that explored how this technological complexity progressed exponentially.

We've heard the sayings … "Hundreds of millions of lines of code on a modern vehicle" and "software complexity that is orders of magnitude greater than those of a fighter jet."

These aren't myths, but facts of life now. And we all have to be prepared.

NHTSA also has 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.

Another area of rapid development is electrification. Electric vehicles are claiming a larger share of the marketplace, and automakers recognize that the future is electric. I expect the volatile gas prices we saw this 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. We are evaluating potential mitigation strategies, cyber design best practices, and the resiliency posture 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.

While the use of software and electronics raises cybersecurity concerns, technology also holds the promise to help prevent crashes and reduce the severity of the crashes that do occur. Virtually all new vehicles come with some advanced driver assistance technologies now. Lane-keeping assistance, automatic emergency braking and blind spot detection are just a few – these technologies are more common, and increasingly more complex.

We cannot afford a cyberattack or vulnerability to compromise the progress of safety technologies – or the public's trust in them.

Last month, NHTSA released our latest fatality data, our early estimates for the first quarter of 2022. And I'm sorry to report that the overall numbers are still moving in the wrong direction.

When everyday life came to a halt in March 2020, risky behaviors skyrocketed, and traffic fatalities spiked. We'd hoped these trends were limited to 2020, but sadly, they aren't.

We project that 9,560 people died in motor vehicle traffic crashes in the first quarter of this year. This is an increase of about 7% compared to the first quarter of last year, making this the highest number of first-quarter fatalities since 2002.

Because these are early estimates, we don't have specifics or causes yet. But we know it will take a combination of factors – including education, enforcement, vehicle design, and technology, along with improvements in infrastructure and designing safer streets– to turn the tide. The Bipartisan Infrastructure Law provides significant new resources to expand our efforts in all of these areas and we are hoping that these investments will turn the fatality curve back downward rapidly.

Technology can be part of the solution, but that technology must be safe and protected against cyber intrusions. Every one of you here today has a role to play in Driving a Secure Future. The stakes are incredibly high because lives are on the line.

I encourage you to continue to engage with others to share best practices, alert each other to vulnerabilities, and conduct exercises. Auto-ISAC facilitates this information sharing and cooperation, so please stay connected and continue communicating with each other.

I hope this summit will build new connections and lay the groundwork for a safer, more secure future. Thank you so much for your time today, for your commitment to strengthening vehicle cybersecurity, and for welcoming me to this important conference.