2021 Auto-ISAC Cybersecurity Summit Keynote Address

Dr. Steven Cliff, NHTSA Acting Administrator

Wednesday, October 13, 2021 |

Virtual

AS PREPARED FOR DELIVERY

Jenny (Gilger), thank you so much for that warm welcome; I'm so glad to be here with you today. Faye (Francy), thank you for the invitation and for your continued collaboration with NHTSA. I appreciate the opportunity to speak to you, and I know you've heard from some excellent speakers already. I'd like to recognize Congresswoman Debbie Dingell, who you heard from earlier today – she's a strong advocate in Congress for vehicle safety and American auto jobs.

While this is my first Auto-ISAC Cybersecurity Summit, NHTSA has long enjoyed a productive relationship with this organization. I look forward to working with all of you to further our shared safety mission, one that emphasizes the safety and security of vehicles on our roads. In fact, my very first speech during my first week at NHTSA was on cybersecurity, when I addressed the SAE-NHTSA cyber workshop back in February. And October is Cybersecurity Awareness Month, so I'm glad to be with you today to discuss this very important topic.

I'm pleased to announce that we've signed a new cooperative agreement with the Auto-ISAC, formalizing our mutual plan to pilot a new training curriculum specifically on vehicle cybersecurity. I know you've been working on this curriculum for a while now, so thanks, Faye and the Auto-ISAC leadership, for joining forces with us so we can take this to the next level. This partnership demonstrates our full agreement on the importance of preparing the workforce to respond to vehicle cybersecurity threats. I highly encourage all of you to participate in this pilot. It may be a lot of work, but I know it will be well worth your time and investment.

After all, vehicles are quite possibly the most complex items most people own. They're very software intensive, and more intricate than ever before. And while any system compromise is of concern, some malicious actions could lead to imminent and irreversible risks.

We must continue to work to strengthen cybersecurity protections on new vehicles – but we cannot forget about the 275 million registered vehicles already on our roads. They have substantial software components, but they're aging and perhaps weren't designed with cyber resiliency in mind.

The average age of a vehicle on our roads is more than 12 years old, which means its electronic architecture was likely designed 15 years ago. And 15 years? That's an eternity in the cyber world. That would be like still using the first iPhone, which was released 14 years ago. But while we would consider an original iPhone slow and a potential security risk, we don't think that way about an older vehicle. That's why it's so important not only to prioritize cybersecurity for new vehicles but to be sure vulnerabilities are appropriately addressed in older ones as well.

After all, lives are at stake.

Promoting safety motivates me every single day I come to work at NHTSA. I've had the privilege of serving as Acting Administrator since February, and to be part of the Biden-Harris Administration. While

many things change with a new administration, one thing that hasn't is our commitment to safety. Advancing safety is the top priority for the Department of Transportation, Secretary Buttigieg, and me.

At NHTSA, safety is literally our middle name, and we have been committed to it for more than 50 years. This is also true across USDOT, but it feels most urgent on our nation's roadways. Tens of thousands of traffic fatalities make up about 95 percent of all transportation-related deaths in this country, and that is unacceptable.

Over the next four years, you will see us committed to improving safety for all road users – not just drivers and passengers but pedestrians, cyclists, children, older Americans, and people with disabilities – by taking a safe system approach.

The safe system approach is people-focused, meaning that infrastructure serves the needs of its users, not the other way around. A small example is ensuring that there are cross walks at safe intervals to ensure that pedestrians can cross streets safely. A safe system approach incorporates the 5 Es: equity, engineering, education, enforcement, and emergency medical services. We must ensure everyone is working to make our transportation system safe for all its users.

And as we continue to move forward on a safe system approach, we will not forget the voices of those who use the roads, particularly those who are disproportionately harmed, including communities of color, underrepresented communities, and people with disabilities.

Technology will play an important role in this, but it can also introduce a point of potential weakness. President Biden has tasked federal agencies and the private sector with prioritizing cybersecurity, recognizing that doing so is critical to our nation's safety, security and economy.

In August, he signed Executive Order 14028, Improving the Nation's Cybersecurity, which I expect many of you are familiar with and are following. At the White House, he brought together private-sector leaders and challenged them to embrace cybersecurity.

As he told them, "You have the power, the capacity, and the responsibility, I believe, to raise the bar on cybersecurity."

And I believe the President's words are an appropriate challenge for everyone here today. 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 chain.

We're practicing this at the federal level by improving our communication and coordination with other federal agencies. You'll hear from some of these agencies during this summit, including the FBI, the National Institute of Standards and Technology, and the Cybersecurity and Infrastructure Security Agency.

I'd like to share a recent experience we had with a potential vehicle cybersecurity threat. In August, a supplier issued an announcement about vulnerabilities in early versions of their real-time operating system. That software was used in millions of vehicles from 2000 to 2015. CISA immediately sought NHTSA's insight to better understand the potential cybersecurity implications for the motor vehicle industry. Using our experience in risk management, we assessed the situation and made sure the vulnerability notifications and response plans were appropriate. This case is an example of how federal agencies can leverage each other's specialties to better protect the American public.

We're also conducting research to help us better understand risks and improve preparation. We're looking at how response strategies to known vulnerabilities can be improved, as well as how vehicle data can help identify cyber threats earlier. We also want to see what can be learned from other fields, such as the medical device industry, the power grid, and industrial control systems. And we recently tested cameras, lidar, and radar systems to learn more about the effects of interference and malicious attacks.

Electric vehicles are the way of the future, and we want to learn more about cybersecurity of battery management systems. Later this year, we'll be starting research on this, looking at resiliency issues with different battery management systems and designs. We will evaluate potential mitigation strategies, cyber design best practices, and the resiliency of systems in the face of a cybersecurity attack. We look forward to sharing our results with you when complete.

And finally, I know you are likely curious about the next steps on our vehicle cybersecurity best practices, which we have highlighted at previous Auto-ISAC conferences. Thank you to everyone for your robust feedback; our staff reviewed your comments thoughtfully. As you know, we cited the industry's work – the SAE/ISO standard – extensively in our best practices, and we are updating our citations to reflect the final document. So please, stay tuned – we will have details on the next steps soon.

In the meantime, 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.

It's all about managing risk. Software inherently presents cybersecurity risks. However, anticipating and managing those risks afford us the chance to prevent what could quickly become a crisis.

The stakes are incredibly high because lives are on the line. As more elements of the driving task become automated, a split-second interruption when a vehicle is in motion could be catastrophic. Just as we have prioritized the safety and performance of vehicle components, so must we prioritize cybersecurity as well.

As President Biden said, "You have the power, the capacity, and the responsibility."

Act like it's your loved one driving the vehicle in question – because it may very well be.

Thank you for your commitment to this important issue and for your support for our shared safety mission. Thank you for inviting me to speak to you today, and I send you my best for a successful, safe conference.