SAE/NHTSA Cybersecurity Workshop Remarks

Dr. Steven Cliff, NHTSA

Friday, February 5, 2021 |

Good morning, I'm Dr. Steve Cliff, and I'm happy to be here with you today. Thank you to SAE International for your continued partnership with us in organizing this important annual event and helping make it available to as many organizations as possible.

As you may know, I'm new to NHTSA – very new, in fact, since Tuesday was my first day! I'm very glad to be joining the great team at NHTSA and continuing to serve the American public.

I have been a public servant my entire career, first for 10 years as a scientist at the University of California, Davis. And for the past 12 years, I have served in various technical and leadership roles in California government – specifically at the California Air Resources Board, or CARB, and the California Department of Transportation, or Caltrans.

I'm coming to NHTSA from CARB, where I served as the Deputy Executive Officer overseeing numerous environmental vehicle regulations, including passenger vehicle emissions and medium- and heavy-duty engine emissions. I was also a member of the Transportation Research Board's Executive Committee.

My work has focused on reducing emissions from vehicles and engines and integrating electric vehicles into our nation's vehicle fleet. The vast majority of smog forming pollution, greenhouse gas, and carcinogenic diesel particulate matter emissions comes from these sources. These emissions disproportionately impact low income and communities of color. Improvements and innovations are thanks, in large part, to computer hardware and software – after all, vehicles today are more closely related to computers than the classic cars of the 1950s.

Because many advanced safety and efficiency features are driven by computers, automakers and suppliers need to emphasize the importance of cybersecurity in every step of the process and every component.

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. 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.

I encourage you to continue to engage with others to share best practices, alert each other to vulnerabilities, and conduct exercises. Events like this workshop promote stakeholder engagement and lay the groundwork for addressing complex problems. Stay connected and continue communicating with each other.

Our experts have some strategies on how you can help your organizations be better prepared for a potential cyber attack:

First, be proactive. If we try to solve an issue after the problem has surfaced, then we're too late. Everyone in your organization, starting with leadership, needs to be committed to this priority.

Second, measure risks and manage them effectively. As you know, today's vehicles are built with parts from a vast global supply chain, and each component and supplier is a potential vulnerability. Cybersecurity applies both to the assembled vehicle and to each separate component. Cybersecurity is a shared responsibility, and can only be as strong as the weakest link in the chain.

Next, prepare your organization. Your organization, employees, and processes should be trained, tested, and ready to manage cybersecurity for the full life cycle of the product – not just at the launch.

Then, establish and ensure accountability. There are no shortcuts to cybersecurity. Success requires constant re-evaluation and situational awareness, as well as setting metrics and evaluating your performance. Be ready to make updates and changes as necessary. In addition, collaborate openly outside your organization. I said this earlier and I believe it is worth repeating. Cybersecurity requires everyone to work together, although sharing information outside your company may feel foreign. But to meet the challenges and prioritize safety, the industry must stand united and collaborate as openly as possible.

Finally, and perhaps, most importantly: Build trust. Communicate openly, honestly, and clearly to the public. Public trust is essential to building acceptance and confidence in a new technology with life-saving potential. That trust must be earned, and it can be lost in a second. Show the public you are managing potential vulnerabilities, threats, and risks. And when an incident does occur – because it will – communicate directly and in a timely manner with the public so they know you are prioritizing their safety.

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

I'd like to leave you with that thought as we turn to the day's workshops. I have no doubt these experts will lead you in some very productive and thought-provoking discussions today. Please take advantage of this opportunity and ask our panelists some questions, take the surveys throughout the day, and share your opinions on the subjects at hand.

Again, I am honored to be leading NHTSA and look forward to meeting many of you in the near future. Thank you for your commitment to this important issue and for your support for our shared safety mission.