Auto-ISAC 2019 Summit

Keynote | James C. Owens, Acting Administrator

Wednesday, October 23, 2019 | Plano, Texas

As NHTSA's new Acting Administrator, I am deeply committed to our agency's safety mission. As the father of two young children, nothing is more important to me than the safety of everyone's families on our nation's roads.

Let me start by noting the three guiding principles that Secretary Chao has pursued since the beginning of this Administration. First, safety is our number one priority. Second, we need to preserve and improve our nation's transportation infrastructure. And third, we need to prepare for the future by developing rules and practices that accommodate innovation in a tech-neutral way, while ensuring consistency with our core safety mission. We at NHTSA are pursuing these common goals, and each of them applies to cybersecurity.

First, safety. NHTSA is first and foremost a safety agency, and cybersecurity is a critical element of that these days.
One of the key things we do at NHTSA is data collection – as all of you know, it's hard to address a problem without fully understanding the scope of the issue. Every year, NHTSA releases the previous year's crash statistics, giving us all a chance to examine how we can improve safety for vehicle occupants, pedestrians and other vulnerable road users.

According to our FARS data released just this week, the number of people killed in motor vehicle crashes declined by 2.4 percent in 2018. The early data for the first half of 2019 indicates that the recent downward trend in fatalities may be continuing. And while the number of fatalities today is far too high, we have to remember that the fatality rate 50 years ago was about 4 times higher. If we still had the same fatality rate today as back then, we'd be seeing well over 100,000 fatalities every year. That's horrifying.

Technology has helped save hundreds of thousands of lives – even millions over the past decades – and there's no disputing the fact that newer cars are safer cars. Your chances of being killed in a crash in a new vehicle are less than half as high as they are in vehicles that are 18 or more years old. I am confident that technology has played a role in helping reduce the number of lives lost on our roads, along with safe driving practices like wearing seat belts, putting down the phone, and most importantly, driving sober.

So how does cybersecurity fit in? Well, vehicles are software-driven these days, and many of the safety features of a vehicle—like electronic stability control, traction control, and antilock brakes—depend on software. If the software fails, then the vehicle might lose some of its safety features or even have its operations affected. As we rely more and more on software, the need for proper cybersecurity to ensure that our vehicle systems operate as intended is increasingly critical.

We actually think that technology has an even greater role to play in helping us save even more lives. After all, more than 36,500 people were killed in motor vehicle crashes in 2018 – a number that's still unacceptable and avoidable.

I am here to challenge you all to join me and everyone at NHTSA in our mission to save lives.

As I noted earlier, our second guiding principle is to improve our nation's transportation infrastructure. And cybersecurity will play a critical role in achieving our lifesaving mission, and in our nation's highway infrastructure, though it may not be obvious at first. Let me explain.

Automakers routinely use software patches to fix bugs or upgrade their systems, and we are increasingly seeing automakers use over-the-air updates to wirelessly patch their systems. Patching these systems over the air helps to ensure that our cars are kept up-to-date and safe, and can avoid needless delay while consumers find time to visit a dealer.

These wireless networks are and will be a critical component of our nation's infrastructure, and it will be necessary to ensure that they are protected from cybersecurity threats if we are to continue upgrading our vehicles' software in a quick and easy manner. And even when updates are done at the dealership, it will still be necessary to ensure that proper cybersecurity is observed.

There's a second aspect to our cybersecurity infrastructure, and that involves vehicle connectivity. The transformation of automobiles isn't something coming in 20, 30, or 40 years – the building blocks are here now with Advanced Driver Assistance Systems. We have seen that consumers are seeking out vehicles with these new technologies and advanced features. That's because they believe they work, and believe they will keep them safer.

NHTSA and the U.S. Department of Transportation are advancing research into vehicle technology and – in particular – how vehicles will talk to each other on our roads.

We recently launched a V2X research and safety test program to resolve open questions around V2X radio communication technologies in the "Safety Band" of spectrum used for Intelligent Transportation Systems.

This test program, aimed at independent, objective data collection and analysis, will address two key research areas: spectrum sharing and emerging CV2X technologies.

Research like this will help advance the deployment of new technologies and help put newer, safer vehicles into the hands of consumers. But that raises another question: What if consumers begin to fear that these technologies – and even their vehicles – can be hacked?

The Internet of Things is everywhere in our homes, our work, our lives. Think about your toaster. If it's new, there's a chance it may be connected to the Internet. Are you worried about it being hacked?

Ok, so maybe you aren't worried about hackers invading your toaster and learning about your toast preferences. The Internet of Things is a security mess, but fortunately most of those devices aren't safety-sensitive. But what about your thermostat? Or the ever-so-popular door cameras?

If you aren't thinking about cybersecurity for these devices throughout your home, you trust them. And the same should go for your vehicle.

And if you – or the consumer – are worried about it, then that means something is wrong. Cybersecurity is one of those thankless tasks – you know you're doing the right thing when people aren't talking about it.

Even one minor cyber incident could derail or cause significant roadblocks to the deployment of these lifesaving technologies. The public wants assurances that these technologies are safe for their families. They won't adopt it if they don't believe in it.

And we can't save lives and reap the benefits of these new technologies if the public doesn't believe these technologies are safe.

One of the worst things you can do regarding cybersecurity is to be too confident in your own product. Today's vehicles are computers on wheels, with many access points that offer potential vulnerabilities and that someone with enough persistence can - and will - find a way to compromise.

This is something we should expect.

However, even battle-tested professionals can be caught off guard. Being prepared means having a game plan and practicing it routinely to be ready to go when the adversary strikes.

The difference between a manageable and devastating vehicle cyber attack can boil down to the planning and precautions taken in advance of an actual situation.

From knowing who to alert, to taking the most appropriate approach to respond and mitigate any harmful effects, this takes some advance forethought and engagement with other stakeholders.

Communication is critical to being prepared for a cyber attack. Information sharing is why we're here today.

After all, if we're not talking, if we're not sharing, if we don't know the threats, how can we respond?

This community was created for this purpose – sharing and learning, which must continue, knowing that an attack on one is an attack on all, and in an instant, could jeopardize and set us back many years.

As an industry, you must be willing to implement playbooks or best practices, not just the Auto-ISACs, but those of others as well. So yes, while individual company interests are important, collective safety risk management through information sharing is vital.

As careful as you are, it is almost certain that vulnerabilities will be exposed and incidents will happen. How you respond will determine the impact of those incidents and whether the public still trusts you and your products.

Will you hunker down?

Or will you share and use the knowledge gained from the Auto-ISAC and other efforts to turn the incident into just a blip on the radar?

How you prepare and respond is up to YOU.

One way to be prepared is to participate in exercises with other stakeholders. NHTSA, along with many of you here today, participated in Cyber Storm 2018.

Just in case you aren't familiar with it – the Cyber Storm series, run by the U.S. Department of Homeland Security, is used to strengthen cyber preparedness in the public and private sectors. The purpose of a cyber security exercise is to prepare how a group responds to a specific attack scenario, including testing their procedures, policies, and plans.

Now while I wasn't fortunate enough to be a part of the 2018 exercise, I've heard nothing but positive things from our team members who were there.

They're looking forward to taking part in Cyber Storm 2020, and I challenge all of you to join us for this as well. Space is filling up, so please contact Auto-ISAC or DHS to register. We also appreciate Auto-ISAC's leadership for Cyber Storm 2020 to help coordinate industry efforts.

Beyond being extremely useful, it's fun. After all, who wouldn't like to play war games for a few days?

Our third guiding principle at DOT is preparing for the future. That means that we want to accommodate innovation in a technology neutral manner – we don't want to pick technology winners and losers – while adhering to our core safety mission.

At NHTSA, we take cybersecurity seriously, just as we take crashworthiness seriously. And crash avoidance. And driver behavior.

Cybersecurity is just one component of what we do and something we treat as seriously as any other piece of vehicle equipment. NHTSA sets standards for equipment, but we know that competitive forces truly drive innovation.

The industry has accomplished so much with crashworthiness and crash avoidance – we know these technologies are saving lives as we speak.

I want to especially recognize the leadership of our Secretary of Transportation, Elaine Chao, who is a passionate believer in the power of competition and the free market to pioneer safety breakthroughs.

Last week we announced that we will be proposing some big changes to the NCAP program next year. NCAP is a great program – it taps into market dynamics by providing consumers with reliable information on vehicle safety, and then consumer demand drives competition among automakers. That's the way it should be. The results have been wonderful, and vehicles today are safer than ever.

But the program has been a victim of its own success, and now most vehicles get 4 or 5 stars. It's like Lake Woebegone. We will be aiming to make the program more dynamic, and hopefully find ways to future-proof it so that automakers will continue to have incentives to make additional safety improvements.

We'll be looking at adding new crashworthiness tests and upgrading our test instruments, including our crash test dummies. And one of the features will be to better incorporate ADAS crash-avoidance systems into the program.

We want to help stimulate even more competition and even more safety innovation. And we want to do it in a tech-neutral manner through the free market by encouraging automakers to make investments to meet consumer demand.

We also want that innovative process to continue with cybersecurity. We are entering a new realm of security, but it's up to each of you to be responsible actors.

I stand here, on behalf of NHTSA, ready to help. We challenge you, the industry, to take the great responsibility you have seriously.

We encourage you to make improvements, because everyone benefits if there are no harmful cyber incidents – and if consumers have nothing to fear about the cybersecurity of new vehicles.

If you have a problem, if you have a question, if you fear something is wrong – ask us. We have experts in every field and stand ready and willing to help you navigate this new frontier. We want to be good partners with you, because we know that cybersecurity depends on you, the industry.

While NHTSA is not aware of any malicious hacking attempts resulting in safety concerns for the motoring public at this time, we do periodically receive information about potential vulnerabilities, generally uncovered by security researchers.

When NHTSA learns of such potential vulnerabilities, the agency follows its internal incident response process to ensure that any potential safety risks are thoroughly assessed and appropriately mitigated by the affected motor vehicle and/or motor vehicle equipment manufacturers.

One such case resulted in a product recall in 2015.

In my short time at NHTSA, I've already participated in a review of a cybersecurity incident to determine whether it posed an unreasonable risk to safety. I hope that's the last time I'll have to address cybersecurity in that setting.

However, let me be absolutely clear: NHTSA will not hesitate to act if there is any issue, including cybersecurity, that poses an unreasonable risk to public safety. Just as we act if there is a defective component in a vehicle that poses an unreasonable safety risk, we will do the same if there is a cybersecurity defect as well.

We are not in the business of designing your cybersecurity programs – that's up to you, the experts, and we earnestly wish you the greatest success.

But we are - and will remain - vigilant watchdogs, and we will act to protect the public. I come from an enforcement background, and while I believe that the best enforcement is never having to take enforcement action, I have never been shy about using our legal authorities when necessary and appropriate.

I am deeply and passionately committed to saving lives. Technology can help us do this – but no life can be saved if no one is using the technology because they don't trust it.

There are no shortcuts or magic formulas to earning this trust. From sports teams to medical professionals, preparedness and communication are the keys to success. It's no different in our field. Vehicle cybersecurity has high stakes – the safety and security of everyone on our roads depends on you.

I hope to be back here next year to report that fewer lives were lost on our nation's roads, in part because of the technology you are rolling out in affordable new cars, trucks and SUVs.

You can help save lives through the work you do every day – but only if you are working together and communicating like never before. Thank you very much.