Auto-ISAC Annual Summit

Keynote Address | James Owens, NHTSA Deputy Administrator

Wednesday, October 14, 2020 |

AS PREPARED FOR DELIVERY

I want to express my appreciation to Auto-ISAC's staff for all their work to transition this event from in person to virtual. And to the audience, I hope you and your families are safe and healthy.

So much has changed since we met a year ago in Plano, but one thing that hasn't is our commitment to safety. I know you hold that same commitment as we all adapt to these unprecedented times.

Our hearts go out to everyone who has been laid off or faces economic uncertainty during this public health emergency. We can't imagine the choices faced by many small businesses and entrepreneurs right now. Still, NHTSA, the U.S. Department of Transportation, and this Administration are all working to support our nation's economic recovery. I would like to thank our Secretary of Transportation, Elaine L. Chao, for her continued leadership and her unwavering support for NHTSA's safety mission.

The ongoing public health emergency has changed the way we all live, work, and drive. But one thing is clear: We must stay vigilant to protect and save lives, and cybersecurity is part of that.

In Plano, I said I hoped to be back this year to report that our nation lost fewer lives on America's roads. And I can say that today, but with a few caveats. Let me explain.

TRAFFIC TRENDS

Two weeks ago, we published a roundup of the 2019 FARS data, as well as traffic safety projections for the first six months of this year.

Here's what we saw in 2019. Fatalities decreased by 2%, which continues the encouraging three-year downward trend in deaths from traffic crashes. That translates into 739 fewer lives lost than in 2018. Pedestrian and cyclist fatalities were also down, a reversal of recent troubling trends, and the 2019 fatality rate was tied for the second lowest in history. That's all really encouraging news.

Now, let's look at the first six months of this year. We've faced some unprecedented challenges this year, including in traffic safety.
As I'm sure you noticed, our roads emptied as many people began staying at home, but soon after, we started hearing anecdotes about reckless driving, with officers clocking drivers speeding in the triple digits in many cases.

Over the summer, we gathered data from our State partners, and unfortunately, that data confirms some of the emerging trends we had observed back in the spring.

Our projection suggests that the total number of lives lost from traffic crashes in the second quarter was down by 3.3% over 2019, or 302 fewer deaths overall.

At the same time, the volume of traffic in the second quarter declined by 26%, so that the fatality rate per 100 million vehicle miles traveled went up to 1.42, even though fewer people lost their lives on the roads.

We've never seen trends like this, and we feel an urgency to work with our stakeholders to take action and turn this around as quickly as possible. 2019 was one of the best years for highway safety in our Nation's history, and we want to get back to where we were.

Doing so will require a combination of efforts – behavioral changes and technological advancements. Drivers making smarter choices, aided by safety features in their vehicles, can lead to fewer crashes and safer roads for everyone.

NHTSA is working with State and local agencies, safety stakeholders, and many others to address the reasons for these troubling trends. As an industry, you have an essential role in the safe development of vehicle safety technologies. And part of that safety includes cybersecurity.

TRUST

Cybersecurity is one of those thankless tasks – you know you're doing the right thing when people aren't talking about it.

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 compromised. 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.

Even one minor cyber incident could cause significant roadblocks to the deployment of 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.

V2X

Now, many future driver assistance technologies may rely on vehicle-to-vehicle or V2X communications to relay safety and other critical information.

V2X could augment camera and radar-based crash avoidance technologies, providing the driver that extra critical time needed to avoid the crash.

V2X technology also holds the promise of increased protections for vulnerable road users. It has the potential to allow vehicles to exchange information in real time with bicyclists and pedestrians who are carrying cell phones.

However, this new era of connectivity can present new risks. Cybersecurity must be built into every step along the way. The same goes for over-the-air updates, which are growing in popularity. Anytime you have wireless communications, you have the potential for vulnerabilities.

But potential is not the same as inevitability. By incorporating cybersecurity best practices and participating in exercises, you'll be better prepared if a cyberattack occurs.

EXERCISES

As the old saying goes, the more you sweat on the practice field, the less you bleed on the battlefield.

Exercises help us plan for issues before a cyberattack occurs. I urge you to continue them, even if they need to be reconfigured for remote work or virtual participation.

Such was the case with Cyberstorm 2020, and I want to thank Auto-ISAC and all the companies who joined us. Your participation makes us all better prepared for a potential cyber incident and refines our respective procedures.

I know we learned some valuable lessons through Cyberstorm 2020, and I hope you did as well. One takeaway was the importance of cybersecurity throughout the supply chain. OEMs and suppliers should work together to ensure the security of individual components – building cybersecurity into the process shouldn't be ignored.

COMMUNICATION

Exercises like Cyberstorm help us build the muscle memory on how to communicate when faced with potential threats, but let's not let this communication be limited to theoretical scenarios.

Sharing and learning must continue all year long. October is National Cybersecurity Awareness Month, but we need to be ready every single day. An attack on one is in fact an attack on all, and in an instant, could jeopardize our progress and set us back many years.

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

We're finalizing our updated vehicle cybersecurity best practices, which we hope will be published in the Federal Register very soon. When it's published, I invite you all to review it and submit your comments. Your feedback strengthens our work and improves the final product.

In the meantime, we're releasing a new research report today titled "Cybersecurity of Firmware Updates," which examines methods of updating vehicle firmware, including over-the-air updates. We also looked at methods used in similar industries, such as those involving commercial aviation, medical, and consumer electronics. The report is available on our website, and I think you'll find it helpful.

NHTSA

This best practice document is just one of many projects underway at NHTSA to support vehicle safety. We haven't slowed down a bit since the beginning of the national public health emergency.

Later this year, we will announce changes to NCAP, our five-star new vehicle safety ratings program, to make it even more relevant and informative for Americans. When published, the notice will seek public comment on updates, including new technologies, new test procedures, updates to vehicle labeling, and crash test dummy advancements. We'll also consider new technologies related to the safety of pedestrians and bicyclists. It's important to us that NCAP continues to reflect technological advancements, and we welcome your feedback when we publish these changes.

Over the summer, we launched the Automated Vehicle Transparency and Engagement for Safe Testing, or AV TEST, Initiative.
This is the first platform connecting the public, manufacturers, developers, operators, and all levels of

government to voluntarily share information about the on-road testing and development of prototype automated driving systems.

As the nation's highway traffic safety agency, NHTSA is interested in the safe development and testing of these systems, which have the potential to one day help prevent fatal crashes, save lives, and reduce crash severity. These technologies may also improve mobility for underserved communities, including people with disabilities and older adults.

I hope you joined us for at least one of the more than a dozen virtual events we've held so far as part of the AV TEST Initiative. And we hope you'll join us for future events as well.

In September, we rolled out the AV TEST online tracking tool, a first-of-its-kind, transparent way for the public to learn about the on-road testing of automated driving systems in their communities. I hope you'll check it out if you haven't already – it's online at NHTSA.gov/AVTEST.

NHTSA continues to work on numerous rulemakings related to the safe development and deployment of automated driving systems, or ADS.

This spring, we published a notice of proposed rulemaking that would modernize federal occupant protection standards to accommodate ADS vehicles without traditional manual controls. We're working to finalize the rule later this year.

We are also working on an Advance Notice of Proposed Rulemaking, or an ANPRM, on varying regulatory and subregulatory approaches to the safety of motor vehicles equipped with automated driving systems. We plan to seek public comment on creating a safety framework for objectively and transparently assessing and validating each ADS vehicle's safety performance.

We also plan to seek comment on the potential development of a new regulatory approach for ADS. This could include Federal Motor Vehicle Safety Standards for ADS competency, or alternative safety regulations relating to ADS performance.

And, of course, NHTSA continues to conduct rigorous oversight to identify any potential safety risks to the traveling public. We never hesitate to act if there's a defect that poses an unreasonable safety risk, and we will do the same for cybersecurity defects as well.

CLOSING

In closing, I know these are challenging times for everyone, but I also know we can get through them together. Stay strong and never lose sight of our shared safety mission. Continue communicating and sharing information through Auto-ISAC, and please prioritize cybersecurity in every step of the process.

If you have a problem, if you have a question, if you fear something is wrong – please reach out.

NHTSA stands ready to help you address emerging issues and ensure the safety of the traveling public. We want to be good partners, because we know that cybersecurity depends on you.

Now is not the time to let down our guard. It's time to redouble our commitment and stand firm against threats and attacks.

Vehicle cybersecurity has high stakes – the safety and security of everyone on our roads depends on it.