Remarks: Automated Vehicles Symposium 2015

Mark R. Rosekind, Ph.D.
Administrator, National Highway Traffic Safety Administration
U.S. Department of Transportation
Tuesday, July 21, 2015
As Prepared for Delivery

Additional Resources

NHTSA and Vehicle Cybersecurity -- Today's electronics, sensors, and computing power enable the deployment of safety technologies. Given the potential of these innovations, NHTSA is looking at all of our tools, as well as exploring new ones, that can be used to deploy these technologies in safe and effective ways, taking steps to address the new challenges they pose — particularly with respect to cybersecurity.

Jane, thank you for your introduction. The Volpe Center is an invaluable partner in so much that we do at NHTSA and DOT, and it's great to share the stage with you today.

Thank you to TRB and AUVSI for the opportunity to speak with you today. When I joined NHTSA in January, I identified three priority areas for my two years on the job, and technology innovation was one of them. Working for Secretary Foxx at DOT, it couldn't be any other way - the secretary is deeply committed to pursuing innovations that can transform every mode of transportation. Among the topics to discuss with you today is the secretary's commitment to connected automation for our roadways.

Before that discussion, I want to make sure that you're aware of an item at the top of the secretary's agenda, and indeed President Obama's. Politics and engineering don't always mix, but we're in a situation now where what happens in Washington - and what doesn't happen - will have a direct effect on what happens in your labs, on your test tracks, and on your factory floors.

As many of you know, authorization for transportation programs, including many critical NHTSA programs, expires at the end of this month. That's when the clock runs out on a temporary extension - one of more than 30 that Congress has passed since the last reauthorization bill expired. This series of temporary solutions has left our transportation system starved for investment.

Secretary Foxx has proposed a common-sense solution, the GROW AMERICA Act, which would make major new investments in transportation, including innovation that can transform our highways and make them safer. For all of us who care about building a transportation system that embraces innovation, one that creates jobs and opportunity, the next few weeks look to be crucial, and I hope you will all remain vigilant and involved in this important debate.

If there is support for making the right investments, we can open the door to a revolutionary era on our roads. Many of you are helping spur that revolution. A suite of related innovations - vehicle-to-vehicle and vehicle-to-infrastructure communications, and automation that relies on advanced sensors and sophisticated computer systems - are opening new opportunities to save lives. For nearly a century, vehicle safety has been about protecting vehicle occupants from the inevitable crashes they would endure. Today, we are moving toward a fundamentally different goal - preventing those crashes from ever occurring. From the start, motorists have had to accept the risk of death or injury as the cost of mobility. Now, we're poised to massively reduce that risk.

NHTSA and the Department of Transportation are not spectators in this revolution. For a department whose top priority is safety, and for an agency whose primary mission is highway safety, that is not an option. Our responsibility is to ensure that these innovations achieve their life-saving potential. That means ensuring that innovation is aimed squarely at safety, and that innovations with safety potential make it onto the road rapidly and are widely distributed. NHTSA, the Intelligent Transportation Systems Joint Program Office under the secretary, the Federal Highway Administration and other elements of DOT are working together, under the secretary's leadership, toward that goal.

In May, Secretary Foxx made an announcement that underlined our commitment to these innovations. Let's spend a few minutes on that announcement, because it's important for you to know just how strongly DOT and NHTSA are committed to these innovations and our role in helping them reach their potential

Speaking in Silicon Valley, Secretary Foxx announced three significant policy initiatives. First, he announced that NHTSA would accelerate its rulemaking process on V2V communications. Our goal to complete DOT's work on a Notice of Proposed Rulemaking to require V2V equipment in new vehicles is now to have a proposal ready for interagency review by the end of the year. Second, he committed DOT to completing initial testing on potential sharing of the radio spectrum set aside for V2V and other safety-critical road communications within one year of receiving production-ready devices to test. And the secretary directed us at NHTSA to examine our regulatory framework and determine if there were any obstacles to safety innovations, and if so, how to tackle them.

Now, accelerating the calendar for the V2V proposal by a few months may not sound like a big deal. But it means long nights and days for our rulemaking team and technical experts. We believe the hard work is justified, because moving up our timetable is an unmistakable statement of our commitment to V2V.

That's especially important because of the second issue the secretary addressed, testing for potential spectrum sharing and interference with V2V radio signals. As you know, many in Washington would like to use some of the radio spectrum now designated for critical safety communications. We need to ensure that sharing that spectrum can take place without blocking safety-critical signals, and the secretary's announcement was aimed at answering that critical question as soon as possible. To be clear: the department is not opposed to the concept of sharing. We simply need to make sure - through verifiable testing - that sharing works. We can save lives with a clear signal, and we're determined to do the hard technical work to make sure that signal gets through.

The third topic the secretary addressed is our regulatory framework. Unfortunately, much of the conversation about vehicle automation

seems to focus on whether government regulations are likely to get in the way. NHTSA is not interested in erecting roadblocks to safety innovations – we want to encourage those innovations. In response to the secretary's directive, a NHTSA team from across the agency is looking at how we can best speed these innovations; what changes might be necessary in our policies and regulations to make them more flexible and nimble; and whether there are any obstacles that we need help from Congress to clear. This team includes technology experts as well as attorneys, safety defect experts, behavioral safety experts and communications professionals. Just a few days ago, they briefed me on their progress, and I am very encouraged by their work so far.

It's important to note the principle Secretary Foxx articulated here: If an innovation is demonstrated to improve safety, we want to help make it happen. The safety aspect here is essential. I would encourage all of you, in your discussions with NHTSA on how the agency can encourage innovation: put safety first, and bring the data.

Our work to promote safety innovation is important because with all of the challenges in developing and fielding these technologies, government should not be another obstacle. The job is hard enough. Designing, engineering, testing and validating these systems is a significant technical challenge. And as this conference's program acknowledges, the issues aren't just technical. They're legal and ethical.

While those challenges are not simple or easy, they can be overcome with time, skill and a cooperative spirit. But we also must recognize that connected automation isn't just about accounting for human nature when the human is in the driver's seat.

For these innovations to reach their true potential, we've got to account for, well, us – people, with all our failings and foibles. We will need to help folks who can't tell a lidar from a coffee maker understand how these innovations work, and how they will make us all safer, so that the public embraces them. We've got to develop human-machine interfaces that don't require drivers to develop astronaut-like skills of interpretation for all the beeps, tones, buzzes and warnings that come their way

And there's one more human challenge we face: the bad-actor threat. Whether for profit or out of sheer malicious intent, we know these systems will become targets for bad actors. They are a threat to safety, to privacy, and to public acceptance of connected automation. We must reassure vehicle owners that their data is secure, that their vehicle is secure, and that we are looking out for threats from hackers, thieves, and anyone else who might seek to tamper with safety-critical technology.

Cyber-security and privacy must be high-priority items for industry and for NHTSA. And two recent events highlight just how seriously we are, together, taking this challenge.

The first is NHTSA's release, today, of our latest in a series of continuing public documents outlining our privacy and cybersecurity efforts and the major obstacles to success in these areas. Our paper outlines the wide range of NHTSA's work in this area. It details how NHTSA has reorganized its vehicle safety research operation to meet the cybersecurity challenge; our work with the most effective security experts in the business to design, implement and test a security system for V2V transmissions; and our assessment of the various threat vectors that could endanger vehicle security and privacy, and how we're working to defeat those threats.

This paper is in part a response to questions we've received from Congress and the media on these topics. Lots of people are aware that these challenges exist, but as those questions showed, few people were aware of what NHTSA is doing to protect safety-critical systems. When a TV news show hacks a car, that's not news to NHTSA. The folks at our Vehicle Research and Test Center have figured out how to do some remarkable things with vehicle electronics, in order to prevent others from doing them. NHTSA not only is aware of these threats, but we're working to defeat them. We want Americans to know we're on this, because robust protections against malicious actors are absolutely critical in building public enthusiasm for connected automation. V2V and high-powered computers can't save lives if American drivers don't trust that they're secure.

Another significant development is the announcement last week that major automakers will form an Information Sharing and Analysis Center to team up against cybersecurity threats. NHTSA has been urging the industry to form an ISAC for some time, and the agency sees this announcement as a milestone in cybersecurity efforts. ISACs serve as clearinghouses for information on the latest cyber threats, and can help coordinate security efforts, both before an incident occurs and in the midst of a crisis. The finance, aviation and utility industries all have established ISACs to help protect their critical infrastructure. Well, the infrastructure of connected automation is just as critical. Establishing an ISAC is an essential element in protecting that critical infrastructure, and it demonstrates the industry's commitment to that task. Last week's announcement is a great first step, and I urge the involved companies and organizations to press forward as quickly as they can to make their ISAC operational.

In closing, let me connect that joint industry effort to the broader world of vehicle safety, and offer two challenges to all of you.

Certainly, you have all heard about the Takata air bag problem. It is obviously a major focus for us at NHTSA, and within the industry. A couple months ago I met with representatives of the industry consortium that is searching for the elusive root cause of these air bag inflator ruptures. As these executives sat down in my office, I asked, "How often does the industry band together to confront a safety issue like this?" After a few shrugs, their answer was, "It's never happened before. We've never done this."

That has to change. The auto industry will always be a competitive business. But safety isn't a competitive edge to tout in TV commercials – you never see a star rating on the side of an airliner when you board. Safety is a shared responsibility. The more we break down barriers to cooperation and information sharing when it comes to safety, the more lives we will save. The decision to form an ISAC has already demonstrated that the industry is capable of joining together when it comes to safety. Connected automation presents an enormous opportunity to approach safety in a different way. A more cooperative, proactive way. The people in this room – the community of people who are excited about the potential of connected vehicles and automation – can help establish that mindset.

The second challenge I'll offer is also prompted by the Takata situation. Air bags are designed to save lives. And they do – 40,000 Americans have survived crashes that otherwise would have been fatal because an air bag protected them from harm. But these defective inflators are taking lives instead of saving them. For those of us dedicated to life-saving innovation, it's a painful irony.

It's also a warning. When it comes to safety-critical technologies, "good enough" just won't cut it. From design to engineering to production and execution, quality and durability must be exceptionally high. We all know that drivers are the largest source of crash risk on our roads. But, when we design automated systems to reduce the risk of human error, we're taking the steering wheel out of the hands of the vehicle operator, and putting it into the hands of all the engineers, designers and software coders who put those systems together. That is a serious responsibility. I urge you to embrace it, to respect it, and to hold yourselves and your companies to the highest possible safety standards.

The future is filled with tremendous potential to significantly enhance transportation safety through technology innovation. Working together, we will see that potential transformed into lives saved and injuries prevented on our roads.

Thank you.

U.S. DEPARTMENT OF TRANSPORTATION
National Highway Traffic Safety Administration
1200 New Jersey Avenue, SE
Washington, DC 20590
1-888-327-4236
1-800-424-9153 (TTY)