Statement of Nathaniel Beuse, Associate Administrator for Vehicle Safety Research, National Highway Traffic Safety Administration

Before the

House Committee on Oversight and Government Reform

Hearing On

"The Internet of Cars"

November 18, 2015

Good morning Chairmen Mica and Hurd, Ranking Members Duckworth and Kelly, and members of the subcommittees. I appreciate this opportunity to testify about how the National Highway Traffic Safety Administration (NHTSA) is addressing emerging challenges associated with new connected vehicle technologies.

In 2013, there were over 5.7 million motor vehicle crashes in the United States, and 32,719 people died in vehicle-related crashes. The consequences of these crashes range from personal tragedies that impact individual families forever, to billions of dollars in economic damage due to lost productivity, increased congestion, environmental impact and other negative consequences. While we have made significant improvements in motor vehicle safety, vehicle crashes remain the leading cause of death for ages 11 to 27—and a major factor in most other age ranges.

NHTSA's mission is to reduce deaths, injuries, and economic loss resulting from motor vehicle crashes. NHTSA's vehicle safety activities will continue to enhance occupant protection when crashes occur, but, as Secretary Foxx recently said, "The Department wants to speed the nation toward an era when vehicle safety isn't just about surviving crashes; it's about avoiding them."

NHTSA believes this era of innovation that we are entering holds great promise to help us address the approximately 94 percent of crashes that are due to driver error. New technologies such as vehicle-to-vehicle communications and automated vehicle technologies have the potential to dramatically change the safety picture in the United States by helping drivers avoid crashes in the first place. Together, connected and automated vehicle technologies can help a driver operate his or her vehicle in a safer manner; warn the driver of an impending collision; and can even provide active crash avoidance assistance through applying vehicle's brakes or steering if such warnings are not heeded.

These new technologies also bring different challenges that NHTSA is poised to address. For example, consumers hear a lot about cybersecurity as it relates to banks and personal information. Now in the auto space, cybersecurity is taking on new meanings, even showing up in TV shows. NHTSA's research program is aimed at laying the foundation for active collaboration, pushing the state of the art, and informing agency policy decisions. NHTSA, and the entire Department of Transportation (USDOT), believes the emerging challenges associated with new automated and connected vehicle technologies are addressable and that they should not keep us from pursuing the innovative technologies that can save lives.

The Safety Promise of Vehicle To Vehicle Communications

Testing and analysis done by NHTSA and the Intelligent Transportation Systems Joint Program Office (ITS JPO) indicate that vehicle-to-vehicle communications, or V2V, is a crash avoidance technology that can potentially address up to approximately 80 percent of crashes involving two or more motor vehicles. This technology is different than what we hear about when vehicle manufacturers talk about providing WiFi and cellular connectivity. This technology promises to be transformative and is about enabling a new era of safety that may not only save lives, but have other benefits as well. When fully realized, this communications technology is extendable beyond vehicles and the infrastructure. It can even be deployed to other devices that would be carried by pedestrians and cyclist thereby addressing these crashes, which represent an increasing share of total motor vehicle involved fatalities. V2V is based on vehicles wirelessly sharing their position, speed and heading information with each other in near real-time fashion. Each vehicle uses the information from surrounding vehicles to determine if a collision is imminent, and then warns the driver as needed.

V2V is expected to augment today's technologies such as forward collision warning, blind spot warning, and automatic emergency braking systems. V2V technology will likely be fused with other technologies that rely on sensors, such as radar or cameras, to further improve the effectiveness of these safety systems. This allows for potential crash situations to be detected sooner and more reliably. This is because V2V allows for enhanced 360-degree situational awareness; extends the operational range of conventional sensors such as radar and cameras; and allows a vehicle to "see" around corners, it can assist the driver in many challenging crash scenarios. Intersection related crashes is one of those scenarios and is one of the most pervasive and deadliest crash types. V2V communications will also allow development and implementation of safety applications that rely on communicating with roadway infrastructure elements, such as traffic signal controllers, and can address safety issues that cannot be entirely addressed solely by V2V applications

NHTSA and vehicle original equipment manufacturers (OEMs) also recognize that V2V provides an important capability that can be leveraged to improve the performance, reliability and safety of automated vehicles, thus allowing for the full potential of a connected-automated vehicle environment to be realized. V2V communications allows vehicles to (nearly) instantaneously share information about driver intent that is not possible with conventional sensors, including, for example, turn signal, brake and accelerator actuations. Such information can be used in advanced automated vehicle concepts to more accurately coordinate movements among vehicles to improve both efficiency and safety of traffic flow.

Proactive Vehicle Cybersecurity

USDOT and NHTSA are fully committed to the era of crash avoidance through automated and connected vehicles, due to their unprecedented safety improvement potential. These modern crash avoidance technologies have become possible with the increasing use of electronics, software and connectivity in the design of a car, similar to how our lives have been revolutionized by the rapid connectivity made possible by computers, the Internet, cellular, GPS, satellites and other communication and information processing. As these systems became integral to our daily lives, so too did the potential for attacks to those same systems. Cybersecurity rose out of necessity to protect these vital systems and the information contained

within them. Applied to vehicles, cybersecurity takes on an even more important role: systems and components that govern safety must be protected from malicious attacks and incidents, zero-day vulnerabilities, damage, or anything else that might interfere with safety functions. We are fully aware that failure to tackle the cybersecurity challenge would threaten the technology-driven safety transformation we all want to achieve.

For these reasons, vehicle cybersecurity has never been an afterthought for NHTSA. In exploring the potential of connected vehicles and other advanced technologies, NHTSA remained aware that cybersecurity would be essential to the public acceptance of vehicle systems and to the safety technology they governed.

To ensure a robust cybersecurity environment for these dynamic new technologies, NHTSA modified its organizational structure, developed vital partnerships, adopted a layered research approach, considered legislative additions (as contained in the GROW America), and encouraged members of the industry to take independent steps to help improve the cybersecurity posture of vehicles in the United States. NHTSA's goal is to be ahead of potential vehicle cybersecurity challenges, and seek ways to address them.

In 2012, NHTSA modified its research organization to focus on vehicle electronics, including cybersecurity. NHTSA established a new division, Electronic Systems Safety Research, to conduct research on the safety, security, and reliability of complex, interconnected, electronic vehicle systems. More recently, NHTSA expanded its research and testing capabilities in vehicle electronics at its Vehicle Research and Test Center in East Liberty, Ohio. Personnel at that facility are responsible for evaluating, testing, and monitoring potential automotive cyber vulnerabilities, and for leading the agency's research of highly automated vehicles.

To help develop a comprehensive approach to address cybersecurity, NHTSA consulted other government agencies, vehicle manufacturers, suppliers, and the public. The approach covers various safety-critical applications deployed on current vehicles, as well as those envisioned for future vehicles that may feature more advanced forms of automation and connectivity. A few months ago, NHTSA published a white paper, "NHTSA and vehicle cybersecurity,"[i] in which the agency outlined its multilayered approach to cybersecurity in further details. This approach has the following goals:

1. Expand the knowledge base to establish comprehensive research plans for automotive cybersecurity and develop enabling tools for applied research in this area;

2. Facilitate the implementation of effective, industry-based best practices and voluntary standards for cybersecurity and cybersecurity information-sharing forums;

3. Foster the development of new system solutions for automotive cybersecurity;

4. Research the feasibility of developing mandatory minimum performance requirements for automotive cybersecurity; and

5. Gather foundational research data and facts to inform potential future Federal policy and regulatory activities.

There are tremendous opportunities in this realm for proactive steps. In fact, such steps are essential. Regulation and enforcement alone will not be sufficient to address these risks – cybersecurity threats simply move too fast and are too varied for regulation to be the only answer. The auto industry can play an essential role by cooperatively establishing rigorous best practices that address the broad range of cyber threats; by reacting quickly and appropriately when such threats emerge; and by working closely with government and independent security analysts to identify and defeat attacks. The decision to establish the Automotive Information Sharing and Analysis Center (ISAC), which is expected to be in operation by the end of this year, is one important proactive step. The importance of a robust information sharing forum for the industry was demonstrated when NHTSA influenced the first cybersecurity related recall on-record in July 2015 that involved up to 1.4 million vehicles. Vigilance in mitigating the safety risks in that particular case was necessary but not sufficient. It was essential for the rest of the industry, including OEMs, equipment suppliers, and wireless carriers to review designs to determine whether similar or related vulnerabilities existed elsewhere. In the cybersecurity realm, those involved must keep moving, adapting, improving and sharing intelligence. Our efforts will need to be collective, collaborative, comprehensive, and continuous.

Addressing V2V Security

More specifically related to V2V security, for the past several years, USDOT, NHTSA, vehicle manufactures, automotive suppliers, security experts, standards development organizations, and other government agencies have been developing Dedicated Short Range Communications (DSRC) radio technology and the associated architecture and protocols to support trusted vehicle-to-vehicle and vehicle-to-infrastructure communications. We have made significant progress on the architecture and have research plans to conduct large-scale vulnerability testing and to address any security issues that emerge from that testing. In addition, as NHTSA pursues these efforts, the agency will address various aspects of the architecture including the protocols that will ensure interoperability, security and privacy protection.

NHTSA and its partners are developing a Public Key Infrastructure (PKI) based system, termed the "Security Credential Management System" (SCMS), for ensuring trusted and secure V2V and Vehicle to Infrastructure (V2I) communications. PKI security architectures and methodologies are already used extensively in the information technology and communications industries, as well as in the automotive telematics applications. The SCMS would employ highly innovative methods, encryption, and certificate management techniques to address the challenging task of ensuring trusted communications between entities that previously have not encountered each other. This is further detailed in NHTSA's publication, *Vehicle to Vehicle Communications: Readiness of V2V Technology for Application*.

USDOT also has reached out to our government partners at the Defense Advanced Research Project Agency (DARPA) and the National Institute of Standards and Technology for their input as NHTSA works to identify potentially unique cyber vulnerabilities associated with establishing a standardized wireless link with motor vehicles, and develop countermeasures and solutions for such vulnerabilities.

Privacy
NHTSA takes consumer privacy very seriously. The agency is committed to regulating items of motor vehicle equipment that may impact individual privacy in a manner to both protect consumers and promote advances in motor vehicle safety technology. NHTSA plans to address some aspects of privacy, as it relates to V2V, in our upcoming Notice of Proposed Rulemaking on V2V Communications.

Separately, NHTSA is also working with other Federal partners such as the FTC, which has broad authorities in regulating and enforcing relationships between automakers and consumers for purposes of protecting consumers and their privacy.

Importance of Spectrum
V2V technology relies on licensed, dedicated short range communications (DSRC) to operate effectively to provide the safety benefits outlined above. In 1999, the FCC allocated a portion of the 5.9 GHz spectrum for this important purpose, and since that time, DOT and other stakeholders have worked actively to make V2V and V2I a reality. In light of growing demand for spectrum, particularly for unlicensed Wi-Fi devices, there is a proceeding pending before the Federal Communications Commission (FCC) aimed at considering whether, and on what terms, the 5.9 GHz spectrum could be "shared." DOT is not opposed to sharing the spectrum, so long as it can be done in a way that ensures the safe functioning of V2V safety applications, and that sharing proposals do not block or disrupt safety-critical information transmissions between communicating vehicles. Toward that end, DOT is working closely with FCC, NTIA, members of industry, and other stakeholders on an expedited basis to evaluate and test potential sharing solutions for the 5.9 GHz spectrum band as soon as devices are available to test.

Moving Forward with V2V
In August 2014, NHTSA issued an Advanced Notice of Proposed Rulemaking (ANPRM) concerning a DSRC-based vehicle communications safety system on all new light duty motor vehicles.[ii] The ANPRM requested comment on the basic radio system, security features, and functionality to support interoperable communications—but explained that the agency did not anticipate that it did not currently intend to require specific safety applications. Such an approach will allow the market and auto OEMs to innovate and compete in offering safety applications. Concurrently, NHTSA also issued a comprehensive "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application" report (or Readiness Report) that provides details on the technology, results of testing programs, benefits, deployment challenges, as well as security, policy, privacy and regulatory issues.[iii]

NHTSA received more than 900 comments in response to the ANPRM, the V2V Readiness Report, and our questions. The automotive manufacturers stated that the Federal government needed to assume a large role in establishing key elements of the V2V environment, including establishing common operating criteria for V2V devices, establishing a security credentials system, and preserving the 5.9 GHz spectrum for V2V safety. Automotive suppliers generally expressed support for the technology and indicated the technology and standards for the technology were mature enough for initial deployment. Safety advocacy groups also expressed support, but emphasized the importance of ensuring interference-free spectrum for V2V.

Auto companies are supporting V2V technology, as demonstrated by GM's October 2014 announcement that they would be implementing V2V technology "as soon as possible-with a target of 2017 on select models." GM acknowledged that NHTSA's push to mandate DSRC radios was a driving force behind its announcement. This activity is not just limited to manufacturers, but states such as Michigan have also announced infrastructure deployments.

In September, Secretary Foxx announced the first three awards under DOT's national Connected Vehicle Pilot deployment program. The locations in New York City, Tampa and Wyoming were selected in a competitive process to go beyond traditional vehicle technologies to help drivers better use the roadways, relieve the stress caused by bottlenecks, and communicate with pedestrians on cell phones of approaching vehicles.

NHTSA announced its intent to move forward with V2V for light vehicles in February 2014 because of the potential to dramatically improve vehicle safety and V2V's importance as a stepping stone toward achieving safe automated driving. The USDOT-led research program has demonstrated through extensive analysis, controlled testing, and real world field studies that V2V communications offer an important opportunity and has the potential to dramatically improve safety on our Nation's roads.

In May of this year, Secretary Foxx announced USDOT's intent to accelerate V2V rulemaking activities with the goal of sending a regulatory proposal to OMB during 2015. NHTSA has accepted the challenge and the agency and the Department are working diligently to meet this goal. Connected, automated vehicles that can sense the environment around them and communicate with other vehicles and with infrastructure have the potential to revolutionize road safety and save thousands of lives. NHTSA already is laying the groundwork needed for the road ahead, and looks forward to working with Congress, manufacturers, suppliers, others in the Administration, and the American public in our exciting transportation future.

---

[i] Found at www.nhtsa.gov/Research/Crash+Avoidance/Automotive+Cybersecurity
[ii] Found at www.safercar.gov/v2v/index.html
[iii] Found at www.safercar.gov/v2v/index.html

Mr. Nat Beuse works as the Associate Administrator for Vehicle Safety Research at the National Highway Traffic Safety Administration (NHTSA). In that role, he is responsible for NHTSA's vehicle safety research activities which are focused on achieving the agency's mission of reducing fatalities and injuries caused by motor vehicle crashes. This includes developing and conducting research aimed at supporting Federal motor vehicle safety standards and consumer information programs, spurring voluntary industry actions through guidelines, and advancing the state of the art on wide variety of vehicle programs. He is also responsible for the Vehicle Research and Test Center where a significant amount of laboratory testing and analysis occur. Prior to this role, Mr. Beuse worked as the Office Director for Crash Avoidance Rulemaking located within the rulemaking arm of the National Highway Traffic Safety Administration (NHTSA). Nat has published and presented several technical papers dealing with occupant safety, consumer information, and vehicle design. Nat received his undergraduate and graduate degree from Marquette University located in Milwaukee, WI. He received a Bachelor of Science in Biomedical Engineering and a Masters degree in Mechanical Engineering.