Comments of the Association of Global Automakers Concerning The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things; Docket No. 160331306–6306–01

The Association of Global Automakers, Inc. (Global Automakers)[1] appreciates the opportunity to comment on the National Telecommunications and Information Administration's (NTIA) April 1, 2016, Request for Public Comments on The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things (IoT).

Given that motor vehicles are increasingly becoming an important aspect of IoT, Global Automakers supports NTIA's efforts to establish a positive regulatory environment that promotes innovation and ensures that consumers can benefit from increased connectivity. Like many other sectors in the U.S. economy, the automobile industry has undergone a wave of innovation over the past decade, sparked in part by increased connectivity. This connectivity not only provides greater comfort and convenience to drivers (*e.g.*, through navigation and infotainment systems), but it will also play a key role in vehicle automation through dedicated short range communication (DSRC) and other technologies. This, in turn, will present significant opportunities for saving lives, enhancing mobility and access to transportation, improving transportation efficiency, reducing fuel consumption, and lowering emissions.

However, these transformative technologies also present a number of challenging questions, and resolving these issues will require significant coordination among the automobile industry, federal legislators and regulators, as well as state and local governments and other stakeholders. The automobile industry welcomes federal leadership that will create national policy facilitating the introduction of advanced automotive technologies. It is important that any government actions be considered in a way that is flexible and responsive to changes in technology, so that the benefits of connected and automated vehicles can be fully achieved. Global Automakers looks forward to further engagement with NTIA as it moves forward to address these important questions.

A. Motor Vehicles Are Becoming Increasingly Automated And Connected

The automobile industry has made, and continues to make, substantial investments in the research and development of advanced technologies that save lives on the American roads. Over the past several decades, automakers have made tremendous strides in safety by improving vehicle crashworthiness, *i.e.,* how well the interior cabin protects occupants in the event of a crash. Today, the industry is taking the next giant leap in safety and mobility, developing automated crash avoidance technologies that seek to prevent crashes from occurring altogether—

[1] The Association of Global Automakers represents international motor vehicle manufacturers, original equipment suppliers, and other automotive-related trade associations. Our members' market share of both U.S. sales and production is 40 percent and growing. We work with industry leaders, legislators, regulators, and other stakeholders in the United States to create public policy that improves motor vehicle safety, encourages technological innovation and protects our planet. Our goal is to foster an open and competitive automotive marketplace that encourages investment, job growth, and development of vehicles that can enhance Americans' quality of life. For more information, visit www.globalautomakers.org.

technologies such as crash imminent braking, lane-keeping assist, and adaptive cruise control. These systems, which are often considered foundational to the development of more highly automated vehicles, are designed to provide support to the driver only in certain situations, and automated vehicle control is not typically sustained over an extended period of time. As these systems become more advanced, a vehicle's capability to operate without the active control and/or monitoring of the driver will increase, and the ability to communicate with surrounding vehicles and infrastructure will be key to realizing the full potential of this technology.

Connectivity is expected to play an important role in automation in the future. This connectivity is expected to be achieved through various channels. Currently, motor vehicles are connected to the world around them through satellite links to GPS-enabled navigation systems, imbedded cellular, and portable devices. The next evolutionary step in vehicle connectivity—and one which will significantly enhance motor vehicle safety—is vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-pedestrian communication enabled through DSRC technology. DSRC technology, supported by the 5.9 GHz spectrum band, enables continuous, high-speed, and authenticated data exchange among moving vehicles and between vehicles and roadway infrastructure or mobile devices (collectively referred to as V2X), to support safety-critical applications, as well as mobility and environmental applications. DSRC-supported V2X applications allow the transmission of messages between vehicles about vehicle speed, heading, brake status, and other information with range capabilities that exceed camera or radar-based systems currently supporting automated features. As connected vehicles penetrate the market, the capabilities provided by DSRC technology will greatly enhance the situational awareness of automated vehicles and help expand their functionality.

Private industry and the federal government, in an over ten-year partnership, have made major investments to develop, test and perfect DSRC technology and create V2X applications. This technology has already been deployed in vehicles on public roads in Ann Arbor, Michigan. In September 2015, DOT selected three additional locations—New York City, Tampa, and the State of Wyoming—as Connected Vehicle Pilot sites. These sites will deploy DSRC-based solutions in public settings to address pedestrian safety, expressway and urban congestion, and weather events affecting an interstate corridor heavily used by trucks. The New York City pilot will include 10,000 vehicles and hundreds of intersections. In addition, one major auto manufacturer has already announced that it will be introducing DSRC capabilities on one of its models this year.

B. The Federal Government Must Support DSRC Technology By Finalizing The Mandate And Protecting The Spectrum

Vehicle-to-vehicle and vehicle-to-infrastructure communication will be enabled through DSRC systems utilizing the 5.9 GHz band. There are two important actions the federal government can undertake to encourage the development and deployment of this technology.

First, the National Highway Traffic Safety Administration (NHTSA) should finalize its proposed rule to mandate DSRC systems on new vehicles.[2] A DSRC mandate is critical to the

[2] *See* Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications, Advance Notice of Proposed Rulemaking, 79 Fed. Reg. 49,270 (August 20, 2014).

fleet-wide adoption of this game-changing technology as it would ensure that all vehicles are able to communicate with each other using a compatible protocol. Based on the Advance Notice of Proposed Rulemaking, we anticipate that the rule will require the installation of the DSRC hardware, while providing automakers the freedom to innovate in the development and implementation of applications. This rulemaking and the underlying technology is a critical building block for future advances in automotive safety and mobility.

Second, the Federal Communications Commission (FCC) should act to preserve the spectrum that has been allocated to automobile DSRC technology. The FCC allocated the 5.9 GHz band for intelligent transportation services covering numerous safety and mobility applications. While deployment of DSRC is moving ahead, a regulatory proceeding is pending at the FCC to consider opening up the band for unlicensed use, which could cause harmful interference to DSRC applications, jeopardizing the deployment of the latency-sensitive applications designed for the 5.9 GHz band. While Global Automakers supports spectrum sharing, no decision should be made until a sharing approach is adopted that will not cause harmful interference to any DSRC applications deployed throughout the band.

C. The Federal Government Should Take A Leadership Role In Automated Vehicles

A supportive regulatory environment for automated vehicles will require strong leadership at the federal level. A principal goal of this leadership should be avoiding a patchwork of different federal and state standards for automated technologies. In January 2016, Secretary Foxx signaled that the Department of Transportation (DOT) was taking proactive steps to provide federal leadership and guidance in the development of a more consistent national policy on automated vehicles. Among the initiatives announced were commitments not only to work with industry stakeholders to develop guidance for the safe deployment and operation of automated vehicles, but also to work with the American Association of Motor Vehicle Administrators (AAMVA) and other state partners on the development of model state policy. These are positive steps, and automakers are continuing to engage with NHTSA on these efforts.

Despite these actions, many states have stepped into what they perceive to be a policy vacuum in the field. The result is that states such as California, Nevada, and Florida, have all enacted laws that will impact the way automakers can design automated vehicles. Each of these states has taken a slightly different approach to the issue, even using different definitions of what constitutes an automated vehicle. California is in the process of drafting its own automated vehicle regulations that would establish the "behavioral competencies" (*i.e.* subjective performance requirements) an automated vehicle must possess in order to be operated in the state.

These different state actions will present significant challenges to innovation and deployment. A patchwork of state laws establishing inconsistent design and performance criteria for automated vehicles would be unworkable for the industry and for consumers. Federal policymakers have long recognized the public benefit of having Federal Motor Vehicle Safety Standards that limit state action and allow manufacturers to design, produce and sell the same vehicles across fifty states. NHTSA is the expert federal agency charged with ensuring that motor vehicles are designed and manufactured to meet safety performance criteria established by the agency; state governments, in contrast, typically focus on issues related to the operation of those vehicles on their roads, such as driver licensing, vehicle registration and insurance.

A strong national policy is therefore critical to the continued development and deployment of connected and automated technologies. Global Automakers has urged NHTSA to act quickly to expand its leadership role in the autonomous vehicle space, and to issue guidance and model policy that are clear and concise, reflect the respective roles of federal and state regulators, and foster the development of these transformative technologies.

D. The Federal Government Should Continue Its Support For The Testing Of Automated And Connected Vehicles

The rigorous testing of automated and connected vehicle systems is critical to ensure that they can be safely deployed and provide drivers with the mobility benefits for which they are designed. In order to test and deploy automated vehicles, the industry will need a variety of different test environments that replicate real-word driving conditions, covering a range of terrain, weather, and climate. Although the current federal and state regulatory frameworks provides sufficient flexibility for testing, the auto industry would welcome federal action to support upgrading existing facilities or construction of new testing facilities that can support the research being undertaken by both NHTSA and industry concerning automated vehicles.

One positive step currently being taken is the recently-announced "Smart City Challenge," which will provide up to $40 million to one city to help it become the country's first city to fully integrate innovative technologies such as connected and automated vehicles into their transportation network. The Department of Transportation received 78 applications in response, and has narrowed the field down to seven finalists.[3] Global Automakers believes that this initiative, and others like it, will be instrumental in the testing and deployment of DSRC-enabled vehicles.

E. The Federal Government Should Support Industry-Led Efforts To Enhance Motor Vehicle Cybersecurity

In addition to creating tremendous benefits, innovation in the automated and connected vehicles brings with it new challenges that must be addressed, one of which is cybersecurity. Cyber-threats in all sectors of the economy are constantly evolving, and the security landscape is therefore dynamic. As NHTSA Administrator Rosekind has recognized, regulators and industry must be nimble and flexible to address rapidly changing technologies.[4]

The auto industry has been working proactively to address motor vehicle cybersecurity. In 2015, the industry established the Automotive Information Sharing and Analysis Center (Auto-ISAC) to share intelligence on immediate threats and vulnerabilities between trusted industry stakeholders, and did so before any real-world cyber incidents materialized. The organization reached initial operating capability and shared the first industry intelligence report

[3] The proposals of each of the finalists, each of which outlines the applicant city's view of the role of DSRC in enhancing mobility, can be found on the DOT's website at: https://www.transportation.gov/smartcity/visionstatements/index

[4] *See* http://www.nhtsa.gov/About+NHTSA/Speeches,+Press+Events+&+Testimonies/remarks-mr-automated-vehicles-07212015

on December 20, 2015. The Auto-ISAC reached full operating capability on January 20, 2016, following the launch of the secure information sharing portal.

In addition, the Association of Global Automakers, Alliance of Automobile Manufacturers, and the Auto-ISAC are currently working collaboratively to develop cybersecurity best practices which will be modelled after the Cybersecurity Best Practices Framework the auto industry published in January of this year.[5] This Best Practices Framework, which was inspired by the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity and other cybersecurity models, provides a foundation for the development of industry-led best practices that will provide greater flexibility to respond in a dynamic technology environment, compared to the traditional regulatory and guidelines models typically used by NHTSA.[6]

These industry-led efforts will result in a robust and nimble framework for protecting against, and responding to, motor vehicle cyber-related threats and incidents. The federal government can support these efforts in several ways. For instance, to the extent that federal authorities are aware of cyber-threats that impact the auto industry, a process could be developed to provide that intelligence to automakers. Additionally, Congress should consider imposing criminal sanctions for hacking into a motor vehicle without the consent of the owner. Finally, the U.S. Copyright Office has recently ruled in favor of several exemptions to the Digital Millennium Copyright Act (DMCA) related to access to automotive software. These exemptions could potentially compromise the cybersecurity (in addition to the safety and emissions performance) of the vehicle. NHTSA and the U.S. Environmental Protection Agency (EPA) are now working with industry to find a way to mitigate the potential negative impacts posed by these exemptions. Global Automakers recommends either eliminating the exemption or sharply limiting it only to uses that do not affect the cybersecurity of the vehicle.

F. The Federal Government Should Support Industry-Led Efforts To Protect Consumer Privacy

Protecting consumer privacy is another area where the auto industry has taken a proactive approach with respect to IoT. Automobiles increasingly are equipped with technologies and services designed to enhance vehicle safety, improve vehicle performance, and augment the driving experience, and many of these technologies and services rely upon information collected from vehicle systems. Sometimes, that information includes the precise location information of vehicles, or information about how drivers operate their vehicles. Automakers recognize that this information, which is critical to safety and the driving experience, deserves protection.

[5] *See* "Framework for Automotive Cybersecurity Best Practices," available at https://www.globalautomakers.org/member/media/press-release/automakers-develop-framework-for-automotive-cybersecurity-best-practices.

[6] Enhancing motor vehicle cybersecurity was an aspect of the "Proactive Safety Principles" announced by NHTSA and eighteen automakers this past January. *See* https://www.globalautomakers.org/member/media/bulletin/dot-and-automakers-announce-proactive-safety-principles

In 2014, automakers established FTC-enforceable privacy principles to protect consumers' personal information.[7] These principles outline the various types of vehicle and driver information that are collected and how this data is used, and they embody the following seven Principles: Transparency; Choice; Respect for Context; Data Minimization, De-Identification & Retention; Data Security, Integrity & Access, and Accountability. They are based on the Fair Information Practice Principles (FIPPs), which have served for over forty years as the basis for privacy frameworks in the United States and around the world. Under the Privacy Principles, personally identifiable information, such as geolocation, driver behavior, and biometric information, is treated with additional heightened protections. All major automakers have committed to putting these standards into practice on all of the vehicles they produce on or after January 2016.

As reflected in the Privacy Principles, automakers believe that the proper use and confidentiality of personal data is necessary in order to promote consumer trust in advanced automotive technologies. Global Automakers welcomes federal action that would foster this trust. For instance, the federal government, particularly Department of Commerce, could continue its commitment to, and support for, self-regulatory models with respect to consumer privacy. Additionally, the federal government could encourage other participants within the connected car ecosystem—such as the manufacturers of after-market devices that connect to the vehicle—to adopt similar consumer protections.

G. Connected And Automated Vehicles Will Have A Significant Positive Impact On The U.S. Economy

The increased deployment of connected and automated vehicles on the road will yield tremendous societal and economic benefits. Enhanced mobility will reduce collisions, and fewer collisions means saved lives, less traffic congestion, and greater productivity. An estimated 90-95% of crashes are attributable to driver error, whether it be from driver impairment, a failure to recognition roadway hazards, or poor decision-making. Advancements in vehicle sensors, communications technology, and vehicle automation have the potential to significantly reduce the occurrence or severity of crashes in the future by helping correct for these errors in human driving.

Traffic accidents impose significant costs on society in terms of lost lives, time and productivity. According to estimates from the National Highway Traffic Safety Administration (NHTSA):

> The price tag for crashes comes at a heavy burden for Americans at $836 billion in economic loss and societal harm. This includes $242 billion in economic costs – nearly $800 for each person living in the United States

[7] *See* http://www.globalautomakers.org/media/papers-and-reports/privacy-principles-for-vehicle-technologies-and-services

> based on calendar year 2010 data — and $594 billion in harm from the loss of life and the pain and decreased quality of life due to injuries.[8]

Increased vehicle automation and connectivity will reduce these costs, and will also add to economic productivity in multiple sectors of the U.S. economy. According to a White Paper undertaken by Morgan Stanley, vehicle automation and connectivity could have a net positive impact of $1.3 *trillion* dollars on the U.S. economy. These benefits stem from accident avoidance, fuel savings, and productivity gains from enhanced mobility and congestion avoidance.[9] These economic impacts underscore the importance of fostering an environment that promotes the research, development and deployment of automated and connected vehicle technologies.

* * *

The Internet of Things has already changed the way Americans live, and will continue to provide new and exciting societal benefits. In the automotive sector, advances in technology will solve significant problems that have persisted since the invention of the automobile—problems such as lives lost and productivity squandered because of accidents and traffic congestion. Industry and federal legislators and regulators should move forward and work collaboratively to encourage innovation and help realize the benefits that new technologies will bring.

[8] *See* http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/NHTSA-study-shows-vehicle-crashes-have-$836-billion-impact-on-U.S.-economy,-society.

[9] *See* http://www.morganstanley.com/articles/autonomous-cars-the-future-is-now.