Harry M. Lightsey III
Executive Director
Global Connected Customer Experience
Global Public Policy

General Motors Company
25 Massachusetts Avenue, N.W.
Suite 400
Washington, D.C. 20001
Phone: 202-775-5039
Fax: 202-775-5054

May 25, 2016

Via E-Mail

National Telecommunications and Information Administration
Attn: IOT RFC 2016
U.S. Department of Commerce
1401 Constitution Avenue N.W., Room 4725
Washington, D.C. 20230

Re: The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, Docket No. 160331306-6306-01

Comments of General Motors, LLC

General Motors, LLC's ("GM") connected and autonomous vehicle technology is at the forefront of the Internet of Things ("IOT"), which has the capability to provide significant societal benefits. These comments focus on the National Telecommunications and Information Administration's ("NTIA") threshold inquiry on "the potential benefits and challenges of these technologies and what role, if any, the U.S. Government should play in this area."[1] We provide our view in the context of autonomous and connected vehicle technology.

I. GM IS AT THE FOREFRONT OF BRINGING THE BENEFITS OF AUTONOMOUS AND CONNECTED VEHICLES TO CONSUMERS

Autonomous and connected vehicles are part of a growing and evolving IOT. In fact, the connected vehicle already is a reality, and in-vehicle wireless connectivity is rapidly expanding from luxury models and premium brands to high-volume and mid-market models. By 2020, one in five vehicles will have some sort of wireless network connection, accounting for more than a

[1] National Telecommunications and Information Administration, Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, 81 Fed. Reg. 19956, 11956 (Apr. 6, 2016).

quarter of a billion cars on global roads.[2] Moreover, the market for connected vehicles is projected to reach $54 billion in the next two years alone.[3]

The attributes of autonomous and connected vehicle technology provide a compelling illustration of IOT's potential benefits. The modern vehicle has numerous electronic control units, or ECUs, that operate on millions of lines of computer code. With this tremendous computing capability—and connectivity—great opportunities for innovation exist, creating the potential to transform transportation by making it safer and more accessible. Not only can a networked vehicle include internal sensors that determine such things as speed, location, or temperature of the vehicle, but it also may interact with surrounding roads, buildings, and other vehicles to provide up-to-the-minute information to improve safety and avoid traffic.

GM is fully embracing this IOT technology, building upon its longstanding leadership in this area. GM is a global leader in connected and autonomous vehicles, delivering innovative services that are enhancing the overall ownership experience for customers. In fact, GM has led the industry in delivering connected vehicle services since the launch of OnStar in 1996. Today, OnStar serves more than 7 million customers in the U.S., Canada, China, Mexico, Europe, and Brazil. OnStar's suite of services include, among other things, automatic crash response, stolen vehicle assistance, remote door unlock, turn-by-turn navigation, vehicle diagnostics, hands-free calling and, through a partnership with AT&T, 4G LTE wireless connectivity.

OnStar's emergency services and automatic crash notification have helped prevent loss of life, underscoring GM's commitment to safety. OnStar's automatic crash notification service helps to automatically alert a call center advisor when certain crashes occur so they can provide help. In most situations, even if the driver is unable to speak, the advisor can use GPS technology to send emergency responders to the crash location. OnStar also has technology that can inform first responders about crash details to help them assess the likelihood of severe injuries. Today, OnStar handles on average two calls every second, 185,000 calls per day, and four million requests for assistance every month, including 100,000 emergency responses and 5,000 automatic crash responses every month.

GM, through a partnership with AT&T, also offers 4G LTE connectivity on more than 30 vehicle models. The bandwidth of 4G LTE allows the provision of a Wi-Fi hotspot in the vehicle. In the future, this platform will make more capabilities and services available to customers, and will further enhance their driving experience.

GM also continues to expand OnStar's Remote Link app that allows vehicle owners to perform a remote start from a long distance on a cold day or quickly unlock a vehicle with the keys locked inside. Electric vehicle owners can even use the Remote Link app to decide when they want to charge their batteries, potentially saving money and load on the power grid. All of these connected vehicle features improve the driving experience and increase safety and security.

[2] Laruen Davidson, The Telegraph, "How Connected Cars are Driving the Internet of Things" (Jan. 27, 2015).

[3] Smriti Tuteja, Hackerearth, "Connected Car Revolution in Automotive Industry" (Apr. 13, 2016.

In addition to its connected vehicle innovations, GM has a long history with autonomous vehicle research and is leading in promoting autonomous driving technologies. Recent statistics indicate that more than two million vehicle crashes occur annually in the United States. These crashes result in over 32,000 fatalities and significantly more injuries and property damage each year.[4] According to the most recent government data, more than 94 percent of these crashes are caused by human error.[5] Autonomous driving systems ("ADS"), specifically Level 4 and Level 5 ADS as defined by SAE J3016,[6] can dramatically increase public safety by removing human error. In addition, increased ADS vehicle utilization holds significant positive environmental and economic benefits, including reduced traffic congestion, elimination of unnecessary vehicle idling, and more efficient route choices. The technology also has the potential to create increased independence through mobility for the disabled and elderly communities.

GM is not doing this alone. The next phase of automotive innovation must include diverse business models, new technology, and evolving consumer interests. GM's recent investment in the ride-sharing company Lyft complements its expertise in autonomous vehicles by providing a ride-sharing platform to support potential deployment programs. GM's acquisition of Cruise Automation, a developer of autonomous-driving technology, is another important milestone in its work to deploy autonomous vehicles. Cruise's software expertise and rapid development capability will further accelerate GM's progress in autonomous vehicle technology.

Finally, GM also expects to be the first automaker to bring Dedicated Short Range Communications, or DSRC, Vehicle to Vehicle ("V2V") safety technology to market late this year in the 2017 Cadillac CTS. This technology will enable vehicles to communicate important safety and mobility information to one another to help avoid or mitigate a crash. V2V has huge safety potential—the National Highway Traffic Safety Administration ("NHTSA") estimates that once all vehicles are equipped, V2V could potentially mitigate 80 percent of non-impaired crashes, reducing costs to our nation's economy by $871 billion each year.[7]

II. GOVERNMENT SHOULD PROCEED CAUTIOUSLY IN A NASCENT LANDSCAPE AND ALLOW INNOVATION TO FLOURISH IN THE AREAS OF AUTONOMOUS AND CONNECTED VEHICLES

Connected and autonomous vehicle technology offers tremendous societal benefits. Transformative technologies, however, may beget new policy challenges. The NTIA's request for comments appropriately notes many of the challenges facing IOT and, in particular, autonomous and connected vehicles. For these comments, GM focuses specifically on the safe and expeditious deployment of autonomous vehicles, on cybersecurity and data privacy, and on protection of the road safety spectrum necessary to operate V2V technology.

[4] http://www.iihs.org/iihs/topics/t/general-statistics/fatalityfacts/overview-of-fatality-facts

[5] National Highway Traffic Safety Administration, Traffic Safety Facts, "Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey" (Feb. 2015).

[6] *See* SAE International Standard J3016.

[7] *See* National Highway Traffic Safety Administration, "The Economic and Societal Impact of Motor Vehicle Crashes, 2010 (Revised)," DOT HS 812 013 (May 2015).

A. Publicly Authorized "SAVE" Projects Will Bring the Benefits of Autonomous Vehicle Technology to Consumers in a Safe and Timely Manner

One of the principal benefits of autonomous technology is safety. Self-driving vehicles promise to reduce traffic-related death rates by taking the biggest risk out of the equation—the human behind the wheel. Computers do not get tired or distracted. At the same time, no technology is completely failsafe. GM recognizes and appreciates the need to address ADS safety concerns from the outset in order to achieve the full potential of autonomous vehicle technology. Indeed, one of the most important policy challenges for autonomous vehicles will be to ensure that societal benefits are realized quickly while implementing this new technology in a safe and controlled manner.

Federal and state governments can encourage the safe and rapid development and deployment of ADS technology by authorizing Shared Autonomous Vehicle ("SAVE") projects in geographically bounded areas that might include urban residential areas, business districts, or university campuses. Publicly available on-demand ridesharing, car sharing, or similar platforms will help ensure that ADS technology is rapidly scaled to realize the full safety, environmental, and economic potential that the technology promises. In addition, SAVE projects' higher vehicle utilization rate—compared to public operation of household vehicles—will efficiently accumulate data that may be used by policymakers and others to assess autonomous vehicle safety and to inform further policy initiatives. SAVE projects also will provide the public with access to ADS technology without requiring a significant financial investment, which could speed public acceptance while at the same time protecting public safety through controlled roll-outs. This real-world pilot approach also will foster the development of regulatory best practices, which can serve as a model for consistent state regulations that complement federal authority and remove unnecessary obstacles to deployment.

Of course, safety considerations must be at the forefront of any autonomous vehicle initiative, including for SAVE projects. The following safeguards for SAVE projects, taken together, will encourage safe and timely deployments of ADS technology:

- Only vehicles owned or controlled by an entity that has previously manufactured and distributed vehicles certified to federal motor vehicle safety standards should be allowed to participate.

- A participating motor vehicle manufacturer should be responsible for integrating ADS technology into the vehicles and for the safe operation of SAVE projects.

- Participating vehicles should meet all safety requirements, including that they be operated to comply with all federal, state, and local laws.

- Vehicles should be equipped with event data recorders and be capable of providing automatic crash notification to emergency responders.

- Once data from SAVE projects appropriately demonstrate superior safety performance, SAVE project vehicles should be permitted to function without human intervention in the vehicle. ADS technology without human intervention presents the greatest potential to reduce human error that results in vehicle crashes and fatalities. It follows that in this scenario, the ADS technology should be considered the operator for purposes of assessing conformance to applicable laws and regulations.

SAVE projects present the next logical step toward public availability of high-level autonomous vehicles. GM encourages federal and state policymakers to further policy initiatives to accelerate the development and adoption of safe, high-level vehicle automation through real-world SAVE projects. Indeed, governments around the world are moving forward and establishing regulatory structures to encourage the testing of autonomous vehicles on their streets. The United Kingdom, for example, places no geographical limitations on tests, does not require special licenses or permits, and is opting not to require additional insurance.[8] An enabling environment for ADS in the United States will be critical to our national competitiveness in this space.

B. Prescriptive Cybersecurity Regulation Would Hamper Ongoing, Proactive Industry Efforts

For autonomous and connected vehicle technologies to deliver on their promise, they must earn the absolute trust of customers and the public that they will work as designed over the life of the vehicle. This includes protecting against cybersecurity threats. However, prescriptive, top-down cybersecurity regulation at this time would hamper proactive industry collaborations that already are addressing these risks. Numerous efforts are underway in the automotive sector and other standards bodies to address the myriad technical and operational issues that impact IOT innovation. Automakers should be free to develop and choose solutions that appropriately protect against cyber threats and that best fit both the needs of the product and the demands of automotive safety, as these factors evolve.

A voluntary, collaborative approach is a more meaningful mechanism for the promotion of cybersecurity than top-down regulation. Cybersecurity risks and responses are constantly evolving, and there is no single solution or set of requirements or standards. In fact, due to the rapidly changing nature of the cyber threat landscape, predefined, top-down cyber standards quickly could become obsolete. A better approach to address IOT cybersecurity challenges is through voluntary risk management, collaboration, and information sharing.

To that end, GM has devoted substantial resources and taken significant organizational and technical measures to respond to potential cybersecurity threats. GM takes a multi-layered approach to cybersecurity and is designing vehicle systems that can be updated with enhanced security measures as potential threats evolve. In this way, GM proactively is anticipating and addressing evolving cybersecurity challenges involving vehicles. Some examples of GM's cybersecurity efforts include the following:

- GM was the first auto manufacturer to create an integrated and dedicated global organization focused on minimizing the risks of unauthorized access to vehicles

[8] *See* Alex Davies, WIRED, "The UK Just Made Itself a Fantastic Place to Test Self-Driving Cars" (Feb. 12, 2015).

and customer data. Jeff Massimilla, GM's Chief Product Cybersecurity Officer, has responsibility for the end-to-end cybersecurity of our vehicles and vehicle connected services.

- GM has collaborated with experts in the defense and aerospace industries, government organizations, academia and industry consortiums on best practices and key lessons.
- GM has launched a Security Vulnerability Disclosure Program through which security researchers, who are not already working with GM, find security bugs or vulnerabilities related to our products or services can inform GM via a secure website portal.

The automotive industry as a whole also has taken a proactive, as opposed to reactive, approach to cybersecurity, including sharing vehicle threat and vulnerability information to encourage appropriate safeguards. For example, automakers formed the Automobile Industry Information Sharing and Analysis Center ("Auto ISAC") in July 2015 to serve as the central point for the analysis and sharing of cyber threat information.[9] GM is an active participant, and Jeff Massimilla is the Vice Chairman of the Auto ISAC Executive Committee. GM and the industry have also published a Framework for Automotive Cybersecurity Best Practices,[10] and are working towards industry best practices. GM also leads the Society of Automotive Engineers ("SAE") cybersecurity committee which includes other OEMs and suppliers where cybersecurity practices are discussed and standards are developed. Finally, GM is engaged with other domestic and international industry consortia on cybersecurity practices and procedures.

This is not to say that government should be sidelined on cybersecurity issues. Regulators, non-regulatory experts like NIST, and entities like NTIA can play an important role in the development of cybersecurity solutions, best practices, and standards by encouraging industry to collaborate in the development of open, voluntary and consensus based standards. Government can also assist the private sector by sharing information and promoting a culture of voluntary efforts to raise the bar. The NIST Cybersecurity Framework illustrates the benefits of this approach. The NIST Cybersecurity Framework is based upon the understanding that security is not static and a single prescriptive approach is not appropriate in the cybersecurity context. Thus, a voluntary framework of ongoing risk assessment is the best model to address cybersecurity. GM supports the NIST Cybersecurity Framework and bases its sophisticated cybersecurity program, in part, upon the Framework's tenets.

[9] Current Auto ISAC members include BMW, FCA, Ford Motor Co., General Motors, Hondo Motor Co., Hyanai, Kia, Mazda, Mercedes, Mitsubishi, Nissan, Subaru, Toyota, Volkswagen. This membership represents more than 98 percent of cars on the road in North America.

[10] *See* http://www.autoalliance.org/index.cfm?objectid=E5E3C2B0-BEC2-11E5-9500000C296BA163.

C. Regulators Should Allow the IOT Market to Develop Within the Existing Consumer Privacy Framework

Privacy is a legitimate concern, but not a novel one. At this stage, it is unclear whether or how nascent IOT markets heighten privacy concerns for consumers. Rather than rush to action prematurely, regulators should allow IOT to develop within the clear rules of the road that already exist to protect consumer privacy. As the Federal Trade Commission ("FTC") has cautioned, IOT-specific legislation may stifle IOT innovation and even penalize companies that attempt to implement reasonable privacy measures.[11]

It is unclear what unique IOT privacy issues connected vehicle services present, if any. While some connected vehicle services may involve the collection, storage, and sharing of data, much of this activity will not implicate consumer privacy in any way. The very nature of some services will be to leverage data in which there is no cognizable privacy interest, *e.g.*, exhaust system performance or fuel efficiency. Other services will access consumer data but will provide clear consumer benefits. Consumers gladly will share information where they are provided notice and choice, and the value proposition is clear. Connected vehicle services are no different in this respect than many existing technologies and services.

GM agrees with the conclusion of the FTC's Staff Report on IOT, which does not yet see a need for regulators to aggressively step in and regulate IOT privacy.[12] At this stage, regulation, which by its nature is inflexible and rarely technology-neutral, could stifle innovation. Rather, the onus should be on device makers to build features that safeguard consumers and their data, where appropriate, and to communicate appropriate information to consumers. As the Staff Report recognizes, some data uses are generally consistent with consumers' reasonable expectations, and providing choices for every instance of data collection is not necessary to protect privacy.[13] Moreover, to ensure that privacy efforts are appropriately focused on potential harms, regulators' interest in IOT should be limited to *consumer* IOT devices – enterprise or business-focused devices should be cordoned off from regulatory scrutiny.

For its part, GM designs its vehicles with consumer privacy expectations in mind. Indeed, GM works to ensure that its customers are notified of data collected and how it will be used. OnStar is GM's primary mechanism for collection of vehicle data. The OnStar User Terms and Privacy Statement implemented across our customer-facing channels are designed to provide customers with clear, meaningful descriptions of applicable data policies and practices. GM publishes its policies in order for consumers to make informed choices about products and services. It is also GM's practice to obtain opt-in consent for any services that may fall outside those described in the OnStar User Terms and Privacy Statement. Similarly, customers can cancel connected services at any time. Upon cancellation, data is no longer collected.

[11] *See* Federal Trade Commission, Staff Report, "Internet of Things: Privacy and Security in a Connected World" (January 2015) ("FTC IOT Staff Report").

[12] FTC IOT Staff Report at 48.

[13] FTC IOT Staff Report at 40.

The automotive industry also has responded to rapidly evolving technology by developing and voluntarily adopting industry best practices and guidelines to protect privacy. In November 2014, the Alliance of Automobile Manufacturers, Inc. and the Association of Global Automakers, Inc. published the Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services.[14] These principles are based upon the Fair Information Practice Principles ("FIPPs") and relate to the collection, use, and sharing of personal and vehicle information associated with vehicle technologies that collect, generate, record, and store this information. The principles call for automakers and manufacturers to ensure the following by 2017:

- Provide consumers with clear notice and choice in the use and collection of personal information;
- Use personal information in a way that is consistent with the context in which it was collected;
- Collect information only as legitimately needed, and retain it only for as long as necessary;
- Implement reasonable data security measures;
- Maintain the accuracy of the data, and provide access to users; and
- Remain accountable to consumers for adherence to these principles.

Participating companies have committed to taking reasonable steps to ensure that they and other entities that receive relevant information adhere to these principles. These voluntary guidelines are meaningful commitments that will promote sound privacy practices within the auto industry while also ensuring that important autonomous and connected vehicle technology is brought to the public in a timely and complete manner. This effort shows that the private sector can and should lead the way on developing practical, flexible approaches that assist consumers.

D. Regulators Must Ensure the Availability and Protection of Road Safety Spectrum

As noted above, GM expects to be the first automaker to bring V2V technology to market late this year in the 2017 Cadillac CTS. GM believes that V2V is an exciting safety technology that could dramatically improve vehicle safety. The process is going to involve a rapid learning cycle for GM and for the industry as a whole, and GM applauds the federal government for wanting to do everything it can to facilitate the application of this technology as quickly, and as safely, as possible.

[14] Privacy Principles for Vehicle Technologies and Services (Nov. 13, 2014), *available at* http://www.globalautomakers.org/media/papers-and-reports/privacy-principles-for-vehicle-technologies-and-services.

V2V systems are on the brink of widespread deployment, and the U.S. government must ensure the availability of spectrum to support safety-critical V2V communications. The Federal Communications Commission ("FCC") has allocated 75 MHz of spectrum at 5.850-5.925 GHz to the mobile service for use by DSRC systems operating in the Intelligent Transportation System radio service ("Road Safety Spectrum").[15] In making this allocation for DSRC, the FCC noted that DSRC and V2V applications are a key element in meeting the nation's transportation needs and in improving the safety of our nation's highways.[16] Indeed, as noted above, NHTSA estimates that the technology could mitigate up to 80 percent of the over four million annual unimpaired vehicle crashes saving thousands of lives and reducing the $871 billion cost to our nation's economy each year.

However, the availability of much-needed spectrum for V2V communications is now under threat from proposals seeking to open the 5.9 GHz band for sharing with unlicensed Wi-Fi users.[17] To be clear, GM does not oppose sharing the 5.9 GHz band so long as sharing is done without harmful interference to V2V spectrum and without significantly disrupting DSRC deployment. In fact, automakers have been begun testing a sharing proposal that may enable Wi-Fi devices to operate in the 5.9 GHz band without causing harmful interference to DSRC units operating in the same area. However, further testing is needed to identify the best and most secure approach to protecting V2V communications and avoiding interference. In the meantime, it is critical that the spectrum allocated for V2V should not be opened for use by (or sharing with) unlicensed Wi-Fi users until testing conclusively establishes that sharing will not adversely impact or interfere with the operation of V2V systems.

Interference will impair our collective ability to achieve the important benefits that the FCC and NHTSA have so clearly stated. With so much at stake, GM urges policymakers to proceed extremely cautiously with any proposed sharing of the Road Safety Spectrum. While sharing the 5.9 GHz band remains a strong possibility, it is extremely important that sharing not be allowed until all measures have been taken to ensure the viability and promise of V2V technology.

[15] *See Amendment of Parts 2 and 90 of the Commission's Rules to Allocate the 5.850-5.925 GHz Band to the Mobile Service for Dedicated Short Range Communications of Intelligent Transportation Systems,* Report and Order, 14 FCC Rcd 18221 (1999).

[16] *Id.* at ¶ 9.

[17] *See, e.g.*, Letter to President Barack Obama, available at http://glenechogroup.isebox.net/wififorward/sharing-spectrum-for-gigabit-wi-fi?default=wjT98ye0.

III. CONCLUSION

Autonomous and connected vehicles hold enormous opportunity for businesses, consumers, and the country. GM is committed to working with the U.S. government, as well as other stakeholders, to continue promoting a reasonable and effective regulatory framework for autonomous and connected vehicles, and for IOT generally, that encourages innovation and consumer confidence.

Respectfully Submitted,

/s/ Harry Lightsey

Harry Lightsey
Executive Director, Connected Customer, Public Policy