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

September 2, 2016

Via E-Mail

Ms. Nakia Grayson
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
cybercommission@nist.gov

Re: Input to the Commission on Enhancing National Cybersecurity/Comments in Response to Request for Information, Docket Number: 160725650-6650-01

Comments of General Motors, LLC

I. INTRODUCTION AND BACKGROUND

General Motors LLC ("GM") respectfully submits these comments in response to the proceeding referenced above. GM appreciates the opportunity to highlight its cybersecurity efforts, and to offer its view regarding how the federal government can best promote increased cybersecurity in the automobile industry.

GM is a global leader in connected and autonomous vehicles, delivering innovative services that are enhancing safety and the ownership experience for customers. In fact, GM has led the industry in delivering connected vehicle services since the launch of OnStar in 1996. For example, OnStar's emergency services and automatic crash notification have helped save lives consistent with 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 facilitate first responder assistance. In most situations, even if the driver is unable to speak, the advisor can use GPS location technology to send emergency responders to the crash location.

In addition to its connected vehicle innovations, GM has a long history with autonomous vehicle research and is leading in promoting autonomous driving technologies. GM's recent investments in the ride-sharing company Lyft and Cruise Automation, a developer of autonomous-driving technology, demonstrate its leadership commitment. Autonomous and connected-car technology has the potential to significantly improve mobility and safety for all people. It is important to

note that 94% of all vehicle crashes are caused by driver error. The great promise of highly automated technology is that it has the potential to drastically reduce that number.

GM also expects to be the first automaker to bring Dedicated Short Range Communications ("DSRC"), or Vehicle to Vehicle ("V2V") safety technology to the U.S. in its Model Year 2017 Cadillac CTS. V2V also has huge safety potential—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.

These examples illustrate the promise of technological advances and vehicle connectivity. For these technologies to deliver on their promise, they must earn our customers' trust that they will work as designed. This includes protecting against potential cybersecurity threats. To that end, General Motors continues to prioritize the cybersecurity of its products and systems, and is grateful for the opportunity to highlight these efforts below.

II. GM'S CYBERSECURITY EFFORTS

GM has devoted substantial resources and taken wide ranging organizational and technical measures to address cybersecurity. In fact, GM was the first auto manufacturer to create an integrated and dedicated global organization focused on minimizing the risks of unauthorized access to vehicles 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 bases its organization and program upon the National Institute of Science and Technology ("NIST") Framework for Improving Critical Infrastructure Cybersecurity, released in early 2014. The NIST Framework, along with other resources, serves as a guide to industry as it addresses cybersecurity threats. GM utilizes the NIST Framework to cover development and production phases of the vehicle lifecycle and provides milestones for review, analysis, testing, and vulnerability remediation.

GM takes a multi-layered approach to cybersecurity and utilizes a security by design approach. For example, GM is now designing vehicle systems that can be updated with enhanced security measures as potential threats evolve. GM also continues to collaborate with experts in other industries, government organizations, academia and industry consortiums on key lessons and best practices. A GM employee also leads the Society of Automotive Engineers Vehicle Electrical Systems Security Committee, which includes other OEMs and suppliers, where cybersecurity practices are discussed and standards are developed. GM has also launched a Security Vulnerability Disclosure Program through which security researchers who find potential vulnerabilities related to GM products can inform GM via a secure website portal.

The automotive industry as a whole also has taken a proactive approach to cybersecurity. An example of these efforts include the Automobile Industry Information Sharing and Analysis Center ("Auto ISAC") formed in July 2015. The Auto ISAC provides for the analysis and

sharing of cyber threat information among almost all major U.S. automobile companies.[1] GM is an active participant, and Jeff Massimilla is the Vice Chairman of the Auto ISAC Executive Committee.

The Auto ISAC also recently published its Automotive Cybersecurity Best Practices Executive Summary in addition to the industry's previously published Framework for Automotive Cybersecurity Best Practices.[2]

The industry also designed DSRC and V2V technology with cybersecurity at the forefront. With input from multiple stakeholders, the V2V system utilizes public infrastructure security and contains multiple technical, physical, and organizational controls to guard against cybersecurity threats.

It is clear that GM and the industry have made significant strides in addressing vehicle cybersecurity, and these proactive measures were accomplished through voluntary collaborative efforts that allow the flexibility to adjust to an ever changing threat landscape.

III. THE FEDERAL GOVERNMENT SHOULD CONTINUE TO FOSTER COLLABORATIVE INDUSTRY EFFORTS TO ADDRESS EVOLVING CYBERSECURITY RISKS

Consistent with its experience described above, GM believes that a proper role for the federal government is to foster a voluntary flexible and collaborative approach to further cybersecurity in the automobile context. Such an approach would further the ongoing proactive measures taken by GM and the industry. Regulators and entities such as NIST and NTIA play a vital role in furthering these solutions through industry and cross-industry efforts. The NIST Cybersecurity Framework utilized by GM illustrates how well these mechanisms can work. The Auto ISAC and industry best practices and collaborations are further examples.

A prescriptive, top-down cybersecurity regulatory approach, on the other hand, would hinder ongoing efforts by the auto industry to address cybersecurity risks. Cybersecurity threats and responses to them are constantly changing, and there is no single binding solution or set of requirements that would be effective. Rather, predefined, top-down cyber standards or regulations would likely become obsolete very quickly.

The preferable approach to address these challenges is through the voluntary risk management, collaboration, and information sharing efforts currently taking place within the industry. Automakers should be free to develop and choose solutions that appropriately protect against

---

[1] Current Auto ISAC members include BMW, FCA, Ford Motor Co., General Motors, Honda 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.

[2] See http://www.autoalliance.org/index.cfm?objectid=E5E3C2B0-BEC2-11E5-9500000C296BA163; https://www.automotiveisac.com/best-practices/

constantly changing cyber threats. It is important that the industry design solutions that best fit both the needs of the product and the demands of automotive safety, as these factors evolve.

IV. CONCLUSION

Autonomous and connected vehicles hold enormous potential to greatly improve society particularly with safety. GM is committed to working with the U.S. government, as well as other stakeholders, to continue an effective regulatory framework for autonomous and connected vehicles in the context of cybersecurity.

Respectfully Submitted,

/s/ Harry Lightsey

Harry Lightsey
Executive Director, Connected Customer, Public Policy