General Motors Company
25 Massachusetts Avenue, N.W.
Suite 400
Washington, D.C. 20001
Phone: 202-775-5080
Fax: 202-775-5023

Marlene H. Dortch
Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Re: Petition for Rulemaking and Request for Emergency Stay of Operation of Dedicated Short-Range Communications Service in the 5.850-5.925 GHz Band (5.9 GHz Band); RM 11771 (Petition)

Dear Ms. Dortch:

On behalf of General Motors Company (GM), this *ex parte* notice memorializes a meeting between representatives of GM and Commission staff. On Tuesday, September 13, 2016, Jeff Massimilla, Chief Product Cybersecurity Officer; Kevin Tierney, Director of Vehicle Architecture Cybersecurity; Luke Simon (participating by phone), Lead Counsel; Andrew York, Executive Director of Federal Affairs; Rich Lopez, Director of Federal Affairs; and Susan Buck of The Fritts Group, LLC., met with Admiral David Simpson, Nicole McGinnis, Jeffery Goldthorp and Peter Shroyer of the Public Safety and Homeland Security Bureau; Jon Wilkins, Charles Mathias, and Charles Eberle of the Wireless Telecommunications Bureau; and Julius Knapp of the Office of Engineering and Technology. The purpose of the meeting was to discuss broadly the numerous actions GM has taken and continues to take to secure vehicle architecture, telematics, and the connected vehicle ecosystem from cybersecurity vulnerabilities and to further discuss GM's efforts and experience working with others in the automotive industry on these topics.

In 2014 GM created a global organization within the company, Product Cybersecurity, which consolidated cybersecurity functions for product development and connected services into a centralized, well-resourced organization, with senior level leadership. Since its creation, it has quickly grown and matured. GM was the first automaker with this type of integrated and dedicated global product cybersecurity organization, and this team collaborates with outside specialists and third parties with a mission of minimizing the risk of unauthorized access to vehicles and the customer data in vehicles. The guiding principles of the organization are based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Mr. Massimilla and Mr. Tierney gave a lengthy overview of the actions GM takes in carrying out the mission of the Product Cybersecurity organization. They include:

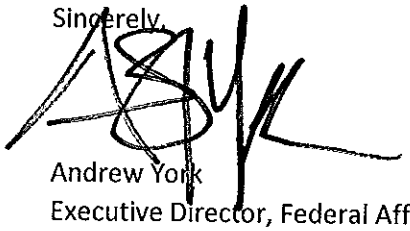
- security by design for GM products from the earliest days of development throughout the manufacturing process;
- defense in depth strategies with multiple layers of defenses presented to attack surfaces of cyber critical systems;
- work with security researchers, including the GM Security Vulnerability Disclosure Program, through which security researchers can inform GM of bugs or vulnerabilities via a secure website portal;
- vendor and supply chain management, including engaging with suppliers to provide education and training on how to minimize risk; and
- external collaboration with experts in the defense and aerospace industries, government organizations, academia and industry consortiums on best practices and key learnings.

Mr. Massimilla and Mr. Tierney also described the recently created Automotive Information Sharing and Analysis Center (Auto ISAC), of which GM is a member. The Auto ISAC was created for Original Equipment Manufacturers and suppliers as an industry-operated environment created to enhance cyber security awareness and coordination across the global automotive industry. They explained that the Auto ISAC to date has been successful because of the willingness of members to share threat and vulnerability information. In July, the Auto ISAC released an Executive Summary identifying cybersecurity "best practices" for the auto industry, that builds upon the Proactive Safety Principles agreed to by the auto industry and the Department of Transportation. Mr. Massimilla explained that GM supported and endorsed all recommendations in the Executive Summary and committed to implementing the actions and best practices outlined in the document.

In response to questioning, Mr. Massimilla urged the Commission to consider the implications of the Petition that could have the potential to delay the deployment of life saving technologies, such as Dedicated Short Range Communications (DSRC). He cautioned the Commission that prescriptive rules and regulations that would be potentially outdated by the time they were published could actually hinder cybersecurity rather than enhance it. Instead, he stressed an emphasis on risk management and cross industry and governmental collaboration as an appropriate approach to cybersecurity. He noted the interaction between GM, the auto industry, and the National Highway Traffic Safety Administration (NHTSA). He stressed that NHTSA, as a safety regulator of the auto industry, is developing best practices in cybersecurity and is in regular communication with OEM's regarding cybersecurity topics. Mr. York noted that NHTSA interprets its authority to include cybersecurity–related safety of motor vehicles and equipment and that a safety recall due to cybersecurity vulnerabilities has already occurred. Furthermore, he stressed that OEM's have a statutory obligation to report any defect in vehicles affecting safety, including those due to cybersecurity vulnerabilities. In addition, the Federal Trade Commission (FTC) has used its authority under Section 5 of the FTC Act to exercise oversight of cybersecurity incidents affecting privacy. Because of the comprehensive nature of regulatory oversight that already exists, he pointed out that additional regulations and oversight by the Commission was unnecessary.

This letter is being filed electronically pursuant to Section 1.1206 of the Commission's rules. Should you have any questions, please contact the undersigned.

Sincerely,



Andrew York
Executive Director, Federal Affairs