U.S. Department of Justice

Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

National Highway Traffic Safety
Administration
1200 New Jersey Avenue SE
Washington, DC 20590

May 1, 2017

Re: Connected Cars Workshop, Project No. P175403

Thank you for inviting public comments in advance of the June 28, 2017 workshop examining the consumer privacy and security issues posed by connected vehicles. We at the United States Department of Justice (the "Department") work every day to protect the American people from cyber threats and to uphold their privacy rights online. This is a multifaceted, coordinated, and sustained effort. Last year, we were glad to participate in the NHTSA Cybersecurity Roundtable to discuss how cybersecurity may be improved over a vehicle's lifecycle. We are now similarly pleased to have an opportunity to provide our perspective on how to ensure that these exciting innovations in personal mobility continue to advance.

The era of Internet-connected vehicles holds tremendous promise for a safer, more efficient, and increasingly integrated transportation sector. Inter-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication systems, and increasingly autonomous vehicles, are only some of the many emerging technologies that will potentially reduce traffic congestion, improve public safety, and avoid many collisions caused by human error.

As with similar innovations, there will also be novel security challenges. Sophisticated cybercriminals interested in accessing personal data will seek to target vulnerable systems wherever they find them, and so it can be expected that they will test the interfaces of connected vehicles with other vehicles, infrastructure, and the world. Furthermore, we will need to consider risks associated with (and the security of) the back-end systems that not only aggregate information from vehicles and infrastructure, but also rely on that information to direct vehicles or dynamically adjust the infrastructure. To mitigate the cybersecurity costs of emerging vehicle technologies, relevant public and private stakeholders must work collaboratively and proactively to minimize their data security vulnerabilities and to combat cybercriminals and other bad actors seeking to exploit them.

Like you, the Department is committed to advancing the privacy and safety of drivers, passengers, and owners of connected cars. For our part, the Department is working with the automotive industry and other private- and public-sector partners to identify and combat cyber threats; to help to disseminate information about effective defensive measures against those threats; and to investigate, attribute, and prosecute cybercriminals who seek to compromise networks and information on computer systems. Through effective public-private cooperation,

we are disrupting, deterring, and mitigating significant data breaches by even sophisticated transnational organized cybercriminals.

Towards that end, and in accordance with the Cybersecurity Information Sharing Act of 2015 ("CISA"), the Department has played a critical role in developing a set of policies and procedures to help the private sector better share indicators of cyber threats and defensive measures with the federal government. The Department encourages members of the automotive industry to study and take advantage of these policies and procedures, which are available on the Department of Homeland Security's website at https://www.us-cert.gov/ais. In addition to promoting the public-private cooperation vital to all cybersecurity, this guidance will help members of the automotive industry secure CISA's liability protections and other statutory safe harbor advantages that come with the authorized sharing of cybersecurity information. Further, when incidents do occur, affected entities that promptly report breaches may also receive the benefit of cyber threat intelligence from law enforcement to mitigate the incident and combat future threats. As of April 2017, more than 296,000 unique cyber indicators had been sent out to participants of the CISA program.

Because the general public also serves as an important line of defense against cybercriminals, the Department will continue to build upon intergovernmental efforts to help consumers maintain their vehicle privacy and security. For instance, the Public Safety Announcement produced by the FBI and NHTSA entitled *Motor Vehicles Increasingly Vulnerable to Remote Exploits* helps to inform consumers of past and potential vehicle vulnerabilities and recommends some easy steps for minimizing vehicle cybersecurity risks. *See* Alert No. I-031716-PSA, https://www.ic3.gov/media/2016/160317.aspx (March 17, 2016).

The Department supports the efforts of FTC and NHTSA to protect the security of current and emerging vehicle technologies. We look forward to working with you, the automotive industry, and the general public as these issues are explored, both at the upcoming workshop and beyond.