United States Senate
WASHINGTON, DC 20510

July 28, 2015

The Honorable Dr. Mark Rosekind
Administrator
National Highway Traffic Safety Administration
1200 New Jersey Avenue, SE, West Building
Washington, D.C. 20590

Dear Administrator Rosekind:

We write concerning the shocking revelations that a software defect in cars may enable hackers to remotely access critical vehicle controls through the information and entertainment systems. Security experts have now demonstrated that it is possible to disable or control vital vehicle systems such as the engine, braking system, steering, and transmission – all from a wireless computer that could be located anywhere. We were deeply troubled to learn that these software defects can be exploited by malicious hackers to potentially wreak havoc on our roads. And we were also stunned to learn that despite being aware of this vulnerability for almost 9 months, Fiat Chrysler Automotive (FCA), the manufacturer of the 2014 model Jeep Cherokee featured in *Wired*'s article, only recalled the 1.4 million impacted vehicles last week after the publication of the article in question. These revelations highlight the acute risks now facing modern motorists as automakers continue to connect cars ever closer to the digital world.

We urge the National Highway Traffic Safety Administration (NHTSA) to take all necessary steps to address this unprecedented safety threat and protect American drivers. To restore consumer confidence in our nation's auto safety system it is imperative that NHTSA act quickly to develop a fuller understanding of the breadth and depth of the safety threat now confronting motorists. NHTSA must rapidly determine whether other vehicle models are affected by this particular vulnerability, and how remedial actions can be deployed by manufacturers and regulators to secure all vehicles on our roads.

We have serious concerns that regulators and manufacturers have only exposed the tip of this iceberg – Americans do not yet know if FCA's vehicles are the only models to suffer from the security vulnerabilities recently exposed. While NHTSA recently asked the supplier of these vulnerable components to issue information on this particular vulnerability to all of the automakers that it supplies, our concerns are not only with the vehicles suffering from a vulnerability similar to the FCA recall, but with all of the millions of increasingly-connected vehicles on the roadways and the additional vulnerabilities that may exist within them.

Modern vehicles are continuously expanding and advancing their connectivity–incorporating advanced systems for navigation, vehicle-to-vehicle communication, and infotainment. We expect that the number of potential attack surfaces in modern vehicles will only increase, and we are only just beginning to understand the nature of the emerging threat posed by car-hacking. Until we can identify all vulnerable systems and vehicles, car-hacking will continue to present a critical threat to the safety of drivers, passengers, and road users.

We strongly urge NHTSA to conduct an investigation to determine whether there are other vehicles currently on American roads that suffer from similar or entirely new security and safety defects and to determine whether additional recalls should be issued. In addition, we urge NHTSA to endorse our legislation that calls for the development of cybersecurity standards for all new motor vehicles that will help prevent future vulnerabilities and recalls that endanger millions on our roadways. While the Internet of Things has improved the driving experience for countless Americans, those same consumers deserve the utmost attention by automakers and their regulators to ensure this increased connectivity does not expose drivers and their passengers to greater risks on the road.

Sincerely,

Edward J. Markey
United States Senator

Richard Blumenthal
United States Senator