



**U.S. Department
of Transportation**

Office of the Secretary
of Transportation

Assistant Secretary
for Governmental Affairs

1200 New Jersey Avenue, SE
Washington, DC 20590

December 5, 2019

The Honorable Edward J. Markey
United States Senate
Washington, DC 20510

Dear Senator Markey:

Thank you for your letter regarding the cybersecurity of Internet-connected cars. We appreciate the opportunity to address important cybersecurity issues relating to these vehicles.

First, you requested information on whether the National Highway Traffic Safety Administration (NHTSA) has ever been notified of malicious hacking attempts against or vulnerabilities in Internet-connected cars. To date, NHTSA is not aware of any malicious hacking attempts that have created safety concerns for the motoring public. NHTSA does periodically receive information about potential vulnerabilities, generally uncovered by the security researcher community. A software vulnerability could result in various types of outcomes, from simply being a nuisance to consumers, to potentially posing serious motor vehicle safety concerns. Vulnerabilities also could present other types of risks, including compromising consumers' privacy or manufacturers' intellectual property. When NHTSA learns of such potential vulnerabilities, the agency follows its internal incident response process to ensure any potential safety risks are thoroughly assessed and appropriately mitigated by the appropriate manufacturers. One such case resulted in a product recall in 2015.

In accordance with its statutory authorities, NHTSA's primary interest with respect to Internet-connected cars focuses on the potential vehicle safety consequences of cybersecurity vulnerabilities. NHTSA coordinates and communicates with other agencies who have the primary responsibilities in handling motor vehicle cyber vulnerabilities that may result in other concerns not related to vehicle safety. Furthermore, NHTSA continues to monitor such vulnerabilities to make sure that if they become a safety concern, risks are appropriately assessed and addressed by the industry.

While advanced vehicle technologies provide the potential to reduce the number of crashes and save thousands of lives per year, the increase in software-intensive motor vehicle components introduces new and different risks. In recognition of these new risks, NHTSA emphasizes vehicle cybersecurity and follows a comprehensive approach that includes activities such as increasing public engagement, performing technical research, building internal capabilities,

The Honorable Edward J. Markey

December 5, 2019

Page 2

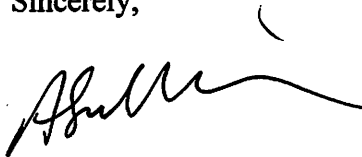
enhancing preparedness through meetings and drills, and establishing partnerships and communication channels with and among stakeholder groups. For example, NHTSA has organized vehicle cybersecurity roundtable discussions since 2016, convening a broad group of stakeholders to discuss difficult questions around this topic and identify actionable next steps the vehicle industry can address. NHTSA also has been investing in internal capabilities to perform applied research and maintains a vehicle cybersecurity lab at its Vehicle Research and Test Center in East Liberty, Ohio.

With respect to NHTSA's process for receiving reports of hacking and vulnerabilities in Internet-connected cars, NHTSA allows any member of the public to submit concerns about any safety-related issue, including cybersecurity concerns. NHTSA's regulations also require manufacturers to report all defects—including cybersecurity defects—that they identify. In addition, NHTSA proactively monitors other information sources such as media reports; participates in annual security researcher conferences; and holds routine meetings with vehicle manufacturers, suppliers, service providers, aftermarket systems providers, security researchers, test labs, and other Federal agencies. When NHTSA becomes aware of a new vehicle cybersecurity issue, the agency assesses potential safety risks and takes appropriate actions as outlined above.

Finally, you asked about public disclosure in the event of a cyber incident or vulnerability involving the security of an Internet-connected vehicle. In the case of cyber vulnerabilities that present unreasonable safety risks to the motoring public and result in a safety recall, NHTSA's existing processes provide the framework for legally required public disclosure and recall remedy. During a significant incident, as defined in the Presidential Policy Directive – United States Cyber Incident Coordination (PPD-41), coordination will be handled through the Department of Homeland Security's National Cybersecurity & Communications Integration Center. In such a scenario, NHTSA has an informational and advisory role, while performing its statutory responsibility under the Motor Vehicle Safety Act.

Thank you for your continued interest in promoting safe, reliable, and efficient transportation in the United States. If you need more information or have any additional questions, please contact the Department's oversight staff at (202) 366-4072. A similar response has been sent to Senator Blumenthal.

Sincerely,



Adam J. Sullivan
Assistant Secretary for
Governmental Affairs