FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

September 12, 2016

The Honorable Mark R. Rosekind
Administrator
National Highway Traffic Safety Administration
1200 New Jersey Avenue, S.E.
West Building
Washington, DC 20590

Dear Administrator Rosekind:

In the past several years, information security researchers have discovered and demonstrated increasingly effective – and increasingly frequent – attacks on the internal networks of automobiles through the use of On-Board Diagnostics (OBD-II) ports and the devices that connect to them.[1] The most recent of these was made public in early August, when researchers Charlie Miller and Chris Valasek demonstrated a series of attacks against the internal network of a late-model automobile that enabled them to force the vehicle to behave in an erratic and unsafe manner. Through the use of the OBD-II port, the researchers were able to successfully override built-in safeguards within the vehicle's network and, for instance, activate the parking brake or turn the steering wheel.[2]

The Environmental Protection Agency originally mandated that OBD-II ports be included in vehicles in 1994 as a means through which vehicle emissions could be tested for compliance with the Clean Air Act.[3] At that time, the Internet was still in its infancy, and while the eventual

---

[1] Researchers have been able to leverage either a direct connection to the OBD-II port, or devices that connect to the port, to cause a range of effects, from nuisances like digitally engaging the windshield wipers or car horn, to more consequential exploits such as remotely unlocking a vehicle's doors or cutting a vehicle's brakes or power steering. *See* David Wagner, *Car Hacking Research Accelerates at UC San Diego*, KPBS, Oct. 29, 2015, http://www.kpbs.org/news/2015/oct/29/car-hacking-research-accelerates-uc-san-diego/, *and* Doug Newcomb, *The Next Frontier in Car Hacking*, PCMAG, Aug. 14, 2015, http://www.pcmag.com/article2/0,2817,2489402,00.asp.

[2] Andy Greenberg, *The Jeep Hackers are Back to Prove Car Hacking Can Get Much Worse*, WIRED, Aug. 1, 2016, https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/.

[3] ON-BOARD DIAGNOSTICS (OBD) REGULATIONS AND REQUIREMENTS: QUESTIONS AND ANSWERS 3 (U.S. Envtl. Protection Agency) 2003.

networking of vehicles through technologies such as vehicle-to-vehicle communications was envisioned, the use of computers to control vehicle operations and functions was just beginning. Today, of course, modern vehicles are significantly computerized, and many standard functions such as steering and braking rely not on the physical act of a driver turning the wheel or pressing the brake, but on electronic signals sent by those objects along a vehicle's internal network. When a driver turns the steering wheel, an electronic message is sent to the wheels to turn; when a driver presses a vehicle's brake to slow down or stop, an electronic signal instructs the brake pads to engage. As a result, the integrity and security of a vehicle's internal digital communications are of vital importance.

The existence of the OBD-II port therefore presents a complicated challenge to vehicle digital security. Due to the design mandated in the original 1994 specification,[4] a direct connection to the OBD-II port is a direct connection to a vehicle's internal network. Devices that connect to the port may not only observe vehicle data, but also influence its physical behavior by means of injected electronic messages. In today's modern vehicle ecosystem, where routine maintenance more often than not requires the adjustment of digital variables instead of physical objects, and where insurance companies and cellular carriers alike provide diverse services through the use of aftermarket "dongles," this OBD-II-based direct connection may expose the vehicle, its passengers, and its environment to substantial risk if compromised.

For the past year, our staffs have met with stakeholders across the automotive industry in order to identify the equities, opportunities, and challenges posed by the existence of OBD-II ports and to explore possible paths forward. In each of these meetings, stakeholders cited the ports and the direct connection they provide to vehicle internal networks as one of the fundamental sources of cybersecurity risk in the modern vehicle ecosystem. At the same time, however, stakeholders explained that over the last two decades, OBD-II ports and the access they provide have become integral tools for independent repair shops, the aftermarket industry, vehicle hobbyists, and others. These groups rely on the OBD-II port as currently designed in order to carry out vehicle repairs, to provide consumer benefits such as insurance discounts or vehicle-based wireless hotspots, and to perform maintenance on their own vehicles. Any changes made to the port could therefore have severe consequences for these industries and individuals.

We are keenly aware of the risks and disadvantages that may come from attempting to address the cybersecurity risks created by the existence of the OBD-II port. We acknowledge that the port has grown beyond its original purpose, and appreciate the fact that there now exist industries and individuals that rely on its current design and the access it provides. In addition, we recognize that automakers have undertaken efforts to secure the OBD-II port within both its original specification and its expanded modern uses. However, as the growing series of OBD-II-based vulnerabilities shows, the OBD-II port as it currently exists creates a growing risk to the safety and security of passengers.

As such, we are writing today to request that NHTSA convene an industry-wide effort to develop a plan of action for addressing the risk posed by the existence of the OBD-II port in the modern vehicle ecosystem. This will require an open and collaborative process to ensure that all

[4] *Id.*

interested stakeholders have an opportunity to contribute to this discussion in the interest of achieving the strongest and most equitable solution. While we understand that the agency is currently in the process of developing cybersecurity guidance that may account for this vulnerability, given the potential severity of the risk, the diversity of stakeholders involved, and the complicated equities that must be balanced, we believe that this effort requires immediate and more comprehensive attention from NHTSA and the automotive industry.

We understand that this request will require significant coordination and effort among several diverse stakeholders, and we therefore request that you provide us with this plan of action no later than October 12, 2016. In addition, we request that by October 19, 2016, you make your staff available to provide a briefing to the Committee on the outcome of this work.

We appreciate your assistance with these requests. If you should have any questions, please contact Olivia Trusty or Jessica Wilkerson of the committee staff at (202) 225-2927.

Sincerely,

Fred Upton
Chairman

Greg Walden
Chairman
Subcommittee on Communications and Technology

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

Michael C. Burgess, M.D.
Chairman
Subcommittee on Commerce, Manufacturing, and Trade

cc: The Honorable Gina McCarthy, Administrator
United States Environmental Protection Agency

Mr. Mitch Bainwol, President and CEO
The Auto Alliance

Mr. Bill Hanvey, President and CEO
Auto Care Association

Ms. Mary D. Nichols, Chair
California Air Resources Board

Mr. John Bozzella, President and CEO
Global Automakers

Mr. Joshua Corman, Co-Founder
I am The Cavalry

Mr. Cuneyt L. Oge, President
The Society of Automotive Engineers