U.S. Department
of Transportation

**National Highway
Traffic Safety
Administration**

Administrator

1200 New Jersey Avenue, SE
Washington, DC 20590

October 14, 2016

The Honorable Fred Upton
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Upton:

Thank you for your letter regarding automotive cybersecurity and your observations regarding vulnerabilities associated with On-Board Diagnostics (OBD-II) ports installed in light vehicles. I appreciate the opportunity to outline the Agency's general approach to vehicle cybersecurity and current activities underway associated with the OBD-II port.

Cybersecurity is essential to the public acceptance of increasingly computerized vehicle systems, to the vehicle control systems they govern, and to the safety-enhancement potential they offer. Since 2012, the National Highway Traffic Safety Administration (NHTSA) has been pursuing an approach on vehicle cybersecurity that is based on sound research, proactive actions by industry, best practices, regulatory considerations, and enforcement. These activities support a risk based approach with the goal of improving the general cybersecurity posture of modern vehicles in a holistic fashion.

Within available resources, the Agency has taken steps to:

- help manufacturers improve their vehicle architectures through effective use of a best-practices and lessons-learned framework;
- support the sharing of cybersecurity intelligence amongst the automotive industry to establish capabilities to rapidly identify and collectively respond to emerging cybersecurity vulnerabilities;
- clarified the Agency's enforcement approach on software and vehicle cybersecurity; and
- conduct research that is supportive of policy and regulatory decisions.

At NHTSA's urging, SAE International has started a working group that is looking to explore ways to harden the OBD-II port. This group is making good progress and the Agency remains hopeful that the group will move expeditiously to develop a set of recommendations.

While securing vehicle interfaces appropriately is an essential feature, effective cybersecurity must employ an expansive and layered approach to equip the vehicle with the ability to prevent, detect, and respond to intrusions beyond focusing only on hardening each individual potential

entry port one at a time.[1] NHTSA's work considers all access points into the vehicle, more broadly than, but also including, the OBD-II port. For example, our best-practices will be based on the National Institute for Standards Technology's cybersecurity framework and other frameworks that include five principal functions: Identify, Protect, Detect, Respond, and Recover.

In the past six months, NHTSA held a public meeting and several discussions with the Environmental Protection Agency and the California Air Resources Board on the cybersecurity posture of the OBD-II port. Similarly, the Agency held discussions with the insurance industry and U.S. Computer Emergency Readiness Team regarding third-party devices that may use the OBD-II port for other purposes. Also, in conjunction with the Federal Bureau of Investigations, NHTSA issued a consumer advisory warning advising consumers on the use of 3rd party devices and the OBD-II port. These activities illustrate that further securing of the OBD-II port involves many stakeholders and should consider the serviceability requirements outlined in the Massachusetts' right-to-repair act, and legitimate needs of the automotive repair aftermarket.

Likewise, NHTSA expects to publish a set of best practices for modern vehicles soon, which will address the OBD-II port. NHTSA will remain proactive in this space to understand how vehicle manufacturers are implementing changes to vehicle designs to address cybersecurity issues.

I have sent a similar response to each cosigner of your letter. If I can provide further information or assistance, please feel free to call me or Alison Pascale, Director of Governmental Affairs, Policy and Strategic Planning, at 202-366-2775.

Sincerely,

Mark R. Rosekind

Mark R. Rosekind, Ph.D.

cc: The Honorable Gina McCarthy, Administrator
U.S. Environmental Protection Agency

Mr. Mitch Bainwol, President and CEO
The Auto Alliance

Mr. Bill Hanvey, President and CEO
Auto Care Association

[1] *NHTSA and Vehicle Cybersecurity,*
http://www.nhtsa.gov/staticfiles/administration/pdf/presentations_speeches/2015/NHTSA-VehicleCybersecurity_07212015.pdf.

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 Calvary

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