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

May 28, 2015

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

Dear Administrator Rosekind:

Every year, advancements in information and communications technologies incorporate new aspects of our daily lives into the digital universe, introducing previously unimagined convenience to consumers, businesses, and society as a whole. However, these benefits do not come without risks. Reliability and security weaknesses exist as part of the Internet ecosystem, and the pace of innovation and adoption of new technologies ensures that new weaknesses will continue to be created and introduced. As these technologies are incorporated into automobiles to improve safety, convenience, and performance, they also create the unavoidable potential for cyber threats. Therefore, it is important to understand how the National Highway Traffic Safety Administration (NHTSA) intends to address the challenge of cybersecurity as vehicles and transportation infrastructure become increasingly integrated and dependent upon the Internet and information technology.

We are entering a new era in cybersecurity. The explosion of new, connected devices and services is exacerbating existing cybersecurity challenges and has introduced another potential consequence – the threat of physical harm – as products responsible for public health and safety are integrated into the Internet ecosystem. This will be a significant challenge for the automobile industry. The integration and convergence of transportation and communications technologies in connected cars offers tremendous opportunity for innovation, improved performance, convenience (e.g. in-vehicle Wi-Fi, infotainment systems, smartphone interface and/or integration, etc.) and safety (e.g. Vehicle-To-Vehicle, Vehicle-To-Infrastructure, Autonomous Vehicles, etc.). All of these features, however, provide a gateway for potential threats.

Compounding the challenge, modern vehicles are extremely complex machines reliant on multiple computers, networks, and systems. According to some estimates, a modern high-end car can contain approximately 100 million lines of code – double that of the Windows Vista operating system and nearly ten times that of a Boeing 787.[1] With expected advancements in vehicle technology, this number could approach 300 million lines of code in the future.[2] Information technologies are inherently complex, and as a result are inherently vulnerable. The ability to identify and remediate vulnerabilities in vehicle technologies is therefore critical to maintaining robust, trustworthy systems. In light of recent failures in identifying safety defects, some of which were mechanical, the industry and safety regulators ability to keep pace with increasingly sophisticated technologies and systems is a source of concern.

Connected cars and advancements in vehicle technology present a tremendous opportunity for economic innovation, consumer convenience, and public health and safety. These benefits, however, depend on consumer confidence in the safety and reliability of these technologies. While threats to vehicle technology currently appear isolated and disparate, as the technology becomes more prevalent, so too will the risks associated with it. Threats and vulnerabilities in vehicle systems may be inevitable, but we cannot allow this to undermine the potential benefits of these technologies. The industry and NHTSA have an opportunity to prepare for the challenges that advanced vehicle technologies present, and to develop strategies to mitigate the risks.

To assist the committee in evaluating NHTSA's efforts to address the challenge of cybersecurity, please respond to the following questions by June 11, 2015.

1. Who within your organizational structure is responsible for evaluating, testing, and monitoring potential cyber vulnerabilities?
    a. Does NHTSA have a dedicated office, division, or staff?
        i. If so, how large is this function or group and where do they reside in the organization?
        ii. If NHTSA does not have a dedicated office, division, or staff, how does the agency manage this responsibility?

2. How does NHTSA track or evaluate potential cyber vulnerabilities in vehicles or vehicle systems once a product is in the field?

3. What steps are NHTSA taking to evaluate and address dealer and/or vehicle maintenance infrastructure as a potential attack vector for automobiles?

4. Has NHTSA evaluated the use or potential use of over-the-air (OTA) updates to upgrade or "patch" vehicle systems or technology?
    a. If so, what steps has the agency taken to evaluate or understand the security of these transactions?

[1] Presentation by Dr. Andrew Brown, Jr, V.P. & Chief Technologist, Delphi, *Connected and Automated Vehicles and the Cybersecurity Threat – How the Industry is Responding,* (February 17, 2015), *available at*, , http://www.cargroup.org/assets/files/bb_02-17-15/car_bb_2.17.15_brown.pdf
[2] *Id.*

5. To what extent do existing vehicle systems and technologies utilize public key infrastructure and/or certificates for secure communications?
    a. If vehicles utilize this technology, please explain NHTSA's awareness of how it is implemented and for which vehicle systems.
    b. If vehicles do not utilize this technology, please explain NHTSA's understanding or expectation of how vehicle system communications are protected.

6. What is NHTSA's plan for development and implementation of the technological infrastructure – specifically a protocol suite and architecture – capable of supporting Vehicle-to-Vehicle and Vehicle-to-Infrastructure (collectively,V2X) communications?
    a. Who is involved in developing this protocol suite and architecture?
    b. Who is responsible for implementing the protocol suite and architecture?
    c. How is NHTSA working with industry and suppliers to develop the V2X protocol suite and architecture?
    d. What is being done to evaluate potential security challenges associated with the protocol suite and architecture?

7. What steps has NHTSA taken to evaluate how connected elements, such as in-vehicle Wi-Fi and infotainment services, connect to or interact with vehicle safety systems and/or functions?
    a. Can these connections serve as a potential attack vector for vehicle safety systems?
        i. If so, what steps has NHTSA taken or are under consideration to minimize this risk?
        ii. If not, please explain why not.

8. In light of the fact that connected vehicles interact with technologies outside the specific vehicle architecture such as mobile devices, what is NHTSA doing to evaluate potential vulnerabilities introduced by these connections?
    a. Does NHTSA have the authority to address potential vulnerabilities introduced by third party mobile applications, devices or products that connect to or interact with vehicle systems?
        i. If so, please explain the basis of this authority.
        ii. If not, who is responsible for overseeing these connections?

9. Does NHTSA interact with the security research community regarding potential cyber threats and/or vulnerabilities in vehicles?
    a. If so, please describe who within NHTSA is responsible for coordinating with the research community and the nature of these interactions.
    b. If not, please explain why not.

10. What are the greatest challenges to cybersecurity in the automobile industry?
    a. What is NHTSA doing to address or minimize these challenges?
    b. What additional steps or actions, if any, do you believe are necessary to improve NHTSA and the industry's ability to address this challenge?

11. How is the automobile industry working with NHTSA to address the challenge of cybersecurity?
    a. Please provide a list and description of any recent, ongoing, or planned collaborative or cooperative engagement with the industry on this issue.
    b. Is NHTSA working with other federal partners to address this challenge?
        i. If so, provide a list and description of any ongoing or planned engagements with other federal agencies or institutions.
    c. Are there areas where the federal government could be doing more to address or prepare for this challenge?
    d. Do you have confidence that the industry is keeping NHTSA and/or other federal agencies adequately informed about their efforts to address this challenge?

We appreciate your prompt attention to this request. If you have any questions, please contact John Ohly or Jessica Wilkerson of the Majority committee staff at (202) 225-2927 or Elizabeth Letter, Michelle Ash or David Goldman of the Minority committee staff at (202) 225-3641.

Sincerely,

Frank Pallone Jr.

Fred Upton
Chairman

Frank Pallone Jr.
Ranking Member

Joe Barton

Joe Barton
Chairman Emeritus

Diana DeGette

Diana DeGette
Ranking Member
Subcommittee on Oversight
and Investigations

Marsha Blackburn

Marsha Blackburn
Vice Chairman

nna G. Eshoo

Anna G. Eshoo
Ranking Member
Subcommittee on Communications
and Technology

Tim Murphy

Tim Murphy
Chairman
Subcommittee on Oversight
and Investigations

Jan Schakowsky
Ranking Member
Subcommittee on Commerce,
Manufacturing and Trade

Greg Walden
Chairman
Subcommittee on Communications
and Technology

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

Attachment