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

Mary Barra
Chief Executive Officer
General Motors Company
P.O. Box 33170
Detroit, MI 48232-5170

Dear Ms. Barra:

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 automotive industry 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 has 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 the industry'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 in your products?
    a. Do you 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 you do not have a dedicated office, division, or staff, how does your company manage this responsibility?

2. How does your organization incorporate cybersecurity best practices into information technologies that currently exist in your products, networked or otherwise?

3. What policies, procedures, and practices do you employ to evaluate potential cyber vulnerabilities during the design, implementation and testing of vehicle components or technology?

4. Who within your organizational structure is responsible for evaluating, testing, and monitoring potential cyber vulnerabilities in the products of your suppliers?
    a. Do you 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?

---

[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.*

ii. If you do not have a dedicated office, division, or staff, how does your company manage this responsibility?

5. How do you work with suppliers to minimize, evaluate, and address potential vulnerabilities in the supply chain?

6. How do you track or evaluate potential cyber vulnerabilities in vehicles or vehicle systems once a product is in the field?

7. How do you, or how do you intend to, remediate vulnerabilities after a vehicle has entered the market?
    a. Will this require dealer service?
        i. If so, will this be conducted during routine maintenance or will it require a safety campaign or recall?
        ii. If not, what other capabilities do you possess for addressing vulnerabilities?
    b. What steps are you taking to evaluate and address dealer and/or vehicle maintenance infrastructure as a potential attack vector for automobiles?

8. Do you currently, or intend to, use over-the-air (OTA) updates to upgrade or "patch" vehicle systems or technology?
    a. If so, what steps have you taken to secure these transactions?

9. To what extent do existing vehicle systems and technologies utilize public key infrastructure and/or certificates for secure communications?
    a. If your vehicles utilize this technology, please explain how it is implemented and for which vehicle systems.
    b. If your vehicles do not utilize this technology, please explain how vehicle system communications are protected.

10. What steps have you 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 have you taken to minimize this risk?
        ii. If not, please explain why not.

11. In light of the fact that connected vehicles interact with technologies outside the specific vehicle architecture such as mobile devices, what steps are you taking to evaluate potential vulnerabilities introduced by these connections?
    a. Does your company offer, or intend to offer, a mobile application that is able to control vehicle functions such as door locks or remote start?
        i. If so, what steps are you taking to provide security for these connections?
        ii. Could they serve as a potential attack vector?

b. How do you address potential vulnerabilities introduced by third party mobile applications, devices or products that connect to or interact with vehicle systems?
    i. If a vulnerability was introduced through a third party product, mobile application or device, would you be able to identify and remediate such a vulnerability and, if so, how?

12. How do you interact with the security research community to identify potential threats and/or vulnerabilities?
    a. Do you have any programs or policies that encourage responsible disclosure from internal and/or external sources?

13. What are the greatest challenges to cybersecurity in the automobile industry?
    a. What is your company doing to address or minimize these challenges?
    b. How is the industry working together to address these challenges? Are there specific programs and/or initiatives? If so, please provide a list and description of each effort.
    c. What additional steps or actions, if any, do you believe are necessary to improve the industry's ability to address this challenge?

14. How is the automobile industry working with the federal government 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 federal government on this issue.
    b. Are there areas where the federal government could be doing more to address or prepare for this challenge?
    c. Do you have confidence in federal agencies, including but not limited to the National Highway Traffic Safety Administration, knowledge, capabilities and/or actions associated for this issue?

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,

Fred Upton
Chairman

Frank Pallone Jr.
Ranking Member

Joe Barton
Chairman Emeritus

Diana DeGette
Ranking Member
Subcommittee on Oversight
and Investigations

Marsha Blackburn
Vice Chairman

Anna G. Eshoo
Ranking Member
Subcommittee on Communications
and Technology

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