

May 13, 2016

Questions for the Record for Association of Global Automakers President & CEO, John Bozzella

The Honorable Michael C. Burgess, M.D.

- 1. As vehicles become increasingly connected and communicate with other vehicles and surrounding infrastructure, what role will encryption play in those communications to protect the security and integrity of those messages? Who would have access to the encryption keys?**

Connected vehicle technology presents significant opportunities for increased safety, mobility, reduced fuel consumption, and greater transportation efficiency. As vehicle-to-vehicle and vehicle-to-infrastructure technology (collectively referred to as V2X) allows vehicles to communicate with other vehicles and the surrounding infrastructure, security certificates and encryption are critical to ensuring that messages can be trusted. We support the Department of Transportation's ongoing work with stakeholders to define the specific security requirements in a Security Credential Management System (SCMS) that would be used to issue, distribute, and revoke security certificates.

- 2. Rigorous testing of autonomous vehicles is a critical part of certifying that these vehicles are ready for commercial use. Do we have the right regulatory framework in place to allow maximum research and testing of autonomous vehicles?**

Global Automakers agrees that rigorous testing of automated vehicle systems is critical to ensure that they may be safely deployed and that they provide drivers with the mobility benefits for which they are designed. At this time, we believe the current federal framework provides sufficient flexibility for testing, and we believe it is unnecessary to put in place prescriptive requirements with respect to the testing of automated vehicles and systems. Automakers are currently testing automated vehicles on the road in a number of states pursuant to the states' respective testing requirements, as well as in controlled test environments. This testing is providing automakers with tremendous knowledge concerning the operating capabilities of automated systems in a variety of driving environments. The auto industry would welcome federal action to support upgrading existing facilities or construction of new testing facilities that can support both National Highway Traffic Safety Administration (NHTSA) and industry automated vehicle research. In order to test and deploy automated vehicles, the industry will need a variety of different test environments that replicate real world driving conditions, covering a range of terrain, weather, and climate.

As the industry moves beyond the testing phase towards the manufacture, certification, and deployment of automated vehicles, we see an important role for the federal government in the establishment of a regulatory framework that is consistent throughout the United States and, where possible, harmonized with other countries. We think that NHTSA has taken a number of positive steps in the right direction. In January 2016, Secretary Foxx signaled that the Department of Transportation was taking proactive steps to provide federal leadership and

guidance in the development of a more consistent national policy on automated vehicles¹. Among the initiatives announced were commitments to work with industry stakeholders to develop *guidance for the safe deployment and operation* of automated vehicles, and to work with the American Association of Motor Vehicle Administrators (AAMVA) and other state partners on the development of *model state policy*.

A principal goal of the agency—and of all of the stakeholders involved in the process—should be avoiding a patchwork of different federal and state standards for automated technologies. Despite NHTSA’s important actions to date with respect to automated vehicles, many states have stepped into what they perceive to be a policy vacuum in the field. The result is that states such as California, Nevada, and Florida, have all enacted laws that will impact the way automakers design and manufacture automated vehicles. Each of these states has taken a slightly different approach to the issue, even using different definitions of what constitutes an automated vehicle. Federal policymakers have long recognized the public benefit of having Federal Motor Vehicle Safety Standards (FMVSS) that limit state action and allow manufacturers to design, produce and sell the same vehicles across 50 states. NHTSA’s regulatory activities should reflect the respective roles of federal and state regulators in this space as well. To the extent that specific design and performance requirements are necessary and appropriate for automated vehicles, these should be established by NHTSA and applicable nationwide.

As technology continues to evolve, it is important that NHTSA work collaboratively with industry and other stakeholders in the development of a policy framework that balances the need for safety while ensuring that innovation can continue in the connected and automated vehicle space.

a. How should Congress work with NHTSA and the auto industry to facilitate more testing and research of advanced automotive technologies?

Congress should exercise its oversight authority to ensure that that federal agencies are working together to advance automotive technologies that can save lives and dramatically improve vehicle transportation. Regulatory clarity will facilitate the testing and research necessary to move these technologies to deployment. There are two critical near term opportunities for federal regulators and policymakers to provide certainty and support for innovation. First, Congress must ensure that the 5.9 GHz spectrum band is protected from harmful interference to support the rapid deployment of connected vehicles which have the potential to save thousands of lives on our highways. Second, Congress must work with federal agencies to provide federal leadership on automated vehicles and to avoid a patchwork of different state laws from stifling innovation.

3. Please provide an update on the Auto-ISAC, including current membership, any plans to expand membership, how often the ISAC meets, and any plans to develop cybersecurity best practices and when they will be developed. Please also include

¹ Secretary Foxx unveils President Obama’s FY17 budget proposal of nearly \$4 billion for automated vehicles and announces DOT initiatives to accelerate vehicle safety innovations - <http://www.nhtsa.gov/About+NHTSA/Press+Releases/dot-initiatives-accelerating-vehicle-safety-innovations-01142016>

how much information sharing is occurring between members of the Auto ISAC and whether any vulnerabilities been uncovered that were not previously known to certain ISAC members through the information sharing process?

The Auto-ISAC was incorporated on August 17, 2015, to analyze and share intelligence on cybersecurity threats and vulnerabilities between industry stakeholders. The organization reached initial operating capability (IOC) and shared the first industry intelligence report on December 20, 2015. The Auto-ISAC reached full operating capability (FOC) on January 20, 2016, following the launch of the secure information sharing portal. The Auto ISAC has briefed Global Automakers on its recent developments. According to Auto ISAC staff, since IOC, the Auto ISAC has reported and shared vulnerabilities that have been identified by both Auto-ISAC members and other cyber intelligence sources. Current members of the Auto-ISAC include BMW, FCA, Ford Motor Co., General Motors, Daimler, American Honda Motor Co., Hyundai, Kia, Mazda, Mitsubishi, Nissan, Subaru, Toyota, and Volkswagen. In addition to OEM members, the first automotive supplier member, Delphi, joined the Auto-ISAC in April and additional large supplier members are anticipated soon. Staff from the Auto-ISAC would be best able to provide additional information about its activities.

In addition to industry taking proactive steps to develop information sharing capabilities, on January 19, 2016, Global Automakers and the Alliance of Automobile Manufacturers (“Alliance”) released a Framework for Automotive Cybersecurity Best Practices to serve as the foundation for the development of voluntary industry-wide automotive cybersecurity best practices. Working collaboratively with the Auto-ISAC, Global Automakers and Alliance members have made significant progress toward this objective, and we expect to complete the development of initial best practices in the near future. As the cybersecurity landscape continues to evolve there are significant challenges for policymakers in developing regulations or guidance that reflect the current state of technology. While neither the Framework, nor the Best Practices, is intended to replace applicable laws and regulations where they already exist, we believe this type of industry-led approach is necessary to ensure greater flexibility in responding to changes in technology.

The Honorable Gregg Harper

- 1. The FAST Act requires manufacturers to include the name, description, and part number of components or components in its Part 573 report for defects or noncompliance, if a recall involves a defect in a specific component. Can you comment on how your member companies have been able to address the requirements of the passage of the Act?**

In accordance with the FAST Act, Global Automakers members will provide the component information required by the Part 573 report.