Consumers Union®

POLICY & ACTION FROM CONSUMER REPORTS

Statement of William C. Wallace, Policy Analyst, Consumers Union
Before the U.S. House of Representatives Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection

Hearing on "Self-Driving Vehicle Legislation"
Tuesday, June 27, 2017

Summary

- Self-driving cars have enormous potential to make our roads safer by significantly reducing crashes attributable to driver error. There is a smart, safe path to realizing this promise.

- As highly automated vehicles reach market and improve mobility—including for seniors, underserved populations, and individuals with disabilities—companies and policymakers should set a clear expectation: these cars also must significantly improve safety.

- It is not clear what the actual safety impacts will be as companies extensively introduce automated driving systems to our roads. This stands in contrast with proven advanced active safety systems, such as automatic emergency braking.

- Automotive innovation is essential, and has brought about features with major benefits for consumer safety. But any accelerated deployment should be evidence-based and should include sensible, binding measures to protect consumers against any new hazards.

- Our more detailed recommendations are:

    - Exemptions from federal safety standards for highly automated vehicles should be limited to equipment required exclusively for the driving task which may be fully replaced by automation, and granted only if backed by evidence provided through a publicly defined National Highway Traffic Safety Administration (NHTSA) process. No exemptions should be given for crashworthiness or occupant protection aspects of safety standards under these proposals.

    - Additional research, disclosure, and mitigation measures should be in place to protect consumers in vehicles that have Level 2 or 3 driving automation, which can provide a dangerously false sense of security, increasing the risk of driver inattention or error.

    - Automakers should make their safety-related data public and share it with regulators in a timely manner.

    - Preemption of state and local authority should be narrowly tailored and limited to areas where NHTSA has set strong federal standards.

    - The Federal Trade Commission (FTC) and NHTSA should be given the authority to jointly set baseline, enforceable privacy and security standards.

    - NHTSA's capabilities should be strengthened significantly through increased funding and authority—not just for self-driving cars, but also so it can better save lives and prevent injuries due to chronic problems, like drunk and distracted driving, seatbelt non-use, and automakers' failure to make the best new safety features standard on all vehicles.

- As the Subcommittee crafts legislation, we stand ready to assist in its efforts to ensure auto safety and accountability.

Testimony

Good morning, Chairman Latta, Ranking Member Schakowsky, and members of the Subcommittee. My name is William Wallace. I am the safety policy analyst for Consumers Union, the policy and mobilization arm of Consumer Reports, an independent, nonprofit organization that works side by side with consumers to create a fairer, safer, and healthier world.[1]

At Consumer Reports, we consider it a responsibility and a privilege to work for safer cars. We push for policies that advance safety, and we help consumers make informed choices that help them stay safe on the road, through testing, journalism, survey research, advocacy, and consumer mobilization.

We evaluate safety technologies every day at our Auto Test Center. The experts on our team are methodical and rigorous, testing about 60 vehicles per year and driving them a total of about 900,000 miles annually. They drive each vehicle Consumer Reports rates for 2,000 break-in miles before even starting formal testing, which includes more than 50 tests using state-of-the-art tools.

The safety features we evaluate range from seat belts and the fit of child car seats to driver-assistance technologies, which we have identified in more than a dozen models for sale in the United States. Our testers take cars that can steer within a lane, adjust speed, and brake automatically and assess them thoroughly. As more features hit the market, our testers will be carefully evaluating them for safety, and reporting our findings to consumers.

Looking to the future, we see the potential for self-driving cars to make our roads safer

[1] As the world's largest independent product-testing organization, Consumer Reports uses its more than 50 labs, auto test center, and survey research center to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million subscribers to its magazine, website, and other publications.

by significantly reducing crashes attributable to driver error.[2] There is a smart, safe path to realizing this promise, one which we encourage automakers, regulators, and Congress to follow.

As highly automated vehicles reach the market and improve mobility for consumers, including seniors, underserved populations, and people with disabilities, companies and policymakers should set a clear expectation: these cars also must significantly improve safety. This means that they should meet all crashworthiness and occupant protection aspects of Federal Motor Vehicle Safety Standards (FMVSS), while also demonstrating that enhanced driving automation further reduces deaths and injuries resulting from traffic crashes. At present, it is not clear what the actual safety impacts will be as companies extensively introduce automated driving systems to our roads. This stands in contrast with proven advanced active safety systems,[3] such as automatic emergency braking with forward collision warning.

The advent of self-driving vehicles represents the single biggest change in the relationship between cars and their passengers since the invention of the motor vehicle itself. In considering legislation on driving automation, we urge members to embrace both technological ambition and accountability. Automotive innovation is essential, and has brought about numerous features with major benefits for consumer safety. But any accelerated deployment

---

[2] In this testimony, "self-driving cars" or "self-driving vehicles" refers to motor vehicles with Level 4 or Level 5 driving automation, as defined by the standards-setting organization SAE International. These levels include only vehicles for which the automated driving system must be capable of performing not just the dynamic driving task but also the fallback function, as well as achieving a minimal risk condition, as defined by SAE International. In other words, the system must perform the driving task even if the human driver does not respond appropriately to a request to intervene. Additionally—and once again in line with definitions established by SAE International—the term "automated driving system" refers to SAE Level 3, 4, or 5 vehicles. Just as the National Highway Traffic Safety Administration (NHTSA) and the discussion drafts refer to them, we use "highly automated vehicles" in this testimony to refer to motor vehicles equipped with an automated driving system. Surface Vehicle Recommended Practice, SAE J3016, Taxonomy and Definitions for Terms Related to Automated Driving Systems, issued January 2014, revised September 2016 (hereinafter, "SAE J3016_201609") . The term "car" refers to any motor vehicle, except a commercial motor vehicle, as those terms are defined in Subtitle VI of Title 49, United States Code.

[3] Per SAE International, "active safety systems" are "vehicle systems that sense and monitor conditions inside and outside the vehicle for the purpose of identifying perceived present and potential dangers to the vehicle, occupants, and/or other road users, and automatically intervene to help avoid or mitigate potential collisions via various methods, including alerts to the driver, vehicle system adjustments, and/or active control of the vehicle subsystems (brakes, throttle, suspension, etc.)." SAE J3016_201609 at 3.

should be evidence-based—requiring manufacturers to demonstrate how highly automated vehicles improve safety—and should include sensible, binding measures to protect consumers against new hazards that may emerge.

With these principles in mind, we make the following more detailed recommendations related to the draft bills that are the subject of the hearing:

- Exemptions from federal safety standards for highly automated vehicles should be limited to equipment required exclusively for the driving task, such as steering, braking, and mirrors, which may be fully replaced by automation, and granted only if backed by evidence provided through a publicly defined National Highway Traffic Safety Administration (NHTSA) process. No exemptions should be given for crashworthiness or occupant protection aspects of federal safety standards under these proposals.
- Additional research, disclosure, and mitigation measures should be in place to protect consumers in vehicles that have Level 2 or 3 driving automation, which can provide a dangerously false sense of security, increasing the risk of driver inattention or error.
- Automakers should make their safety-related data public and share it with regulators in a timely manner.
- Preemption of state and local authority should be narrowly tailored and limited to areas where NHTSA has set strong federal standards.
- The Federal Trade Commission (FTC) and NHTSA should be given the authority to jointly set baseline, enforceable privacy and security standards.
- NHTSA's research, enforcement, and other capabilities should be strengthened significantly through both increased funding and authority.

First, exemptions from federal safety standards for highly automated vehicles should be limited to equipment required exclusively for the driving task, such as steering, braking, and mirrors, which may be fully replaced by automation, and granted only if backed by the evidence provided through a publicly defined NHTSA process. No exemptions should be given for crashworthiness or occupant protection aspects of federal safety standards under these proposals.

Collectively, several of the draft bills would greatly expand the ability of NHTSA to grant exemptions from FMVSS for highly automated vehicles. NHTSA's governing statute requires, among other things, that the agency may grant only those exemptions that are "consistent with the public interest" and with 49 U.S.C. Chapter 301, whose overarching purpose is "to reduce traffic accidents and deaths and injuries resulting from traffic accidents."[4] To comply with these requirements, exemptions should be limited to equipment where the sensors or actuators of a vehicle's automated driving system can fully, effectively, and safely replace a human driver's observations or actions related to a particular driving task or FMVSS. Only under such circumstances could the vehicle's manufacturer show that it is not necessary for the vehicle to meet a federal performance standard for a part of the car has been replaced because the human driver never needs to use it.[5] Because a vehicle should provide crash protection regardless of whether it is driven by a human driver or automated system—and because exemptions must be consistent with the public interest—no exemptions should be provided for equipment required for crashworthiness or occupant protection.

In the current versions of the draft bills, it is unclear what statistics or analyses support

---

[4] 49 U.S.C. §§ 30101 and 30113.

[5] For this reason, we are skeptical that there are any appropriate automation-related FMVSS exemptions that could be granted to vehicles with driving automation systems of only Level 3 or lower, since these cars require fallback performance by a human driver.

the dramatic expansion of exemptions available for highly automated vehicles. In particular, no specific safety-related justification has been presented for increasing the maximum annual number of a manufacturer's exempted vehicles from 2,500 to 100,000, for increasing the time period of exemptions from two years to five years, or for determining that it is necessarily consistent with motor vehicle safety and the public interest for NHTSA to grant exemptions with the goal to "promote the public adoption and acceptance or facilitate meaningful commercial deployment of a new motor vehicle safety feature or system."

To determine appropriate statistical backing and whether exemptions truly are justified by the body of the evidence, Congress should direct NHTSA to define a specific process and criteria for granting exemptions using official notice-and-comment procedure. This process and criteria should be followed by manufacturers in seeking exemptions, and by the agency in determining whether to grant them. Asking NHTSA to develop a formalized process would not only make the agency's review of exemptions more robust, but also ensure that highly automated vehicles only receive exemptions from FMVSS appropriately, when they would not risk the protection to consumers that the relevant standards are intended to provide. Such a process likely also would enhance consumer confidence in the safety of any exempted vehicles, and promote business certainty compared to an exemption process that operates entirely on a case-by-case basis.

Second, additional research, disclosure, and mitigation measures should be in place to protect consumers in vehicles that have Level 2 or 3 driving automation, which can provide a dangerously false sense of security, increasing the risk of driver inattention or error. Based on Consumer Reports' first-hand experience testing cars with advanced driver-

assistance systems, we are very concerned that the significant potential for driver confusion over automated driving system capabilities will lead to crashes, particularly of cars with the SAE International Level 2 and Level 3 driving automation systems whose capabilities can most readily be overstated by the automaker or overestimated by the driver. In these vehicles, it may seem to consumers that the car can drive itself, when in reality these consumers need to be prepared to take over the controls at a moment's notice, always keeping their eyes on the road and their hands on the wheel. By contrast, Level 4 and 5 vehicles must perform the driving task even if the human driver does not respond appropriately to a request to intervene.

In Level 2 and 3 vehicles, we are particularly concerned about safety issues related to human-machine interface (HMI), which is the combination of hardware and software that allows a human to interact with a machine to perform a task.[6] NHTSA, too, has taken seriously the need to better understand how HMI factors affect safety. The agency has noted that drivers' ability to return to the task of monitoring and driving is limited by humans' capacity for staying alert and re-engaging after having disengaged their attention, and that it may be appropriate for companies to consider incorporating driver engagement and responsiveness monitoring in the vehicles and stepping up consumer education and training related to HMI factors.[7] We agree with these recommendations; however, we understand that the agency proposed significant additional research into HMI that has yet to be funded.[8] This research is an urgent necessity for NHTSA so that it can better understand HMI-related safety issues and propose steps necessary to protect safety—including any possible performance requirements for driver monitoring. We urge the

---

[6] NHTSA, Federal Automated Vehicles Policy at 84 (Sept. 20, 2016) (online at one.nhtsa.gov/nhtsa/av/pdf/Federal_Automated_Vehicles_Policy.pdf).

[7] *Id.* at 22-24.

[8] *See, e.g.*, NHTSA, *Budget Estimates – Fiscal Year 2017* (Feb. 2016) (online at www.nhtsa.gov/staticfiles/administration/pdf/Budgets/FY2017-NHTSA_CBJ_FINAL_02_2016.pdf).

Subcommittee to push for additional funds for this research, and to direct NHTSA to seek preventive solutions.

We also urge the Subcommittee to improve disclosure regarding vehicles with Level 2 automated driving systems. One of the draft bills, the DECAL Act, is a sensible proposal that would help prospective buyers better understand highly automated vehicles as long as the information provided on the Monroney label clearly and simply explains the car's capabilities. This bill's disclosure coverage should be extended to Level 2 vehicles so that consumers interested in those cars—which are becoming increasingly available—can readily understand what types of driving tasks those cars are capable of doing, and what they are not capable of doing.

Third, automakers should make their safety-related data public and share it with regulators in a timely manner. Right now, auto industry claims of the safety benefits of highly automated vehicles appear to be speculative or based on data held internally by the companies. Regulators and consumers should know the basis that companies use to determine: (1) that an automated driving system is safe; and (2) that it can provide added safety benefits—especially if any exemptions to FMVSS are to be granted.

This kind of disclosure, and process, would help companies build trust in their products, which right now is lacking, according to recent research by MIT and others. For example, preliminary survey results released by MIT AgeLab in late May indicated that only 13% of respondents would be comfortable with a fully autonomous car, which represented more than a ten percentage point drop from a similar survey the previous year. The researchers pointed out

that the declining trust in automation was particularly notable among younger respondents.[9]

One possible mechanism for the public release of safety information could come through companies' submissions to NHTSA of safety assessment letters, which represent a key component of the agency's September 2016 Federal Automated Vehicles Policy guidance. Under that guidance, the letters represent one of the primary ways for NHTSA and the public to assess how entities developing and testing highly automated vehicles are addressing safety.[10] However, at the time this guidance was released, we were concerned that companies would choose to submit only the bare minimum of information to NHTSA—which would be of little use to consumers and would not necessarily provide the agency with the robust data it needs to independently assess the safety of highly automated vehicles.[11] We encouraged the agency to ensure sufficiently robust responses and prevent entities from simply "checking the boxes." As current leaders at the Department of Transportation consider how to proceed with the Federal Automated Vehicles Policy, we urge Congress to prioritize legislative provisions that would help NHTSA receive and make public all of the information needed to protect consumers and provide transparency about the basis for automaker claims and NHTSA decisions.

Additionally, we encourage caution on what information related to highly automated vehicles must be kept confidential by NHTSA. While NHTSA certainly should protect true trade secrets, as well as personally identifiable information, we urge members to ensure that provisions on the treatment of confidential business information do not inhibit the release of information that could keep consumers safe from a hazard that may emerge in an automated driving system.

---

[9] H. Abraham, et al., "Consumer Interest in Automation: Preliminary Observations Exploring a Year's Change" at 6 (Figure 4), White Paper (2017-2), Massachusetts Institute of Technology, AgeLab (May 25, 2017) (online at agelab.mit.edu/sites/default/files/MIT%20-%20NEMPA%20White%20Paper%20FINAL.pdf).

[10] NHTSA, Federal Automated Vehicles Policy at 15-16, *supra*.

[11] The NHTSA guidance asks entities that create automated driving systems to show how they have accounted for a number of key factors inherent to the safety of these systems, but does not currently specify what level of detail the entities should include or what additional data should be submitted to the agency. *Id.*

Fourth, preemption of state and local authority should be narrowly tailored and limited to areas where NHTSA has set strong federal standards. While it is appropriate to clearly delineate federal and state roles in regulating automated vehicles, we caution against going too far in the name of avoiding a "patchwork." It would be inappropriate to preempt states' authority to protect their citizens without strong federal safety standards in place. However, states that do not have the technical expertise of NHTSA should certainly consult extensively with the agency.

If the Subcommittee does advance legislation to preempt the states, which we do not support, we would at the very least urge members to narrow the provision substantially so that it does not prevent states from protecting their citizens in ways states traditionally have done. For instance, in keeping with states' traditional role overseeing whether a vehicle's operation is safe enough for public roads, we have called for states nationwide to prohibit the operation of vehicles' automated driving systems if needed equipment such as sensors or critical safety control systems have been significantly damaged and not repaired. It is unclear, from the extremely broad language of the preemption provision in the current draft of the LEAD'R Act, whether laws such as these could take effect under that bill.

Fifth, the FTC and NHTSA should be given the authority to jointly set baseline, enforceable privacy and security standards for cars. Motor vehicles are increasingly networked, with today's cars having upward of 70 to 100 electronic control units and potentially containing as much as 100 million lines of software code—significantly more than a new

passenger airplane.[12] Further, motor vehicles are increasingly able to send and receive information via cellular, wireless internet, short-range, and other communications technologies. Given consumers' understandable concerns over the privacy of their data,[13] and the seriousness of vehicle data security risks,[14] lawmakers should direct the FTC and NHTSA to jointly develop binding minimum privacy and data security standards for manufacturers of vehicles and equipment.

Today's cars can pose privacy issues and security vulnerabilities just as a computer or a mobile device can.[15] Consumers have deep concerns about how their information is collected and used, with a nationally representative Consumer Reports survey finding last month that 70% of U.S. adults lack confidence that their personal data is private and safe from distribution without their knowledge.[16] We also have found that large percentages of Americans act on their concerns, taking specific steps to prevent their information from security breaches.[17] Moreover, unlike some connected products, a breach of safety-critical vehicle systems comes with serious

---

[12] Government Accountability Office, "Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-World Attack" at 7-8 (Mar. 2016) (online at www.gao.gov/assets/680/676064.pdf) (GAO-16-350).

[13] *See, e.g.*, "Americans Want More Say in the Privacy of Personal Data," Consumer Reports (May 18, 2017) (online at www.consumerreports.org/privacy/americans-want-more-say-in-privacy-of-personal-data).

[14] *See, e.g.*, GAO-16-350, *supra;* Federal Bureau of Investigation, Department of Transportation, and NHTSA, "Motor Vehicles Increasingly Vulnerable to Remote Exploits" (Mar. 17, 2016) (online at www.ic3.gov/media/2016/160317.aspx); Staff of U.S. Sen. Edward J. Markey, *Tracking & Hacking: Security and Privacy Gaps Put American Drivers at Risk* (Feb. 9, 2015) (online at www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

[15] In March 2017, Consumer Reports announced the launch of a collaborative effort to create a digital privacy and security standard for consumers. The standard, available at TheDigitalStandard.org, will help guide companies in the design of mobile and internet-connected products and services, including cars, and empower consumers by enabling independent testing and reporting on whether products protect the privacy and security of their personal data. "Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security," Consumer Reports (Mar. 6, 2017) (online at www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating-products-services-for-privacy-and-data-security).

[16] "Americans Want More Say in the Privacy of Personal Data," Consumer Reports, *supra; see also, e.g.*, "Are You Scared Your Future Self-Driving Car Will Get Hacked," Fast Company (Feb. 22, 2017) (online at www.fastcompany.com/3068051/are-you-scared-your-future-self-driving-car-will-get-hacked).

[17] Consumer Reports, "Consumer Reports Takes On Privacy, Recommends 66 Ways to Prevent Hackers and Companies From Capturing Your Data" (release) (Sept. 20, 2016) (online at www.consumerreports.org/media-room/press-releases/2016/09/onsumer-reports-takes-on-privacy--recommends-66-ways-to-prevent-).

risks that can be associated with life-or-death consequences.[18] Appropriately, NHTSA has recognized the protection of data security as a critical element of motor vehicle safety.

Consumers should be able to know what data their car is collecting and transmitting, and who has access to this information. They should be able to trust that companies are legally obligated to protect their privacy and the security of their data. This trust is important not just for consumers themselves, but also for the broader acceptance and successful deployment of active safety and automated driving systems across the marketplace. Therefore, consumer privacy and data security standards for motor vehicles are too important to be left to voluntary measures alone, and instead, they should be binding and enforceable, and should apply to all motor vehicles, not just highly automated vehicles. At the same time, these standards should allow for appropriate access to safety-related data, including data available beyond an event data recorder, by crash and defect investigators in the event of a crash.

The MEMO Act, one of the draft bills under consideration, proposes to address privacy and security issues by requiring the FTC and NHTSA to enter into a memorandum of understanding on the regulation and oversight of highly automated vehicles with respect to privacy and data security. While we support the Subcommittee's attention to consumer privacy regulation, we disagree with the approach taken in the draft bill. The MEMO Act focuses on limiting overlap and duplication, rather than focusing on which privacy and data security standards would give car consumers the strongest protection and most meaningful choices about their personal data.

We urge the Subcommittee to direct the FTC and NHTSA to work jointly on mandatory rules. The legal authorities of the FTC and NHTSA are separate, with very different purposes,

---

[18] *See, e.g.*, "One in Five Vehicle Vulnerabilities are 'Hair on Fire' Critical," Security Ledger (Aug. 11, 2016) (online at securityledger.com/2016/08/one-in-five-vehicle-vulnerabilities-are-hair-on-fire-critical).

and the agencies have different areas of expertise. The agencies should share oversight where appropriate for the oversight of privacy and data security in cars.

Sixth, NHTSA's research, enforcement, and other capabilities should be strengthened significantly through both increased funding and authority. NHTSA remains chronically under-resourced, both in budget and in staffing. So that it can support the safe and responsible advancement of automated technologies, NHTSA needs expanded funding and personnel. The agency already has a backlog of research needed to independently and thoroughly assess the safety of automated driving systems and the manner in which drivers interact with these new features.[19] However, if the draft bills require NHTSA to complete additional tasks without additional funding or personnel, these and other important efforts (such as addressing critical safety issues around behavioral safety risks, crashworthiness, and occupant protection) would likely continue to stall.

With regard to NHTSA's legal authority, the agency made clear in a September 2016 Enforcement Guidance Bulletin that it has the authority to deem reasonably foreseeable automated system risks to be safety-related defects.[20] But the agency's practical ability to get unsafe cars off the road quickly is limited. For the agency to be the kind of watchdog consumers deserve, Congress should give it the authority to take immediate action on defects that present an imminent hazard, or those that substantially increase the likelihood of serious injury or death. The Food and Drug Administration and Consumer Product Safety Commission already possess this type of authority, and it has been included in the proposed Vehicle Safety Improvement Act

---

[19] As recently as last year, the agency sought additional funding and staff for this research. *See, e.g.,* NHTSA, *Budget Estimates – Fiscal Year 2017* at 30, *supra*.

[20] NHTSA, *NHTSA Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Automated Safety Technologies,* 81 Fed. Reg. 65705 (Sept. 23, 2016).

as introduced in each of the past two Congresses.[21] We also previously called for the agency to receive more detailed information from manufacturers in order to create a more useful Early Warning Reporting program, as well as for increased civil fines authority and a criminal penalties provision to be enacted to deter executives from hiding defects.[22]

Finally, while the potential safety benefits of partly and fully self-driving cars are significant, it still will take some time for all vehicles on the road to benefit from the technology. As a result, additional funding, personnel, and authority for NHTSA would enable the agency to more effectively work to save lives and prevent injuries to vehicle occupants, pedestrians, and bicyclists due to chronic problems like drunk and distracted driving, lack of seatbelt use, and the failure of automakers to make the best new safety technologies standard on all of their vehicles.

Lastly, we have several recommendations about additional priority issues. These include:

- **The proposed federal advisory committees should have broader representation, and come with new resources for NHTSA, if they are to be established.** It is appropriate for NHTSA to receive and carefully consider input from key stakeholders on issues related to driving automation and individuals with disabilities, senior citizens, underserved populations, data security, and the sharing of information about on-road testing of vehicles. For each of these issues, the agency also should receive and carefully consider input from safety and consumer representatives as well as local and state

[21] *See, e.g.*, NHTSA, GROW AMERICA Act at 183 (Apr. 7, 2015) (online at www.transportation.gov/sites/dot.gov/files/docs/GROW_AMERICA_Act_1.pdf) and NHTSA, Federal Automated Vehicles Policy at 75, *supra*; H.R. 1181 (114th Cong.).

[22] *See, e.g.*, Testimony of Consumers Union to the U.S. House Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, "Legislative Hearing on VIN Database and Auto Whistleblower Bills" (Sept. 25, 2015) (online at docs.house.gov/meetings/IF/IF17/20150925/103982/HHRG-114-IF17-Wstate-WallaceW-20150925.pdf).

officials. In addition, because federal advisory committees come with costs and staff commitments, any establishment of such a committee should come with an appropriate amount of additional resources and personnel for NHTSA.

- **If Congress decides to extend the ability to test noncompliant vehicles to entities beyond automakers, it should ensure NHTSA has the authority to determine how, and to what extent, such testing can be carried out safely.** A significant portion of safety innovation in the automotive space comes from suppliers, universities, and others who create new motor vehicle equipment. However, the testing of automated driving systems by those other than motor vehicle manufacturers comes with unique complexities. Accordingly, if Congress is to extend the allowable testing of vehicles not compliant with FMVSS to equipment manufacturers, then it should also direct NHTSA and companies to explain how the equipment will be integrated safely into the broader vehicle system developed by another company.
- **The Subcommittee should consider the future of federal vehicle safety standards.** In addition to crash protection and crash prevention, vehicle safety rules also should account for the process of developing electronic systems. Specifically, given the immense quantity of software and electronics systems in vehicles with some form of driving automation, we urge members to consider the merits of a functional safety standard.[23] NHTSA traditionally has issued standards for individual components, but there is currently no clear way to establish performance standards for software that must be able to work reliably in almost an infinite number of circumstances.

[23] Functional safety is a process to ensure that the system, as a whole, operates correctly and safely in response to inputs, errors, and failures. The Subcommittee could, for instance, direct NHTSA to base a new rule on the existing international voluntary standard for functional safety of electrical and/or electronic systems in production automobiles, ISO 26262.

Conclusion

We see great safety potential in self-driving cars, but that promise will only be realized by following a smart, safe path. Policymakers should set a clear expectation that highly automated vehicles must significantly improve safety, in addition to providing mobility and other benefits to the public. We urge Congress to embrace both technological ambition and accountability, including by requiring sensible, enforceable, evidence-based measures to protect consumers against new hazards that may emerge. As it continues to work on the draft legislation, we stand ready to help the Subcommittee ensure that these principles are upheld in the law.