1402 Third Avenue, Suite 500
Seattle, WA, 98101

www.sightline.org
206 447 1880

Sightline
INSTITUTE

February 1, 2021

Mr. Jack Danielson
Executive Director
National Highway Traffic Safety Administration
US Department of Transportation
1200 New Jersey Avenue SE
Washington, DC 20590

Subject: Framework for Automated Driving System Safety
Docket No. NHTSA-2020-0106)

Dear Executive Director Danielson:

The Sightline Institute is pleased to provide comments on the Framework for Automated Driving System Safety, published in the Federal Register on December 3, 2020. Sightline is a think tank in Seattle, Washington providing original analysis of energy, economic, and environmental policy in the Pacific Northwest. Sightline has a program to research and advocate public policy that will help realize the promise and avoid the perils of automated vehicles.

Properly regulated electric robo-taxi fleets could reduce emissions, improve mobility, increase economic productivity, and enhance the quality of life in our metro areas[1]. The recent histories of the automotive and software industries has shown time and again that well-designed federal regulations are essential to ensuring safety and consumer choice. We therefore offer two key recommendations for federal policy related to self-driving vehicles:

- No vehicle should operate on a public roadway without a human driver unless the automated system is certified as sufficiently safe by a qualified <u>external</u> assessor according to new NHTSA standards.

- UL4600 should serve as the foundation for new NHTSA standards for certifying the safety of automated driving systems.

The private companies racing to market automated vehicles and robo-taxi services would rather "self-certify" their safety. Such a position reflects the narrow financial interests of individual firms rather than the broad public interest. Moreover, it will ultimately undermine the public trust necessary to enable widespread adoption of these beneficial technologies

[1] https://www.sightline.org/2018/01/16/part-1-your-car-of-the-future-is-no-car-at-all/

when they are sufficiently safe. We encourage NHTSA to carefully weigh the case for adopting a standard that doesn't inhibit innovation but does require companies to make a comprehensive argument, supported by data, for the safety of their automated systems prior to deployment.

Arguments for NHTSA requiring compliance with UL4600 include:

1. **Private companies have a history of producing unsafe vehicles prior to the imposition of enforceable standards developed by public regulators.**

The auto industry has fought sensible safety standards for decades, opposing requirements for safety glass, seat belts, airbags, and catalytic converters[2]. Volkswagen recently committed a massive global fraud by falsifying tests of the emissions from its diesel cars[3]. Even Boeing, with every incentive to build safe aircraft, cut corners and deceived regulators[4] about the functioning of an automated system on the Boeing 737 MAX that led to two fatal crashes and forced the plane's grounding for nearly two years. Notwithstanding their claims to the contrary, the companies building automated vehicles face competitive pressures, shareholder demands, and the ego-driven narratives of senior executives that can motivate them to field unsafe products. Indeed, the pedestrian fatality caused by the Uber test vehicle outside Phoenix in 2018 provides prima facie evidence of the deadly consequences of letting a technology company in a race to bring a self-driving vehicle to market adopt fundamentally unsafe practices[5] in the absence of a clear regulatory framework.

2. **Relying solely on private companies' evaluation of the safety of their automated systems will undermine public trust in the technology.**

According to a 2018 Pew survey of attitudes towards high-tech companies[6], "Only 3% of Americans think these companies can be trusted to do what is right just about all of the time...while a total of 72% think they can be trusted to do the right thing [only] some of the time or hardly ever." If anything, public sentiment has shifted further against trusting Big Tech since the spring of 2018. As evidence look no further than the antitrust case filed against Google by a bi-partisan coalition of 40 state attorneys general in December 2020[7].

Waymo, a subsidiary of Google's parent Alphabet, this year began offering robo-taxi service outside of Phoenix without any safety driver. Waymo's passengers, other drivers, pedestrians, and cyclists in that operating environment now rely solely on Waymo's assurances that its technology is safe. In an October 2020 discussion of their safety readiness, Waymo reviewed the emerging safety standards and had this to say:

[2] https://www.pewtrusts.org/~/media/assets/2011/03/industry-clean-energy-factsheet.pdf

[3] https://www.reuters.com/article/us-volkswagen-emissions/vw-executive-gets-seven-years-for-u-s-emissions-fraud-idUSKBN1E01W1

[4] https://www.nytimes.com/2020/01/09/business/boeing-737-messages.html

[5] https://www.theverge.com/2019/11/19/20972584/uber-fault-self-driving-crash-ntsb-probable-cause

[6] https://www.pewresearch.org/internet/2018/06/28/public-attitudes-toward-technology-companies/

[7] https://www.washingtonpost.com/technology/2020/12/17/google-search-antitrust-lawsuit/

> As insightful and well conceived as many of these suggested and developing methodologies are, none of them provides a definitive, widely accepted, empirical methodology for answering the question often asked with regard to AVs: “How safe is safe enough?” Moreover, no consensus exists on a single metric or methodology to demonstrate that an AV is safe. Accordingly, Waymo continues to learn from these various approaches but relies on *our own combination of methodologies* [emphasis added] to help ensure the ADS performs in a reasonably safe manner in its driving environment[8].

Even if one were to believe that Waymo’s experience, scale and business incentives will result in a service that is acceptably safe, some other company eager to gain market share in what they perceive as a winner-take-all market may set a much lower standard before fielding their vehicles. The answer to the lack of an established safety standard is not for regulators to throw up hands and say, “Let the companies decide.” Instead, NHTSA must build the “consensus...on a single ...methodology to demonstrate that an AV is safe.” ANSI/UL 4600 provides an excellent start.

3. Automotive software is often not very good.

In 2019, *one out of five* automotive safety recalls were the result of faulty software. The number of software recalls tripled from 2009 to 2019[9] The most common software problems requiring recalls were for braking and engine controls, two of the most fundamental aspects of vehicle control and safety. As just one example, Toyota’s faulty design resulted in a sudden acceleration malfunction that killed 89 people[10] and resulted in Toyota paying a $1.2 billion settlement of a criminal probe[11]. A jury verdict against Toyota established that defects in its Electronic Throttle Control System (ETCS) software and safety architecture caused the fatal mishaps.[12]

In January 2021, the Wall Street Journal reported on the root causes of VW’s delayed electric vehicle launch[13].

> "The car, however, didn’t work as advertised... the fancy technology features VW had promised were either absent or broken. The company’s programmers hadn’t yet figured out how to update the car’s software remotely. Its futuristic head-up display that was supposed to flash speed, directions and other data onto the windshield didn’t function. Early owners began reporting *hundreds of other software bugs* [emphasis

[8] https://storage.googleapis.com/sdc-prod/v1/safety-report/Waymo-Safety-Methodologies-and-Readiness-Determinations.pdf

[9] https://sibrostech.medium.com/the-current-state-of-automotive-software-related-recalls-ef5ca95a88e2

[10] https://www.cbsnews.com/news/toyota-unintended-acceleration-has-killed-89/

[11] https://www.washingtonpost.com/business/economy/toyota-reaches-12-billion-settlement-to-end-criminal-probe/2014/03/19/5738a3c4-af69-11e3-9627-c65021d6d572_story.html

[12] A Case Study of Toyota Unintended Acceleration and Software Safety, Phil Koopman, Carnegie Mellon University, https://www.youtube.com/watch?v=DKHa7rxkvK8

[13] https://www.wsj.com/articles/how-volkswagens-50-billion-plan-to-beat-tesla-short-circuited-11611073974

> added]. After years of development, Volkswagen decided in June last year to delay the launch and sell the first batch of cars without a full array of software... Electric vehicles are more about software than hardware. And producing exquisitely engineered gas-powered cars doesn't translate into coding savvy."

Recalls and failed product rollouts are the result of shoddy software development practices. As the Toyota sudden acceleration case showed, the auto industry often does not follow its own safety standards for software. In other safety critical industries such standards are either required by law or are universally used in practice (for example, the rail and the petrochemical industries). Automotive is one of the last hold-out industries in which the public must simply take the industry's own word that they have their software safety house in order.

A review of the Voluntary Safety Self Assessments from automated vehicle companies provided to NHTSA shows that only one company (WeRide) unambiguously states that it complies with ISO 26262. By contrast, Waymo simply chooses not to comply with ISO 26262. "However, Waymo does not rely strictly or exclusively on ISO 26262's principles, which are not a perfect fit for a Level 4 ADS, where there is a need for a special focus on the plethora of conditions likely to be encountered in the intended ODD…[14]" No standard is perfect but companies with strong safety cultures follow them anyway.

NHTSA should require automated driving systems to follow industry-written, industry-approved accepted practices for software safety such as ISO 26262. UL 4600 incorporates ISO 26262 and other existing standards into its broader safety case framework.

4. **UL 4600 is not prescriptive. It allows for continued innovation, but OEMs must present evidence that their automated systems are sufficiently safe.**

UL 4600 was developed by a diverse stakeholder group including representatives from the automotive and software industries. The standard does not prescribe how automated systems should operate rather it requires OEMs to make a comprehensive case, backed up with evidence, for why their system is safe. Safety case frameworks have been used in other industries with new and rapidly developing technologies and will allow companies to continue to innovate and compete on cost and performance.

5. **UL 4600 requires information sharing that will promote safety and fair competition.**

Crucially, UL 4600 requires OEMs to share information about potential problems with their systems so others can learn from their mistakes without requiring the disclosure of critical intellectual property. Mistakes include not just accidents but failures of an automated system to accurately identify objects even if that failure doesn't lead to an accident. This process continues after vehicles are deployed so their safety continues to improve. Sharing lessons

[14] https://storage.googleapis.com/sdc-prod/v1/safety-report/Waymo-Safety-Methodologies-and-Readiness-Determinations.pdf

about failures of automated systems allows every firm to build safer systems. NHTSA should not allow safety lessons to become proprietary and a means to block new entrants into the market. Rather NHTSA must create a shared database of best practices and edge cases to watch out for with automated systems. Companies can compete on technology, cost and performance but NHTSA must ensure that they all have access to the best information on how to build safe automated systems.

~~~~~~~~~~~~~

Big tech now dominates lobbying spending in Washington DC[15] so we expect NHTSA will feel strong pressure to maintain its hands-off approach to automated vehicle technologies. That would be a mistake. Even the best automated systems will inevitably fail at some point, killing and injuring innocent people. During this rulemaking, decision-makers at NHTSA should think about how they want to respond when the families and elected representatives of those killed by automated software systems call NHTSA representatives into a public hearing and ask: “What did you do to ensure that these systems were safe?”

“We relied on the company’s assurances” won’t satisfy them.

Sincerely,

Daniel Malarkey

Daniel Malarkey
Senior Fellow

[15] https://www.nytimes.com/2019/06/05/us/politics/amazon-apple-facebook-google-lobbying.html
~~~~~~~~~~~~~