The Center for Auto Safety
1825 Connecticut Ave. NW Suite 330 Washington, DC 20009
www.autosafety.org

December 3, 2018

Secretary Elaine Chao
U.S. Department of Transportation
1200 New Jersey Ave. SE
Washington, DC 20590

Submitted electronically via www.regulations.gov

RE: *Preparing for the Future of Transportation: Automated Vehicles 3.0*, Docket DOT-OST-2018-0149

Dear Secretary Chao:

The Center for Auto Safety ("the Center") appreciates the opportunity to comment on the Department of Transportation's ("DOT") publication of *Preparing for the Future of Transportation: Automated Vehicles 3.0* **("**AV 3.0"), the most recent version of the DOT's voluntary guidance regarding automated vehicles. The Center, founded in 1970, is an independent, non-profit consumer advocacy organization dedicated to improving vehicle safety, quality, and fuel economy. On behalf of our members, and all drivers, passengers, and pedestrians nationwide, the Center maintains our previous objections to the DOT's hands-off approach to basic safety regulation of AV technology. Additionally, the Center is disappointed that AV 3.0 expands this approach beyond the National Highway Traffic Safety Administration (NHTSA) to other DOT agencies.

In order to assuage public skepticism of AV technology, it is critical for the DOT to ensure that automated vehicles, and automated vehicle technology, are safe before allowing their introduction onto public roads. The best way to accomplish this goal is a measured approach that guarantees safety prior to deployment, using the existing tools and authorities provided to the DOT and its agencies. Instead, AV 3.0 turns effective safety regulation on its head, promoting unexamined, unlicensed, unregulated, and unsafe motor vehicle operation on public roads, with no assurance that even vehicles already proven unsafe will be barred from further operation. In fact, AV 3.0 even argues that establishing standards by which vehicles can be determined unsafe somehow runs counter to the interests of safety. Unfortunately, the DOT's continued commitment to voluntary guidance over effective regulation prevents the development of safeguards that would provide the public with basic information on the safety of AVs, and places users of American roads at the mercy of unproven technology.

This is not the first time the Center has called on NHTSA to utilize its current authority to require safety be built into AV technology prior to deployment. In fact, the consistency of the Center's position on the need for action in this area has only been matched by DOT's continued failure to act.

In response to DOT's version 1.0 voluntary guidance for autonomous vehicle development, we wrote: "The ongoing rush to achieve public acceptance and marketability of automated vehicles must not be permitted to minimize the critical importance of such issues, particularly as they address the potentially hazardous consequences of interactions between human operators, conventional vehicles using the highway system, and vehicles embodying various levels of automation. This will be true especially during the decades-long transition between today's driver-dependent fleet and the future potential for a fully-autonomous vehicle fleet. There are serious safety and ethical issues involved in AV which must be resolved by the government with input from the public. A voluntary approach that places automakers in direct control of the deployment of AV technology will not properly protect the driving public during this time of transition."[1]

In the Center's November 6, 2017 testimony on 2.0, we called for mandatory safety assessment reports, and a prohibition on testing on public roads. At the time, we said: "It would be in the best interest of all stakeholders to make sure that NHTSA, researchers, and the public have access to all the necessary data to assure the vehicles are performing as promised – and when there are problems – providing enough information for everyone to understand what happened. This includes making the type of information that is listed in the "Voluntary Safety Self-Assessment Template" on crashworthiness mandatory – and making the same true of the other 11 priority safety design elements. Currently, ADS 2.0 states that Safety Assessment letters are neither required nor is there any mechanism to compel entities to submit them – this must change."[2]

Unfortunately, the DOT's actions to this point make it clear that the department is uninterested in creating a framework that balances both corporate and public interests. Rather, DOT's voluntary approach rests on unproven assumptions and is based on strict anti-regulatory ideology and a willingness to completely defer to industry control over public safety. The most basic of public safety protections have yet to be pursued by NHTSA, which has broad authority in this area. To that end, the Center filed a petition for rulemaking in October to mandate the submission of safety information by companies testing self-driving vehicles on public roads.[3] Manufacturers have bristled at providing the public critical safety information for decades and are doing so once again with the

[1] Center for Auto Safety comment on 1.0, November 22, 2016, available here: https://www.autosafety.org/wp-content/uploads/2016/11/Federal-Automated-Vehicles-Policy-Comment.pdf.
[2] Center for Auto Safety Testimony on AV 2.0, November 6, 2017, available here: https://www.autosafety.org/wp-content/uploads/2017/11/Center-for-Auto-Safety-Written-Comments-for-11-6-17-NHTSA-AV-Listening-Session.pdf.
[3] Center for Auto Safety Petition for rulemaking requiring companies testing automated vehicle systems on public roads to provide information to NHTSA and the public regarding the safety of their systems, October 19, 2018, available here: https://www.autosafety.org/wp-content/uploads/2018/10/Center-for-Auto-Safety-Petition-for-Rulemaking-to-mandate-Safety-Assessment-Letter.pdf.

DOT's blessing in AV 3.0. Why is NHTSA promoting introduction of unlicensed vehicle operations on public roads without any supporting evidence of safe operation?

The Federal Motor Vehicle Safety Standards ("FMVSS") were established so that the industry would have design guidelines and requirements. They have been successful in incentivizing safety enhancements, have harmonized industry safety progress, and undeniably prevented countless tragedies. There is no evidence that similar regulation of the AV development would inhibit technology or undermine safety. What is missing is binding action by DOT and its agencies that would prevent major setbacks and allow truly life-saving, proven AV technology to be deployed on American roads. Such action is consistent with the DOT's traditional oversight and needed immediately as there are already multiple manufacturers who have deployed unproven vehicles in communities across the country. The history of auto safety has demonstrated time and again, mandatory standards are needed to ensure public safety. Autonomous vehicle technology is already on our roads. The time for DOT to act in the name of safety is now.

I. Flawed Assumptions underlying the DOT's Approach

The DOT's position in AV 3.0 is littered with unproven hypotheses, presumptions, and assumptions:

1. Assumption: Regulation stifles technological advancement.

AV 3.0 "Automation technologies are new and rapidly evolving. The right approach to achieving safety improvements begins with a focus on removing unnecessary barriers and issuing voluntary guidance, rather than regulations that could stifle innovation." P6. viii[4]

Regulations can enhance innovation by helping developers avoid dead ends, saving time and money. For example, investment in technologies that cannot provide adequate safety is wasted money. "Recent guidance issued by NHTSA calls for voluntary action surrounding automated driving safety, reflecting preferences to avoid both (excessive) regulation and chilling innovation while also protecting safety. That approach sets aside the possibility of the kind of regulation that a heterogeneous industry can agree to as broadly beneficial."[5] If safety compliance requirements are undefined, it is not possible to make compliant software, hardware, and algorithmic design decisions except by accident, which all can agree is a poor development approach.

[4] Page references throughout this Comment correspond to this version of *Preparing for the Future of Transportation: Automated Vehicles 3.0*, available here: https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf

[5] Measuring Automated Vehicle Safety, pg. 12, available at: https://www.rand.org/pubs/research_reports/RR2662.html

What DOT should do:

Establish objective AV safety standards to guide design and development as early as possible in the design cycle, removing the impediment to AV development, testing, and public acceptance caused by the current void.

2. **Assumption: Regulations applicable to current vehicles are "barriers" to the growth of technology and safe integration of AV.**

AV 3:0: "Identify and remove regulatory barriers to the safe integration of automated vehicles." Pg.5

Abdication of the duty to protect the public is an unacceptable approach to removing regulatory barriers. Current federal regulations provide very few barriers to the development and integration of safe automated vehicles, yet much is being made by the agency of "regulatory barriers" that so far haven't prevented manufacturers from testing on public roads across the country.[6]

AV 3.0: "There may be no steering wheel, accelerator pedal, brakes, mirrors, or information displays for human use. For such ADS-equipped vehicles, NHTSA's current safety standards constitute an unintended regulatory barrier to innovation." **Pg. 7**

NHTSA and automobile designers must carefully consider the human interface devices, potentially including conventional controls, that must be included in vehicles to preserve human life in the event of mechanical failures; or data processing, communication, or software errors in operational AVs.

There is a well-established inverse relationship between degree of transportation automation and the need for designed-in reliability, particularly when humans in the loop cannot safely recover from automation failure.[7] Inability of human passengers and other road users to safely recover from automation failure is clearly the case in many AV operational situations, particularly where there are no human interface devices available to affect vehicle operation (e.g., absence of steering wheel, brake pedals, gear selector, etc.). Safe design standards necessarily impact the design process. To minimize development cost and risk, these requirements must be included at the earliest possible moment in the design cycle.[8]

---

[6] As of October 12, 2018, 60 companies have been issued permits by California alone for autonomous vehicle testing, *see:* https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/permit. At least 39 other states have enacted legislation or executive orders related to autonomous vehicle testing, *see:* www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[7] "For ascent and descent space flight systems, the time constraints of the dynamic flight modes may preclude the opportunity to use in flight maintenance and system reconfiguration to recover from failures. Therefore, two failure tolerance is a critical element in ensuring adequate space flight systems reliability." NASA Procedures and Guidelines NPG: 8705.2 Effective Date: June 19, 2003 Expiration Date: June 19, 2008, Human Rating Requirements and Guidelines for Space Flight Systems.

[8] Systems Engineering for Intelligent Transportation Systems, available at: https://ops.fhwa.dot.gov/publications/seitsguide/section3.htm#s3.3.

NHTSA should establish safe AV control reliability standards immediately, so that AV designers can determine the minimum compliance cost design solutions (e.g., fault tolerant software design, high reliability components, redundancy, parallelism, supervisory controllers, etc.). There are many paths available to designers to conform to reliability standards at the beginning of a design cycle, but few when imposed late in design. DOT and NHTSA failure to establish standards exposes developers to increased development cost and risk, and unnecessarily exposes the public to lethal hazards.

AV 3.0: "U.S. DOT is in the process of identifying and modifying regulations that unnecessarily impede the testing, sale, operation, or use of automation across the surface transportation system." Pg. 35

Autonomous vehicle innovation, development, and deployment would also be accelerated by identification of regulations that impact software or hardware design. For example, objective requirements for cybersecurity and fail-over to safe state operations, are best implemented early in the design cycle to minimize cost and risk. These important design criteria cannot be incorporated if they do not exist. Self-imposed requirements by developers may be woefully inadequate without inputs from the government, public or third-party safety experts. Lives have already been lost due to myopic AV safety design. Implementing such design requirements late in the design cycle is very expensive and disruptive to development plans. It is simply not correct that the best regulation from either a public safety or business perspective is the one undefined.

AV 3.0: "These principles (on Data for Automated Vehicle Safety) include: Promote proactive, data-driven safety, cybersecurity, and privacy-protection practices." Pg. 31

Merely promoting, instead of requiring, safety, cybersecurity, and privacy protection practices is an inadequate approach to autonomous vehicle safety. Postponement of design-driving requirements also adds risk and cost to autonomous vehicle development because accomplishment of effective cybersecurity and software safety impacts both software and hardware design. Changes to either are very expensive to implement when introduced late in the design cycle. By abdicating its responsibility to establish software safety and cybersecurity requirements now, when they could be incorporated at minimal cost and risk, DOT erects unnecessary barriers and inhibits autonomous vehicle innovation and development.

AV 3.0: "Therefore, the U.S. DOT will not rush to regulate a nascent and rapidly evolving technology." Pg. 41

DOT does a disservice to the autonomous vehicle industry and the US public by abdicating its responsibility to establish reasonable requirements for safety and security. These requirements are needed to anchor autonomous vehicle design requirements, thereby reducing investor cost and risk. Incorporating these requirements early in the design cycle avoids the much larger cost of incorporation late in the design cycle. The DOT should also develop a comprehensive protocol for AV operator licensing so that

developers can incorporate those requirements in their development plans, avoiding the risk that free form development will be incompatible with the eventual need to satisfy road access and public safety official regulations.

What DOT should do:

Remove the roadblock to AV development that is caused by inadequate definition of AV operational safety requirements.

3. **Assumption: Industry can be trusted to accurately inform DOT and consumers of the safety risks of technology.**

AV3.0 "Affirms the approach outlined in A Vision for Safety 2.0 and encourages automated driving system developers to make their Voluntary Safety Self-Assessments public to increase transparency and confidence in the technology." Pg. viii

The approach outlined in A Vision for Safety 2.0 was regressive and inadequate and is not an appropriate basis for AV safety.

Encouragement to release Voluntary Safety Self-Assessments alone is inadequate to protect the public. Those released to date include little useful information.[9] The Center believes that safety plans and assessment must be available for public review and comment; they must include an effective strategy for data recording and outside review of safety-related operational data to assure collision reconstruction, post-collision safety, and root cause determination; and NHTSA must retain authority and ability to bar AV operation on public roads following safety assessment review and public comment.

Third party validation and gated AV certification as described in the Appendix to this document and in the forthcoming Center comments on the proposed AV Pilot Program[10] would build confidence in public safety.[11]

What DOT should do:

Develop a gated certification AV operator licensing protocol that includes public disclosure of safety data sufficient to establish meaningful demonstration of compliance with safety requirements included in the protocol.

---

[9] https://waymo.com/safety/, https://www.gm.com/content/dam/company/docs/us/en/gmcom/gmsafetyreport.pdf, https://blogs.nvidia.com/blog/2018/10/23/introducing-self-driving-safety-report/, https://media.ford.com/content/dam/fordmedia/pdf/Ford_AV_LLC_FINAL_HR_2.pdf, https://www.tesla.com/blog/q3-2018-vehicle-safety-report, https://www.uber.com/info/atg/safety/

[10] See Appendix to this document.

[11] Ibid, pg. 25, "As an illustrative option drawing from work by the California PATH Program, a manufacturer generates a safety plan including ODDs and behavioral competencies. If acceptable, a third-party tester decides on a set of test cases to be conducted in a closed course. If the performance of the vehicle is sufficient, the tester or state DMV would conduct various maneuvers on public roads."

4. **<u>Assumption: Industry can be trusted to provide comprehensive reporting of crash data.</u>**

AV 3.0: "Public trust can be built during testing by using an in-vehicle driver engagement monitoring system, a second test driver, or other methods." Pg 30.
The Center agrees with this sentiment, however, it is equally important to note that public trust is diminished by the refusal of DOT to establish a comprehensive licensing protocol for ADS, and is also diminished by developer restrictions on investigator access to crash data sufficient to establish root cause and corrective actions. To build public trust, DOT and NHTSA must require recording and preservation of vehicle safety-related data and unfettered access by official investigators sufficient to determine the cause of autonomous vehicle crashes as part of its autonomous vehicle licensing protocol.

What DOT should do:

Develop requirements for AV event data recorders that include sufficient data collection and preservation from before, during, and after an event that jeopardizes human safety to assure determination of root cause and corrective action, including assuring unfettered access to that data by public safety officials without developer involvement.

5. **<u>Assumption: Complying with wide-ranging voluntary standards adopted from multiple sources is more cost effective and less confusing than mandatory single-source standards compliance</u>**.

AV 3.0: "Standards could provide for a range of potential behaviors—e.g., speed, distance, angles, and size—for surrogate vehicles, pedestrians, and other obstacles that ADS-equipped vehicles would need to detect and avoid." Pg. 7;

"Supports the development of voluntary technical standards and approaches as an effective non-regulatory means to advance the integration of automation technologies into the transportation system." Pg. viii;

"Establish performance-oriented, consensus-based, and voluntary standards and guidance for vehicle and infrastructure safety, mobility, and operations." Pg. 5

Simply put, voluntary technical standards are inadequate to assure public safety.

It isn't clear which voices would be included in 'consensus-based' standards or how conformance to those standards would be verifiable except in court proceedings. The history of auto safety demonstrates time and again that voluntary standards will not be sufficient to assure public safety.

What DOT should do:

Establish sufficient force of law behind AV safety standards to provide a basis for the NHTSA Administrator to carry out the agency's duty to protect the public. Uniform mandatory safety standards are preferred to a patchwork of voluntary standards.

Establish a uniform set of safety standards so that meaningful comparisons between and among developers can be made. Complete abdication of NHTSA's responsibilities does not promote AV development, implementation, or public acceptance.

Promote transparency and consistency among developers that can help assure adequate scope of simulation and test in development.[12] *Absent enforceable standards and public review of conformance, as is currently the case, there is no available mechanism for providing public assurance of AV safety.*

AV 3.0: "**First, companies developing and deploying automation technology need to be transparent about vehicle safety performance." Pg. 26**

The Center agrees there is a need for transparency about vehicle safety performance. A necessary part of that transparency is a requirement that data recorders capture safety critical data before, during, and after a crash to allow resolution of root cause and contributing factors of a crash and its aftermath, including late onset fire ignition (which have been reported in AV crashes). To assure transparency, AV developers may not be permitted to treat safety-related data as proprietary data under their exclusive control, must be required to share it freely with responsible government officials, and must assure that the data are formatted and stored so that they are available to investigators and other stakeholders without procedural or technical restrictions.

AV 3.0 "**However, delaying or unduly hampering automated vehicle testing until all specific risks have been identified and eliminated means delaying the realization of global reductions in risk." Pg. 2**

Establishing objective criteria for evaluating safety and objective determination of developer compliance with those criteria are not 'unduly hampering automated vehicle testing.' On the contrary, establishment of compulsory national safety standards would promote testing and AV development by obviating development and demonstrating compliance with individualized criteria for each additional jurisdiction, and potentially reduce the potential for tort litigation through developer compliance with compulsory safety criteria. Furthermore, without sufficient data obtained via objective testing, the realization of a "global reduction in risk" is nothing more than a marketing slogan.

6. **<u>Assumption: Self-certification is preferable to proof by examination of safety compliance, as it more appropriately balances safety and innovation.</u>**

AV 3.0: "Reaffirms U.S. DOT's reliance on a self-certification approach, rather than type approval, as the way to balance and promote safety and innovation; U.S. DOT will continue to advance this approach with the international community." Pg. 7

[12] Ibid, pg. 25, "Exploiting the expectation that companies will teach to the test, having common scenarios, simulators, or related standards in the demonstration period could present an opportunity to ensure parity earlier in the development process."

The proposition that self-certification is a binary alternative with respect to type approval postulates a false alternative. Gated certification is an optimal approach to examination and safety demonstration to ensure functional safety that, while comprehensive, does not impose burdensome design disclosure and analysis that is an intrinsic part of type approval. AV licensing using gated certification as described in the appendix,[13] focusing on objective operational criteria rather than design, would certify safety at a regulatory level far less intensive than type approval.

AV 3.0: Safety Risk Management Stages along the Path to Full Commercial Integration, Pg. 36

The Center agrees with the concept of safety risk management in stages for AV. The Center believes that the correct approach is gated certification as part of a comprehensive autonomous vehicle operator licensing protocol. A recommended approach to AV operator licensing via gated certification may be found in the appendix or in the Center's forthcoming response to NHTSA's request for comment on AV pilot program.[14]

AV 3.0: "However, reliance on a self-certification approach, instead of type approval, more appropriately balances and promotes safety and innovation;" Pg. 7

This statement has no objective basis and is purely conjecture. There must be factual support for this statement before it can become policy. This statement contradicts analysis of options for AV development that concludes in part, "A formal protocol for the demonstration process (which could apply to simulators, simulations, and scenarios) would facilitate comparisons across companies and evidence of safety to the public and policymakers. This might suggest a role for a third party or department of motor vehicles."[15]

AV 3.0: Safety Risk Management Stages along the Path to Full Commercial Integration, Pg. 36

The Center agrees with the concept of safety risk management in stages for AV. The Center believes that the correct approach is gated certification as part of a comprehensive autonomous vehicle operator licensing protocol. This approach is outlined in detail in both the appendix to this comment and the Center's forthcoming comments on the proposed AV pilot program.[16]

What DOT should do:

Develop safety standards for AV operations in the context of a gated certification procedure for graduated licensing of AV operators.

[13] See Appendix, Sec. 1.3.
[14] See Appendix.
[15] *Supra* FN5, pg. 59.
[16] See Appendix.

7. **Assumption: State and local authorities do not have a role in defining and regulating AV operational design domains**.

AV3.0: "U.S. DOT's role in transportation automation is to ensure the safety and mobility of the traveling public while fostering economic growth…To accomplish these goals, the Department works closely with stakeholders in the private and public sectors to pursue the following activities:…Ensure national consistency for travel in interstate commerce." Pg. 5

Requiring developers to conform to uncoordinated rules and regulations promulgated by numerous state and local agencies responsible for public safety is inconsistent with ensuring safety while fostering economic growth. On the contrary, establishment of Federal safety standards in coordination with states and compliance enforcement are the best way to both assure consistency in interstate commerce of AV and minimize AV development cost and risk.

AV 3.0 "Existing standards assume that a vehicle may be driven anywhere, but future standards will need to take into account that the operational design domain (ODD) for a particular ADS within a vehicle is likely to be limited in some ways that may be unique to that system." Pg.7

Objective validation of AV operational restriction to its ODD must also be part of related standards development and AV operations licensing. This cannot be satisfactorily validated by voluntary standards compliance alone.

Vehicles must be able to operate outside of their ODD on at least a temporary or emergency basis because there cannot be assurance that the AV will never be physically transported or directed outside of its ODD, nor that remote software changes can restrict or modify the ODD while the AV is physically located outside of its ODD. (In the most obvious example, the confines of the factory floor in which the AV is built and from which it must be moved would not be within its ODD.)

It is not clear who determines the ODD scope. Would it be the manufacturer, the licensed operator, the owner, the vehicle occupant, a government official, or anyone at all? This is an important question that must be answered before safe AV operation can be assured. It is also unclear what significance ODD determination has if it is not part of and AV operation licensing protocol. It is meaningless with respect to public safety unless it is coupled with a determination of safety and a means of enforcement. Establishment, approval, and validation of ODD are discussed in the Appendix.

AV 3.0 "**Test procedures could also be developed to ensure that an ADS does not operate outside of the ODD established by the manufacturer." Pg. 7**

This statement implicitly requires ODD establishment by the manufacturer, yet there is no supporting requirement that the manufacturer do so, nor is there a regulation that

prohibits ODD modification by any third parties, including the AV owner. To be meaningful, ODD establishment, administration, and regulation must be a part of AV operator licensing requirements.

AV 3.0: "As part of their important role in the safety assurance of ADS-equipped vehicles, entities are also encouraged to consider such conditions [at-grade rail crossings, roundabouts, bicycle lanes, pedestrian walkways and special designated traffic lanes or crossing areas, entrances and driveways, and other potential hazards, especially in different roadway landscapes (e.g., urban versus rural)] in the design, testing, and validation of the designated fallback method." Pg. 30

It is unconscionable that DOT allow autonomous vehicles to operate on public roads with only voluntary, optional consideration of safety under the listed conditions. It is unsafe to allow vehicles to operate in public without requiring safe operation in and around the listed and other incidental but very common transportation infrastructure features. DOT and NHTSA cannot both assert their advocacy for road safety and simultaneously allow autonomous vehicle developers to ignore, for only one example, at-grade rail crossing safety. Safe operation must be required, not 'encouraged', at all these conditions, and others that may be identified by safety advocates, local or state officials, and other members of the public. It is tragically ironic to include in AV 3.0 the following statement, **"Entities are encouraged to engage with the U.S. DOT and infrastructure owners and operators to understand the full ODD for safe and efficient operations of automated vehicles,"**[17] when the U.S. DOT is unwilling to require specific safe operational requirements or even meaningful safety guidelines under any foreseeable circumstance.

The meaning of 'designated fallback method' on pg. 30 is undefined. This is the only instance of this term in the document. Safe autonomous operation demands that any failures inhibiting safe operation in any circumstance be identified and cause reversion to a safe mode preserving the occupants' lives. The use of the term 'designated' requires that someone be the designator. Who is that entity? In practice, it is unlikely and probably unsafe for a single fallback method to be appropriate for all operational situations, so NHTSA should clarify the meaning of this statement.

AV 3.0: "Entities are encouraged to engage with the U.S. DOT and infrastructure owners and operators to understand the full ODD for safe and efficient operations of automated vehicles." Pg. 30.

It is unacceptable that autonomous vehicle developers are merely encouraged to, "…understand the full ODD for safe and efficient operations of automated vehicles."[18] Autonomous vehicles cannot be operated safely if developers do not consider the full ODD for safe operations. Encouragement is insufficient. A minimum design requirement is both understanding, designing for, and verifying safe operation in "…the

[17] AV 3.0, Pg. vi.
[18] Ibid. at Pg. 30.

full ODD for safe and efficient operations of automated vehicles."[19] ODD definition, approval, and compliance certification should be part of a comprehensive AV operations licensing protocol such as the gated certification approach described by the Center in its NHTSA filings.[20]

AV 3.0: "Safety Risk Management Stages along the Path to Full Commercial Integration," Pg. 36

The Center agrees with the concept of safety risk management in stages for AV. The Center believes that the correct approach is gated certification as part of a comprehensive autonomous vehicle operator licensing protocol. Additional details of a proposed comprehensive approach to safety risk management are provided in the Appendix.

What DOT should do:

Establish guidelines and requirements for ODD establishment, approval, compliance certification, and enforcement, including safety fallback requirements.

8. **Assumption: Identifying and licensing legally responsible operators is not needed for AV operations, and states do not have the legal authority to license AV systems based on demonstrated driver safety performance, when this is exactly what states have been doing with human drivers for many decades.**

The meaning of 'operator' or 'driver' must be established in the context of automation, and the 'operator' must be licensed. The alternative is NHTSA's support for unlicensed motor vehicle operation on public roads, which is unacceptable. In an AV with automated controls outside of occupant control, the control software licensor must be considered the operator, since that software executable is the sole means of operational control. The operator must be licensed and, consistent with established practice for humans, minimum requirements for licensing with appropriate examinations must be established and enforced for AVs such as the gated certification approach described by the Center in the Appendix.

AV 3.0: "**Performance-based safety standards could require manufacturers to use test methods, such as sophisticated obstacle-course-based test regimes, sufficient to validate that their ADS-equipped vehicles can reliably handle the normal range of everyday driving scenarios as well as unusual and unpredictable scenarios." Pg. 7**

We are pleased to see DOT's recognition that performance-based safety standards 'could be' established. The Center maintains our position that in the interest of public safety they must be established. Further, that such standards must be established by NHTSA, consistent with its charter for protecting public safety. Performance-based safety standards need to be established and incorporated into AV operator licensing. The Center

[19] Ibid
[20] Please see Appendix.

recommends the gated certification approach for AV operator licensing described in the appendix and in its forthcoming response to the NPRM for a proposed AV Pilot Program.[21]

AV 3.0: "Notably, however, in the case of vehicles that do not require a human operator, none of the human-specific FMCSRs (i.e., drug testing, hours-of-service, commercial driver's licenses (CDL)s, and physical qualification requirements) apply." Pg. 9

We disagree that the requirement for a commercial driver's license does not apply. There must be a process for licensing and examining operators of commercial vehicles, even if the operator is exercising control via an ADS. Identification and examination of the operator is necessary to establish single point AV control, assign liability and assure public safety. The alternative is that unlicensed operators will be controlling unregulated, potentially unsafe commercial vehicles on public roads and roads. The Center recommends a gated certification process, comprising gates analogous to a vision test for vehicle components and software, a learner's permit that allows limited operations to verify control safety and efficacy, and examination of provisional operations with respect to objective operational safety standards to ultimately grant an AV operator's license.

AV 3.0: "The Department will carefully consider the appropriate division of authority between FMCSA and the States on how or whether CDL qualifications should apply to computerized driving systems." Pg. 9

The Center maintains CDL requirements can and do apply to ADS-equipped commercial vehicles, and that such vehicles must be licensed to operate on public roads via a gated certification process, as outlined in the Appendix.

AV 3.0: "Current FMCSRs would continue to apply, and motor carriers can seek regulatory relief if necessary. Carriers therefore may deploy ADS-equipped CMVs in interstate commerce, using existing administrative processes. Pg. 10"

The Center disagrees that the second statement is the logical corollary of the first. The Center believes it is unsafe to deploy ADS-equipped CMVs in interstate commerce unless and until an 'operator' has been identified, operational liability has been assigned to the operator, and the operator has been appropriately licensed, including examination of its compliance to objective operational safety requirements. CMV operational safety is not enhanced by employment of arbitrarily validated and potentially unapproved software by the AV operator with unknown and uncertified performance capability or safety. Speculative, unexamined conformance of self-driving CMVs to FMSCRs, which were developed and promulgated with the assumption of licensed human drivers, without operational compliance examination and verification is inadequate to assure public safety.

[21] Please see Appendix.

AV 3.0: "FMCSA will also consider whether there is a reasonable basis to adapt its CDL regulations for an environment in which the qualified commercial driver may be an ADS." Pg. 10

The Center believes that CDL regulations must be adapted to define the 'operator' of autonomous CMVs and examine operator conformance to objective operational safety requirements.

AV 3.0: "States may consider identifying and addressing issues that are unique to companies providing mobility as a service using automated vehicle technologies." Pg. 20

The Center agrees that states must also consider the nature of the 'operator' of an autonomous vehicle, and the legal responsibilities of the operator. Federal regulations may be required to establish that the autonomous vehicle software licensor and/or the manufacturer mounting that software in the vehicle are in fact the operator and have legal responsibility for the vehicle's safe operation. DOT should establish national standards and model legislation to assure consistency among the states and across jurisdiction borders, including international boundaries, where autonomous vehicles might be operated. Failure to address designation and licensing of an AV 'operator' is a barrier that impedes innovation and development of autonomous vehicles. Removal of that barrier by establishing appropriate regulations is within NHTSA's legal authority and jurisdiction.

AV 3.0: "Where testing is taking place, State and local agencies should consider ways to establish consistent cross-jurisdictional approaches and work with first responders to develop commonly understood traffic law enforcement practices and emergency response plans for automated vehicle testing and operation." Pg. 21

This statement acknowledges that safety requirements need to be imposed on autonomous vehicle development. Compliance with a multitude of state and local requirements is an expensive and risky burden for developers. Abdication of Federal safety requirements development assures that a patchwork of potentially conflicting state and local regulations will persist, impeding the development and deployment of autonomous vehicle technology.

AV 3.0: "State and local agencies and industry may work together to identify data elements that will help automated vehicles navigate challenging, unique roadway environments and alter operational behavior in relation to changing traffic laws." Pg. 22

Any and every action to "… alter operational behavior in relation to changing traffic laws," is either a design or parameter change to an autonomous vehicle's physical components, software, or operating system. This statement opens the door to unlimited and uncontrolled changes that must be accommodated by developers, and changes that, absent appropriate regulations up front, must be accommodated at an advanced stage of

development and test where such changes are very expensive. DOT would remove a barrier to autonomous vehicle development not by stepping aside but by setting ground rules for development that anticipate local variations and include those ground rules in compulsory safety guidelines for AV development. This is an affirmative step that would remove a barrier to AV development.

AV 3.0: "FHWA suggests working with automated vehicle developers, traffic engineers, and law enforcement stakeholders to revise the UVC to be consistent with automated vehicle operations." Pg. 22

The Center agrees that the UVC must be consistent with automated vehicle operations. The Center also believes that it is incumbent upon DOT to promote the development of consensus standards as quickly as possible and incorporate them into mandatory safety standards so that autonomous vehicle developers will be able to incorporate those requirements in design at the earliest possible opportunity. Design modifications late in the design cycle are very expensive and inconsistent with system engineering practices endorsed by DOT.[22] Failure to establish supportive safety requirements adds risk, adds cost, and unnecessarily impedes development of autonomous vehicles, a self-imposed barrier to AV development that NHTSA can readily remove by establishing safety and reliability standards.

What DOT should do:

Develop AV operator examination and licensing protocols defining responsibilities between Federal and state implementation, similar to the hierarchy of CDL requirements.

9. **Assumption: Cybersecurity vulnerabilities can be addressed by a voluntary reporting process.**

AV 3.0: "U.S. DOT … supports the development of voluntary standards that can enable the safe integration of automation." Pg. 12

"Transportation-related cyber vulnerabilities and exploits can be shared with Government partners anonymously through various Information Sharing and Analysis Centers (ISACs)." Pg. 17

Voluntary compliance by developers to standards that do not yet exist may lead to gaps in cybersecurity with lethal and expensive consequences. The DOT should establish a mechanism for mandatory sharing with the government and among autonomous vehicle developers of cybersecurity threats, issues, intrusions, and remedies to protect both manufacturers and the American public. Cybersecurity and responses to breaches should not be used as a competitive advantage by any company.

[22] *Supra at* FN 8.

What DOT should do:

Require AV operational cybersecurity and develop standards for its implementation.

II. Other Comments/Concerns with AV 3.0

AV 3.0: "The best way to accomplish FMCSA's core mission of reducing fatalities and crashes involving large trucks and buses is to avoid unnecessary barriers to the development of ADS in commercial vehicles." Pg. 8

We disagree with this unsupported, and dangerously presumptive statement. The Center believes the best way to accomplish FMSCA's safety mission is to require AV compliance with a rigorous performance-based licensing process for operators of ADS in commercial vehicles. It is an unconscionable abdication of responsibility to deviate from historical licensing precedents merely because a vehicle is primarily or exclusively controlled by on-board or remote, partial or full potentially unvetted, unexamined, and unattributed automatic controls. The AV operator and its cyber implementation must be identified, examined, and licensed before AV or ADS-equipped vehicle is allowed to use public roads. Moreover, immediately requiring existing advanced technology on new vehicles, such as automatic emergency braking and lane departure notification would (with proper performance standards) improve safety for everyone on the road in the near future, not in the distant one that is envisioned when level 5 autonomous vehicle technology is finally realized.

AV 3.0: Communication both between vehicles (V2V) and with the surrounding environment (V2X) is an important complementary technology that is expected to enhance the benefits of automation at all levels but should not be and realistically cannot be a precondition to the deployment of automated vehicles." Pg. 13

While there is great potential promise from the use of V2V and V2X, the Center agrees that V2X should not be precondition to the deployment of automated vehicles. The Center also believes that autonomous vehicles, whether or not designed with V2X connectivity, must be able to operate safely in the absence or failure of V2X. DOT and NHTSA must develop safety requirements that preserve occupant safety in the events of V2X absence, intermittency, failure, corruption, or malicious alteration of V2X signals, and demand developer compliance to those requirements.

AV 3.0: "Safety risks, such as driver distraction and confusion, should influence early stages of design and vehicle development." Pg. 30

The Center agrees with this statement. The Center also believes that such safety risks need to be considered as design constraints in all levels of automation where vehicle occupants can or must exercise vehicle operational control by any means. Automatic compliance with occupant commands without consideration of current vehicle operational state, environmental conditions, and environs can create lethal hazards for both the occupied vehicle and other road users. Further, an autonomous vehicle must be

capable of rejecting malicious commands from any source within or external to the vehicle to protect both vehicle occupants and other road users.

AV 3.0: "Entities could consider methods that ensure driver awareness and engagement during ADS-equipped vehicle testing, to mitigate the potential for distraction, fatigue, and other possible risks." Pg. 20.

This sentence suggests that DOT also finds it acceptable that ADS-equipped vehicles may not consider methods that ensure driver awareness and engagement. This unacceptable condition for automated driving and automated driving assistance has already led to multiple deaths. This AV 3.0 statement, with an aspiration to encourage rather than require, is yet another example of DOT's abdication of its responsibility to establish and promote autonomous vehicle road safety.

AV 3.0: "Public education challenges are different for automated vehicle technologies at higher levels of automation or Level 4 and Level 5 systems, where the consumer becomes a passenger rather than a driver." Pg. 29

DOT and NHTSA need to establish regulations to identify the 'operator' at SAE Autonomy Levels 4 and 5. Without Federal definition, it is likely that each state or local government will develop its own definition. Safety will suffer as responsibility becomes diffuse. Development cost and risk will rise as (potentially contradictory) requirements proliferate. The definition of 'operator' also has design implications, since it will affect how operational instructions are delivered to the autonomous controls, how the controls are implemented in hardware and software, and how these instructions are updated while the vehicle is underway and outside of the modified constraints. It is difficult, risky, and expensive to modify either hardware or software design late in development. NHTSA's abdication of this task unnecessarily erects a barrier to autonomous vehicle development at the same time as it degrades operational safety.

Public education should encompass AV reliability as well as safety, since control reliability will affect safety of AV passengers as well as other road users. Software design, data processing components, computing system architecture, algorithm maturity and testing, road testing, and mechanical reliability all contribute to overall AV safety and confidence. These are all included in the recommended gated certification[23] process, which the Center believes is the best approach to public education and confidence building.

III. Conclusion

With the publication of AV 3.0, once again, the Department of Transportation has taken an opportunity for progress and managed to accomplish a feat of regression. Instead of "Preparing for the Future of Transportation," which is the title of the publication, this

[23] Please see Appendix.

document cements a completely hands-off approach when it comes to regulating autonomous vehicle technology. Perhaps even more disturbing is that this philosophy has now metastasized to other agencies within the Department with the advent of AV 3.0.

By affirming a position that not only fails to mandate safety, but actively looks to find ways to "unburden" industry from even having minimal safety requirements, such as the submission of basic safety information about self-driving cars being tested in public, the message is clear to the public: you are on your own.

The Center's comments above, and in the Appendix below, are based on the precepts of NHTSA and DOT fulfilling their public service and public safety missions, sometimes even at the risk of adding some minimal short-term costs to industry. The auto industry has demonstrated time and again that absent meaningful oversight it will find ways to sabotage itself in the interest of short-term profits and create long-term health and safety risks for consumers. Sadly, the modern technology industry does not have a better track record.

Instead of a serious framework for how the government will simultaneously provide safety and assist industry in revolutionizing vehicular transportation for the benefit of all, DOT has chosen to publish a glossy brochure masquerading as a policy document. In fact, AV 3.0 looks like it was published by the industry with its failure to require the disclosure of the type of data that would allow for an objective measurement of how close – or far – any given set of autonomous vehicle technology is from deserving to be on our public roads. All parties want to see reduced crashes, deaths, and injuries. Perhaps in AV 4.0, DOT will take real steps towards making that goal a reality.

Sincerely,

Jason Levine
Executive Director

APPENDIX 1 – GATED CERTIFICATION PROGRAM

1.1. **PUBLIC SAFETY** demands that every motor vehicle operated on the nation's public roads be controlled by a licensed operator, qualified by examination, with no exceptions. This simple notion underlies all Federal, state, and local road laws; vehicular tort case law; commercial, for-hire, and private licensing; vehicular law enforcement; operator training and certification; and vehicular design. There must be no exception for high and full driving automation[24] and associated equipment. For high and full driving automation, when the vehicle occupants are not in control of operations or there is no human vehicular occupant, the AV developer[25] is the operator. Passive vehicle occupants are not operators, any more than a taxi passenger is a taxi operator. The high and full driving AV developer is the vehicle operator whether the software is embedded in the vehicle or the vehicle is operated (partially or fully) via remote inputs or affirmative control.

The Center believes that a gated certification licensing program proving conformance to objective safety standards as enumerated below in section 1.2, using examinations as described in section 1.3 is an essential element to ensure the safety of human beings when it comes to high and full driving automation equipped vehicles being tested on public roads. There is ample precedent for such an approach to demonstrating operator competence in the area of a specialized vehicle's operational capabilities. The program would be modelled on the Federal requirements for commercial driver's license and include three gates. These gates, described in more detail in section 1.3 below, are analogous to the present qualification for an operator's driver's license.

1.2. **OBJECTIVE OPERATIONAL STANDARDS** must be established immediately so that designers and engineers can develop governing design requirements. Establishing these requirements are the foundation of cost-effective engineering design and development.[26] The Center recommends the following set of objective safety requirements, for compliance by automated driving systems (ADS) and AV developers:

1.2.1. **AV's shall do no harm**.

Prove[27] that AV technology is safer for both occupants and the public and is as environmentally benign as the equivalent or comparable model year technology available in a full-time human-operated vehicle without AV technology

[24] Automated Vehicles for Safety, https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety , High Automation = Level 4, Full Automation = Level 5

[25] "AV" means autonomous vehicle which is a motor vehicle equipped with high or full automation capability, and "AV developer" is the legal entity that manufactures or provides vehicles equipped with high or full driving automation capability for sale or public use.

[26] http://www.fdot.gov/traffic/its/projects_deploy/SEW/2012_september/SE%20WS%20Session%203%20V%202012-08-29.pdf

[27] The term "proof" as used herein is statistically significant evidence of demonstrable, safe, repeatable, and reliable AV performance.

implementation. AV developers must prove that both test vehicles and vehicles offered to the public for sale or use enhance occupant, driver, and public safety in all specified, experienced, modeled, and tested operational conditions.

Prove that the vehicles modified to include AV capabilities are at least as safe in collisions for all occupants, emergency responders, and recovery personnel as comparable model year full-time human-operated vehicle or equivalent without AV technology.

1.2.2. AVs shall provide built-in-test (BIT)/built-in-diagnostics (BID) to verify safe operational capability prior to embarkation and during operations.

Prove that the AV has BIT/BID capability that identifies and safely mitigates any hardware, software, communications, or data processing fault that might arise before, during, or after passenger transportation.

1.2.3. AVs shall always defer to commands by a designated occupant.

Prove that the AV will:

- override preprogrammed or remote operational commands in favor of commands by designated occupant,
- discriminate between commands by the designated occupant and other occupants
- ignore commands by other occupants
- enable the designated occupant to reassign operational control responsibility to another occupant if necessary or desired
- only accept unambiguous control inputs.

1.2.4. AVs shall respond promptly and appropriately to emergency and public safety vehicles, to emergency situations as directed by emergency personnel, and to police instructions in all traffic situations.

Prove that the AV is capable of responding appropriately and safely to lawful signals and commands from police, fire, ambulance/EMT and other public officials in all traffic conditions, including:

- emergency vehicle lights and sirens,
- yielding to emergency vehicles
- responding to hand, verbal, and visual commands and
- obeying commands that contravene conventional traffic rules (e.g., directions to detour the wrong way down a one-way street).

1.2.5. AVs shall safely transition to occupant control.

Prove that AVs equipped for primary or optional human operational control have suitable control devices, provide human operators with sufficient time and situational awareness to take control, and have a default safe shutdown capability if the human operator cannot or does not take over control safely when needed.

1.2.6. AVs shall assure occupant situational awareness and safe egress.

Prove that AV occupants are notified of any imminent hazardous condition in the vehicle that potentially compromises safety and provides a means for safe passenger egress at any time, for any reason.,

1.2.7. AVs shall provide cybersecurity.

- Prove that the AV will automatically transition to a safe operational fall back state (i.e., minimal risk condition response to faults or failure) in the event of any safety-critical cybersecurity breach; and that AV data processing is secure, reliable, and uncompromised by:
    - communication faults whether caused by communication equipment, terrain, or weather
    - spoofing or misdirection
    - malignant software, firmware, data processing equipment, or other logic-bearing components resident in the AV or remote control system components.

1.2.8. AVs shall respect their mechanically limited and logically limited geographic operational limits.

Prove that the AV cannot be:

- directed to destinations, conditions, or terrain that are outside of its safe automatic operational envelope (its operational design domain [ODD])
- programmed to endanger passengers by routing to a dangerous destination outside of its safe operational limits, and
- that occupants and/or controllers will receive appropriate notification of vehicle fuel or performance limitations inhibiting executing destination instructions in time for them to effectively remedy the condition.

1.2.9. AVs shall respect naturally occurring inclement weather and hazardous environmental conditions.

Prove that the AV will respond safely to naturally occurring weather emergencies (e.g. squalls, thunderstorms, tornadoes, hurricanes, flooded roads, etc.) and other suddenly emerging natural environmental concerns (e.g.,

earthquake, sinkholes, forest fires, dust storms, lava flows, solar or lunar interference with sensors, etc.) that could compromise occupant safety even if such conditions unexpectedly arise after the AV embarkation.

1.2.10. AVs shall appropriately respond to compromising, unusual or undocumented artificial road conditions.

Prove that the AV detects and responds appropriately and safely to unplanned or emergency road conditions due to human action or inaction (e.g., potholes, flag persons, toll booths whether manual or automated, emergency road closures, temporary and dynamic traffic patterns at construction sites, road debris, sensor-disabling glint from surfaces, other vehicles, stray light from illuminations or signs, etc.)

1.2.11. AVs shall protect occupants from uncontrolled or malicious drivers in other vehicles.

Prove that the AV provides a safe response to other drivers performing unsafe or illegal acts that potentially endanger AV occupants.

1.2.12. AVs shall implement data recorders[28] that provide public safety officers and government officials necessary access to operational history and state necessary to understand the cause of a crash.[29]

Manufacturers must:

- include a survivable data recorder
- provide the capability to resolve the state of an AV prior to and immediately following a crash, including sufficient detail on all safety-critical data including speed, environmental conditions, programmed instructions, operational state and user-selectable operational options, communications, data processing capability, and software/firmware configuration to allow unambiguous reconstruction of events leading to the crash and resolution of root cause
- enable recording, archival, and independent access by authorized officials to safety critical data that must be recorded and provided in flat files using non-proprietary formats so that they can be recovered, read, and analyzed without intervention of the AV manufacturer.

1.2.13. AVs shall detect and respond appropriately to collisions.

Prove that an AV will:

[28] See SAE standard Event Data Recorder J1698_201703

[29] https://www.axios.com/when-avs-crash-limited-data-access-can-impede-investigations-fb1440cd-36c0-4115-9cd0-930703cff44d.html

- automatically detect collisions with other vehicles, vulnerable road users, or property,
- automatically and safely stop after the event
- automatically summon emergency response
- allow third parties including witnesses, victims, and law enforcement officers (without electronic access to proprietary operational data) to access operator, vehicle identification, and insurance data (analogous to human drivers exchanging license, registration, and insurance information after a crash).

1.2.14. AV developers shall prove that they have the financial resources to cover the risks that AV development, test, and operations on public roads entail.

Prove that the AV developer has sufficient liquid assets, insurance, security bond, or equivalent to settle claims due to property damage, injury, or death caused by the AV.

1.2.15. AV manufacturers shall provide conspicuous visual and audible warning of automatic vehicle operation to other users of public roads prior to completion of operator licensing.

Prove that a developmental vehicle tested on public roads without a fully licensed operator will be clearly visible and audible to other road users so that they can protect themselves against hazardous AV maneuvers that might occur, analogous to the "STUDENT DRIVER" signs used during human driver training.

1.3. **Recommended Gated Certification** is a disciplined process by which a knowledgeable third party documents that an engineering development conforms to the established set of requirements, such as those listed above. This approach is commonly used in complex projects that expose the public to risk, whether by FAA certification of airlines, Coast Guard certification of ships, professional engineer certification of civil engineering structural designs, Underwriter's Laboratory certification that electrical devices are safe for public use, elevator inspectors reviewing design and operations, etc. All vehicles legally operated on US roads are under the control of licensed operators who have been qualified by proof of capability and competency at incrementally more demanding levels of performance.[30] Vehicles with high and full driving automation and associated

[30] Texas CDL requirements: Note medical certification and basic knowledge examination before applying for CLP (equivalent to gate 0). https://www.dps.texas.gov/DriverLicense/CommercialLicense.htm . Note that the referenced TEXAS COMMERCIAL MOTOR VEHICLE DRIVERS HANDBOOK for interstate CLD https://www.dps.texas.gov/internetforms/Forms/DL-7C.pdf includes its statement of compliance with applicable federal CDL requirements, "In 1989, the Texas Legislature established the Commercial Driver

equipment should also be exclusively operated by licensed operators. In such vehicles the actual operator is the AV developer. Gated certification is a process by which such vehicles and operators may be similarly licensed to operate on public roads with incrementally demanding levels of performance tied to incrementally proven levels of competency by showing conformance to safety requirements such as those provided above in section 1.2. The proposed gated certification process is not a type certification, since it is solely performance based and is agnostic with respect to the vehicle design.

Certification for public use of various transportation assets may be accomplished by government officials, private entities licensed by the government, or private agencies delegated authority by the appropriate government body. Certification typically does not involve proprietary features except to the extent that they potentially impact public safety.

There are many examples of industry/government partnerships related to sophisticated system design and technology development. For one example, the FAA accepts the use of privately developed DO-178C as an acceptable framework for aircraft cybersecurity.[31] There are many other examples of industry/government partnerships related to technology, notably the Department of Transportation, use of the Society of Automotive Engineers vehicle automation levels as the default standard for AV development in its AUTOMATED VEHICLES 3.0, PREPARING FOR THE FUTURE OF TRANSPORTATION, and in many other DOT documents and activities related to AV development. The SAE is developing a host of technical standards aligned with specific component or system technologies for AV development, most or all of which are likely to incorporated into AVs. Still, a gap exists for the high level safety requirements that all vehicles must adhere to, and that all underlying technologies must support.

Gated Certification as proposed is a process for independent evaluation of compliance with objective safety standards at certain points in development, appropriate for that development level, before allowing the development to proceed to the next development phase. Many complex engineering developments are based on gated certification, to make sure that safety, engineering, performance, and financial targets have been reached before committing to the next development level. It is our belief that AV's are complex engineering developments, and present

License Law to comply with the federal Commercial Motor Vehicle Safety Act of 1986. These laws were passed to reduce traffic accidents involving commercial motor vehicles."
Texas, their current Graduated Driver License Program is described at https://www.dps.texas.gov/DriverLicense/gdl.htm.

Tennessee, their GDL program is described at https://tntrafficsafety.org/programs/teen-driver-education/gdl/ and https://www.tn.gov/content/dam/tn/safety/documents/GDLBroc.pdf.

[31] FAA Advisory Circular AC No. 20-115C, Subject: Airborne Software Assurance, specifies acceptability of RTCA DO-178C, "Software Considerations in Airborne Systems and Equipment Certification, dated December 13, 2011"

significant risk to public safety and property. The public needs to be fully aware of the related technical, financial, and legal issues before AV developers are allowed access to public roads. The best way for AV developers to provide needed visibility into the hazards they cause and their plans to manage those hazards is for a gated certification process that includes knowledgeable experts, advocates for safety, government officials, and the public at each stage of development for which access to public roads is sought.

An example of gated certification may be found in DOD 5000, Operation of the Defense Acquisition System[32], where specific milestones include preliminary design review, critical design review, and final design review by a panel of program officials, other government employees, and third party experts who review and critique all aspects of a design's compliance with requirements and intended use as documented and presented by the AV developer. Performance based requirements are agnostic with respect to design.

For AVs in the proposed process, official review of AV certification would include an authorized official examiner, data and presentations by the AV developer, and independent review by qualified third parties assisting the official review. This is fundamentally no different than any other graduated driver's license review process. Third party participants would include DOT representatives, public safety experts, state and local transportation officials to assure requirements compliance in jurisdictions where the AV would be operated, within approved defined and approved ODD's and therefore subject to applicable state and local laws and regulations. The authorized official would then approve a license to operate in the approved regime if the AV developer passes the examination, just like any other licensed motor vehicle operator.

[32] https://www.acq.osd.mil/fo/docs/500002p.pdf

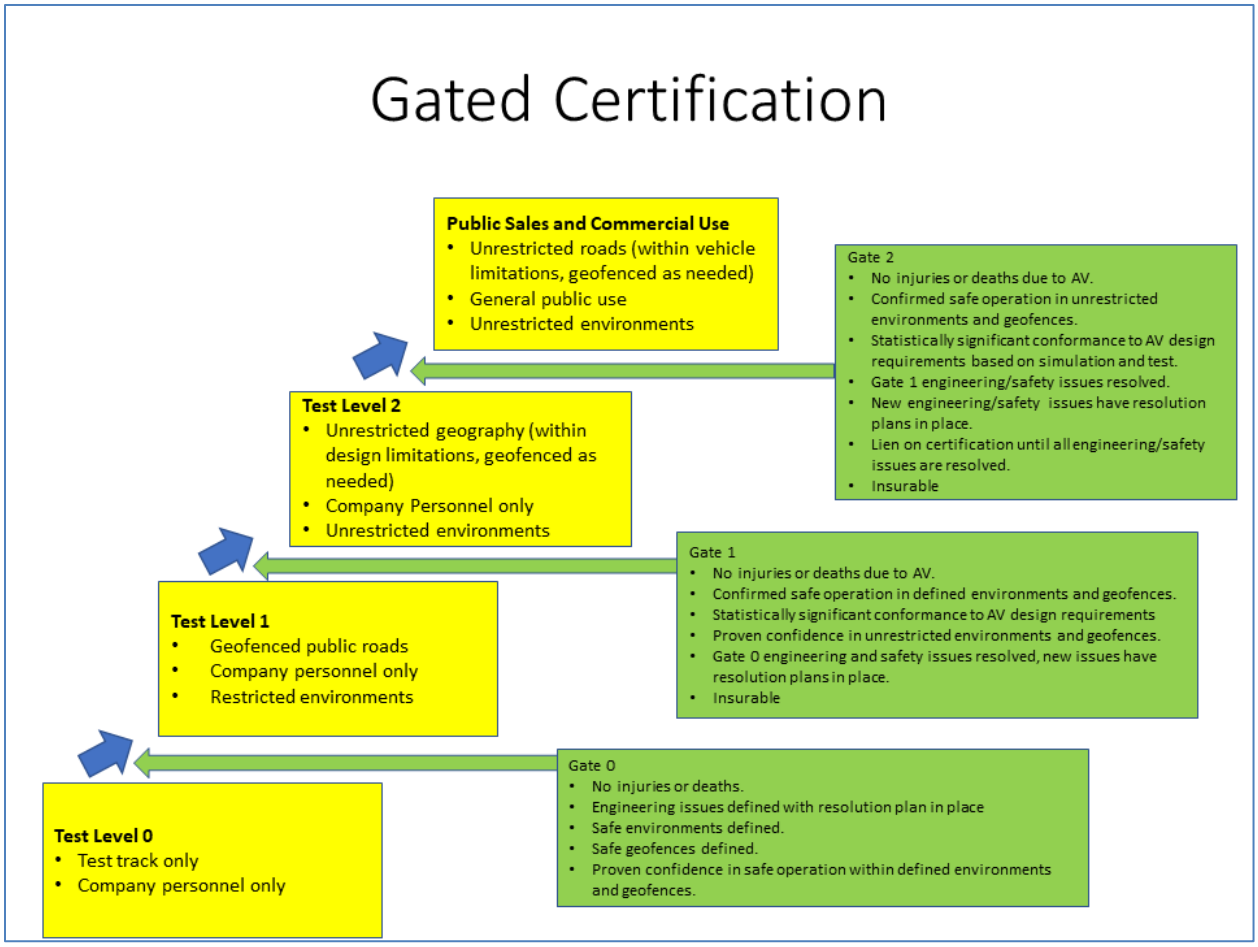

Figure 1 Increased scrutiny commensurate with increased public exposure..

A gated certification process appropriate for AV development is shown in figure 1 above.

In this model, an AV developer would be free to do whatever it wanted on its own test track using its own personnel. This is consistent with current practice. Before leaving the test track and starting tests on public roads, the AV developer would need to pass through a gate and demonstrate that the AV was ready to be safely operated on approved public roads and neighborhoods, assuring public safety.

1.3.1. At **Gate 0**, analogous to satisfying the requirements for a learner's permit, the AV developer would need to show that:

- It has complied with all applicable safety requirements.
- Engineering issues have been defined and resolution plans are in place.
- Software stress testing has been completed and passed.
- Data processing margins have been evaluated and sufficient margins demonstrated.
- No injuries or deaths have occurred in the controlled environment while testing the applicant's current AV hardware/software configuration.

- Safe operating environments (provisional ODD, including geofences) have been defined.
- Demonstrate proven confidence in safe operation within the limits it has defined.
- Demonstrate data recorder sufficiency.

Once the AV developer passes through Gate 0,[33] i.e., the certification authority has determined that the AV developer has achieved the Gate 0 criteria, the AV developer would be licensed by the appropriate public authority:

- Approved provisional ODD.
- Access to geofenced public roads for additional AV testing.
- Operational test using company personnel only.
- Operational test only within the specified safe operating environments (provisional ODD).

1.3.2. At **Gate 1**, analogous to a provisional driver's license, the AV developer would show that:

- There have been no injuries or deaths due to AV operation whose root cause has not been accommodated by design changes.
- It has complied with all applicable safety requirements.
- Confirmed conformity with operational limits of defined by approved ODD.
- Confirmed safe operation in Gate 0 defined environments and geofences.
- Statistically significant[34] conformance to AV applicable safety design requirements.
- Demonstrate proven confidence in projected AV use in unrestricted environments and geofences. All outstanding Gate 0 engineering and safety issues resolved; new issues have resolution plans in place.
- Insurable for use in expanded environments and ranges.

After passing through Gate 1, the AV developer would be licensed to continue testing within:

- Approved interim final ODD.
- Unrestricted geography consistent with approved ODD (within design limitations, geofenced as needed).
- Test within unrestricted environments, as defined at Gate 1.
- Using company Personnel only.

1.3.3. In preparation for public use or commercial release to the public, the AV developer would pass through **Gate 2**, equivalent to a full driver's license. At Gate 2, the AV developer would show that:

[33] Note that passing Gate 0 does not in any way restrict additional use of private company test assets, including test tracks. Additional private tests may be needed to meet the criteria in subsequent certification gates.

[34] https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1478/RAND_RR1478.pdf

- There have been no injuries or deaths due to AV operations, whose root cause has not been accommodated by design changes.
- It has complied with all applicable safety requirements.
- Confirmed safe operation throughout its ODD in otherwise unrestricted environments and geofences.
- Confirmed conformity with operational limits defined by approved ODD.
- Statistically significant conformance to AV design requirements based on simulation and test.
- All outstanding Gate 1 engineering/safety issues resolved.
- Software stress testing has been reconfirmed and passed.
- Data processing margins have been reconfirmed and sufficient margins demonstrated.
- Reconfirm data recorder sufficiency.
- New engineering/safety issues have resolution plans in place.
- Lien on certification until all engineering/safety issues are resolved.
- AV is insurable for intended operations.

After passing through Gate 2, the AV developer would be licensed for:

- Approved final ODD.
- Unrestricted public road use (within vehicle limitations defined by approved ODD, geofenced as needed).
- General public use.
- Unrestricted environments consistent with vehicle design and approved ODD.

1.4. **THROUGH DELEGATION OF AUTHORITY AND COMPOSITION OF THE CERTIFICATION LICENSING BOARD** industrial, governmental, and public interests would all be provided the opportunity to review, understand, and challenge the AV developmental plans and AV developer/operator capabilities, assuring that the public interest would be served. The gated certification process as described would also provide an audit trail, pointing to improvements as experience with AV operations is gained by all stakeholders, without imposing an unreasonable burden on AV developers.

1.5. **CHANGES, UPGRADES, AND COMPONENT IMPROVEMENTS** can readily be accommodated within this licensing process. AV developers would process changes through the certification authority. Major changes, those that affect vehicle safety, range of operation, or environmental suitability, would require corresponding partial recertification of the AV with respect to those changes only. Minor changes, that did not affect safety, range of operation, environmental suitability, or insurability, would not require recertification, once those changes have been evaluated by component test, interface verification, and regression testing. (For example, if an AV component manufacturer modified the range of a RADAR that was being used for vehicle control and that change measurably degraded safety or

impacted operations, recertification with respect to that change would be required. On the other hand, if, for example, a RADAR component change did not affect safety nor its interaction with the vehicle control system and its licensed operator software or logic executable, such as a change from one supplier to another with the same features (e.g., RADAR radiated power, gain, reliability, and interfaces to the AV control system), then AV recertification would not be required. Both AV developers and their supply chain would thus be free to make improvements to components without AV recertification.