Exponent
149 Commonwealth Drive
Menlo Park, CA 94025

telephone 650-326-9400
facsimile 650-326-8072
www.exponent.com

To: Ms. Heidi King
Deputy Administrator,
National Highway Traffic Safety Administration (NHTSA)
Docket Management Facility,
U.S. Department of Transportation, Room W12–140,
1200 New Jersey Avenue SE,
Washington, DC 20590–0001.

July 26, 2019

Subject: Docket Number NHTSA–2019–0036

Dear Acting Administrator King,

Attached please find comments and responses from Exponent, Inc. an engineering and scientific consulting firm to the questions that NHTSA published in its "Advance notice of proposed rulemaking (ANPRM), Docket No. NHTSA–2019–0036, Removing Regulatory Barriers for Vehicles With Automated Driving Systems".

General Comments:

To begin, Exponent suggests that there may be a few general principles NHTSA could perhaps develop and apply to its considerations regarding the methods by which motor vehicles equipped with "Advanced Driving Systems" (ADS) could be certified to the 100 series Federal Motor Vehicle Safety Standards (FMVSS) and what alternative methods and techniques might be applied to demonstrate compliance to those existing standards. Exponent respectively nominates four general principles (below) and suggests that NHTSA may apply them (or others NHTSA may define) in its deliberations about FMVSS compliance evaluations for vehicles with ADS, to the extent possible and practicable:

1. Seek to ensure demonstrable equivalence between any new certification approach to current performance requirements, there must be a scientific or engineering linkage to assure vehicle level performance characteristics equivalent to existing FMVSS requirements for conventional vehicles driven by a human.
2. Assess the potential benefits of alternative approaches to assure; satisfaction of the safety need originally addressed by the FMVSS in question, and that NHTSA's enforcement activity is enabled with the same effect as physical testing of conventional vehicles.
3. Ensure that application of the certification approach will exercise the entire AV system:
    a. sensors,
    b. communication bus (or buses),
    c. processing elements,
    d. control commands,

   e. control actuation,
   f. vehicle response,
4. Avoid burdening autonomous vehicle system providers and integrators with new and unique work tasks that are necessary only for certification, and provide little or no safety value otherwise.

Exponent's responses focus on SAE J3016 at automation levels 4 and 5. Throughout our responses Exponent will refer to the autonomous vehicles at issue as "Automated Driving System-Dedicated Vehicles (ADS–DVs)", the term NHTSA used in its ANPRM. (Reference: "Removing Regulatory Barriers for Vehicles With Automated Driving Systems", FR Vol. 84, No. 102, Tuesday, May 28, 2019.) We will refer to the legal entities responsible for ADS-DVs as "AV Providers". Some "AV Providers" will likely be traditional vehicle manufacturers and others may engineer only an autonomous vehicle system for fitment and integration onto motor vehicles that may not be manufactured by the same entity that engineered the AV system. Under such conditions, the motor vehicle manufacturer that introduced the product into the stream of commerce and the entity that engineered the AV system are jointly referred to as the "AV provider" in our responses.

NHTSA asked for responses "…for Automated Driving System-Dedicated Vehicles (ADS–DVs) that lack traditional manual controls necessary for a human driver to maneuver the vehicle and other features intended to facilitate operation of a vehicle by a human driver, but that are otherwise traditional vehicles with typical seating configurations." Exponent respectfully suggests that the earliest commercial ADS-DV applications may not be units that are designed for human transport, but rather for transport of goods only. It is possible the most immediate applications for ADS-DV FMVSS alternative compliance mechanisms may be for motor vehicles that are not equipped with any seat at all; yet, such ADS-DVs also may not fit within the Low-Speed Vehicle provisions of FMVSS 500 and therefore could present a need for actionable certification test methods to the more complex set of the FMVSS 100 series. Several of Exponent's responses comprehend such circumstances.

NHTSA wrote: "A. Normal ADS–DV Operation - One possible approach for vehicle manufacturers to use for self-certification, and the agency to use for compliance verification, is the ''Normal ADS–DV Operation'' approach.…. Analysis - The Normal ADS–DV Operation approach may provide the most ''realistic'' representation of how the vehicle would perform during normal use. This approach could allow NHTSA to continue acquiring vehicles in the same way that U.S. consumers do, from commercial dealerships, and testing actual vehicles to verify they meet the FMVSS requirements. *NHTSA is interested in maintaining its policy to buy and test new production vehicles from dealership lots*, to the extent possible." (Reference: "Removing Regulatory Barriers for Vehicles With Automated Driving Systems", FR Vol. 84, No. 102, Tuesday, May 28, 2019, emphasis added.) Exponent observes that ADS-DV may not

be delivered into the stream of commerce through the same retail sale/lease model of distribution that is common to the automobile industry today. NHTSA may have to collaborate with AV providers to facilitate acquisition of, or access to, vehicles exclusively for FMVSS compliance testing. For fleet vehicles that are not delivered into a commercial sale/lease outlet stream, vehicles could perhaps be selected from an operational fleet by NHTSA, and returned to operational fleet service after completion of the compliance testing.

As regarding the questions related to "Section E - Technical Documentation for System Design and/or Performance Approach" as a certification method, (Questions: 34, 35, and 36) and "Section D - Simulation" as a certification method, (Questions 9, and 30-33) Exponent offers the following general observations for NHTSA's consideration:

1. There are multiple levels of Software Review that could be applied to ADS-DVs, including: Documentation or Code Review, Virtual Simulation, Physical Simulation.
2. Documentation or Code Review
    a. With respect to requirements documentation, NHTSA may consider reference to and adoption of existing standards that have likely application to ADS-DV as general software testing requirements and/or automotive specific applications, for example:
        i. ISO 9000 series of software standards, in particular ISO/IEC/IEEE 90003:2018: "Software engineering -- Guidelines for the application of ISO 9001:2015 to computer software"
        ii. ISO/IEC 25000: "Software Product Quality Requirements and Evaluation" (SQuaRE) series
        iii. IEEE 1061-1998: "IEEE Standard for a Software Quality Metrics Methodology"
        iv. ISO/IEC12207:2008: "Systems and software engineering -- Software life cycle processes"
        v. ISO/PAS 21448: "Road vehicles -- Safety of the intended functionality"
        vi. ISO 26262: "Road Vehicles - Functional Safety, in particular ISO 26262:6 "
        vii. ISO/IEC 27000 ISO/IEC 27000 family "Information security management systems"
        viii. MISRA C: "Guidelines for the Use of the C Language in Critical Systems"
        ix. MISRA C++: "Guidelines for the use of the C++ language in critical systems"
        x. AUTOSAR: "Automotive Open System Architecture "
    b. Beyond the system level framework standards, coding guidelines and best practices can be applied to the ADS-DV development/validation/certification processes. Automated tools can be used to scan codes and identify non-

compliance areas according to various established and accepted guidelines, including MISRA, MISRA C++, AUTOSAR C++, among others. It may be sufficient in some cases for the AV provider to establish an internal guideline, but it is important for the designers of such an internal guideline to demonstrate the appropriateness and the consistency of that guideline with respect to accepted industry common standards. AUTOSAR coding guidelines have been created to support the development of adaptive platforms using C++ directed to enable connected vehicles and autonomous driving.

c. It is the responsibility of the AV provider to demonstrate that proper processes and frameworks were faithfully applied throughout the development process. This may include a summary of requirements during the initiation of software development (risks, corner test cases, FMVSS, etc.), architectural design (block diagrams), and coding standard compliance (e.g. naming conventions, variable declarations, etc.). Appropriate risk and hazard analyses determine the level of documentation and testing to ensure conformance to industry adopted standards. Hazard analyses are not commonly applied to FMVSS. However, for ADS-DVs, NHTSA and AV providers will probably seek to ensure that the provisions necessary for FMVSS compliance are exercised in the course of normal operations within the vehicles' Operational Design Domain (ODD) and are explicitly addressed in a Hazard Analysis.
d. There are existing frameworks available that may be appropriate for requirements to define the submission materials necessary and sufficient to establish compliance. An industry consortium could collaborate with NHTSA to ultimately determine and specify compliance documentation for submission that are most efficient, applicable, and fulsome in compliance demonstration.
e. Document or code review could be performed by neutral party professionals including software quality auditors, software quality engineers or others as predicate to a NHTSA review for compliance conformation. NHTSA could also consider qualification of such a cadre of experts to review and audit performance compliance.
f. A layered approach could be adapted so that only a restricted set of people have visibility into the source code and IP of the software. For example, NHTSA and/or third-party teams could perform coding convention checks on the software using automated tools without human reading of the source code/algorithm. Once compliance is established, it can be "black boxed"[1] and passed onto a second team that reviews system architecture and block diagrams for consistency and

[1] "Black-box" testing is a method of software review that examines the functionality of an application without access into, and review of the software structures and workings. Specific knowledge of the application code is not required and is not available to the tester. The tester considers and evaluates what the software is supposed to do, but not how the software accomplishes that goal.

quality. Once compliance is again established, blocks of code can further be "black-boxed" for static or dynamic analyses. Then designated portions of code or test libraries can be selected for computer simulation.

g. Virtual Simulations - Existing virtual simulation tools can be standardized to apply to the software of interest. This is a prime opportunity for an industry consortium to collaborate with NHTSA to produce a single consistent, consolidated input/output, and agree on the parameters for new standards.
h. Physical Simulation - Physical simulation tools could be standardized to apply to certification. This approach also presents a prime opportunity for an industry consortium to collaborate with NHTSA to have one consistent, consolidated input/output, and agree on the parameters for new standards such that identical or similar test cases, test conditions, and scenarios applied to different ADS-DVs would maintain consistency and uniformity in compliance assessments.

3. Related observations:
    a. To provide a secure, non-intrusive means of gaining access to the ADS-DV systems, Exponent proposes the following for consideration:
        i. Provide a standard interface specified by industry consortium with NHTSA consultation and agreement.
        ii. Provide a standard port and tool for access.
        iii. Establish a rolling encrypted code necessary for entry access. Access is to be disallowed without matching between the challenge response codes.
        iv. Exercise the entire ADS-DV system through the access port: sensors, communications, data processing, decision making, control command, control response, vehicle response.
    b. Additional mechanisms that could be implemented to ensure security and privacy include:
        i. Air-gap[2] between test programs and key algorithms. Similarly, key algorithms can be reviewed by neutral parties on air-gapped computers under a supervisory authority as is typically a practice applied in consideration of Intellectual Property (IP) related matters.
        ii. A security device to control access:
            1. Software protection dongles.
            2. Hardware connector dongles.

[2] "Air-gap" - a condition of a computer that has no network interfaces, wired or wireless, connected to an outside network.

NHTSA ANPRM Questions and Exponent Responses:

Question 4. "If only one of these approaches can be used to enforce a particular FMVSS requirement, what factors should be considered in selecting that approach? What policy or other considerations should guide the agency in choosing one alternative approach versus another for determining the compliance of a particular vehicle or item of equipment?"
Response: The general principles proposed for consideration in the "General Comments" section would seem to apply directly to this question.

1. Seek to ensure demonstrable equivalence between any new certification approach to current performance requirements, there must be a scientific or engineering linkage to assure vehicle level performance characteristics equivalent to existing FMVSS requirements for conventional vehicles driven by a human.
2. Assess the potential benefits of alternative approaches to assure; satisfaction of the safety need originally addressed by the FMVSS in question, and that NHTSA enforcement activity is enabled with the same effect as physical testing of conventional vehicles.
3. Ensure that application of the certification approach will exercise the entire AV system:
    a. sensors,
    b. communication bus (or busses),
    c. processing elements,
    d. control commands,
    e. control actuation,
    f. vehicle response,
4. To the extent possible, avoid burdening autonomous vehicle system providers and integrators with new and unique work tasks that are necessary only for certification, and provide little or no safety value otherwise.

Question 5. "With respect to any single approach or combination of approaches, could it be ensured that the compliance of all makes and models across the industry is measured by the same yard stick, i.e., that all vehicles are held to the same standard of performance, in meeting the same FMVSS requirement?"
Response: Yes, multiple approaches could be applied and be "…measured by the same yard stick…" so long as each of the permissible alternative approaches have demonstrable equivalence to existing FMVSS; or, in the alternative, demonstrate that there is no safety need to comply to a specific standard. For example, in vehicles that do not carry occupants or in vehicles that have no occupant controls, the physical requirements of FMVSS 111, "Rear Visibility", would seem moot; and the equivalent requirements for an ADS-DV to ensure awareness of the surrounding environment could conceivable be satisfied by several of the alternative methods NHTSA proposed. NHTSA could codify multiple approaches as providing

360 degree lookout coverage. In such a certification regime, the AV provider must declare a certification approach and could not change from that certification approach or elect an alternative after it had declared the selected certification method to NHTSA, presumably on a schedule set by NHTSA in advance of introduction of the ADS-DV into the stream of commerce. The AV provider (or vehicle integrator if not the AV provider), must demonstrate compliance. NHTSA can independently assess compliance using the specific certification approach that had been declared by the AV provider or vehicle integrator during the vehicle development process.

Question 6. "What other potential revisions or additions to terms, in addition to 'driver', are necessary for crash avoidance standards that NHTSA should consider defining or modifying to better communicate how the agency intends to conduct compliance verification of ADS vehicle?"
Response: The SAE "On Road Automated Driving (ORAD) Committee[3] is updating the J3016 standard and that update has been submitted to ballot. Perhaps NHTSA could consider those definitions and the taxonomy now under development at SAE, they may be adequate for NHTSDA's needs. If inadequate, perhaps NHTSA might provide input for Committee consideration.

Question 7. "Should NHTSA consider an approach to establish new definitions that apply only to ADS–DVs without traditional manual controls?"
Response: If the ADS-DV without manual controls could meet all the FMVSS test requirements, then no new definitions appear to be necessary. However some FMVSS reference specific control features, for example, FMVSS 126 specifies input at the steering wheel. In this case, a vehicle without a steering wheel would likely require a new definition since there is nothing that represents a "steering wheel." It is also quite possible that new tests might be required, in which case new definitions might be necessary. It seems likely that some new definitions will be necessary. NHTSA might consider the taxonomy and definitions now under development by SAE ORAD Committee in the J3016 document revisions.

Please see response to Question 6 supra.

Question 8a. "For compliance testing methods involving adjusting current test procedures to allow alternative methods of controlling the test vehicle during the test (normal ADS–DV

[3] The On-Road Automated Driving (ORAD) committee reports to the Driver Assistance Systems Steering Committee of the Motor Vehicle Council. The ORAD committee is responsible for developing and maintaining SAE standards, recommended practices, and information reports related to motor vehicle driving automation system features across the full range of levels of driving automation. "On-road" refers to publicly accessible roadways that provide driving environments for the users of motor vehicles of all classes and all levels of driving automation.

function, TMPE, TMEC), or to allow the use of a surrogate vehicle: a. How could NHTSA ensure that the test vehicle's performance using the compliance method is an accurate proxy for the ADS–DV's performance during normal operation?"
Response: The method to assure equivalence may likely be contingent upon both the compliance testing method and the particular functions and performance of the ADS-DV design. AV providers probably will have to answer this question specifically for a particular ADS-DV.

Question 8b. "For compliance testing methods involving adjusting current test procedures to allow alternative methods of controlling the test vehicle during the test (normal ADS–DV function, TMPE, TMEC), or to allow the use of a surrogate vehicle…. b. If NHTSA were to incorporate the test method into its test procedures, would NHTSA need to adjust the performance requirements for each standard (in addition to the test procedures) to adequately maintain the focus on safety for an ADS–DV?"
Response: Not necessiarilly. The "General Principles" proffered for consideration would suggest it is necessary to demonstrate alternative compliance approaches meet the safety need for the specific standard in question and the alternative approach(s) would demonstrate *equivalence to the standard* or the fact that a standard is not applicable to a specific AVS-DV; the FMVSS 111 example with no occupants or no driver controls.

Question 9a. "For compliance testing methods that replace physical tests with nonphysical requirements (simulation, documentation): a. If the test method is used to determine compliance with a real-world test, how can NHTSA validate the accuracy of a simulation or documentation?
Response: The SAE ORAD Committee has recently launched a Modeling and Simulation (M&S) Task Force in which simulation validation methodology development will be a major initiative. NHTSA may consider participation, monitoring, collaborating, and/or influencing this Task Force to potentially create a document that simultaneously satisfies NHTSA's needs in this domain as well as those of the AV provider community.

Please also see Exponent's "General Comments" supra.

Question 9b. "If NHTSA must run real-world tests to validate a simulation or documentation, what is the advantage of non-physical requirements over these other compliance methods?"
Response: The Rand Corp study "Driving to Safety: How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?" (N. Kalra and S. Paddock, 2016) reported that public road driving, even when large mileage accumulation is possible, is insufficient for verifying and validating an ADS. It could prove to NHTSA's long term advantage to understand and influence the simulations processes that will lead an AV provider to conclude an ADS-DV is reasonably safe for insertion into the stream of commerce. Most of the training and much of the validation processes are likely to be done in simulations. It is likely

to be useful for NHTSA to have insight into these processes and the significance of program results.

Please also see Exponent's "General Comments" supra and responses to questions regarding certification through simulation, questions 30 through 33 infra.

Question 10b. "Would non-physical requirements simply replicate the existing physical tests in a virtual world? If not, what would be the nature of the non-physical requirements (that is, what performance metrics would these requirements use, and how would NHTSA measure them)? Are there ways that NHTSA could amend the FMVSSs to remove barriers to ADS–DVs that would not require using the compliance test methods described in below? ….b Are there any changes that NHTSA could make to the FMVSS test procedures that could incorporate basic ADS capabilities to demonstrate performance, such as using an ADS– DV's capability to recognize and obey a stop sign to test service brake performance?"
Response: Please refer to Exponent's answers to questions numbers 30 to 33 related to the certification by Simulation approach infra, and Exponent's "General Comments" supra.

Question 11. "What research or data exists to show that the compliance test method would adequately maintain the focus on ADS–DV safety? What modifications of the safety standards would be necessary to enable the use of the test method?"
Response: Each AV Provider is performing ongoing research within the specific Operating Design Domain (ODD) established for that ADS-DV. In doing so, the AV provider must establish performance metrics for that particular ADS-DV within the specified ODD and the ADS-DV is engineered and developed to execute specific use case driving elements within that specific ODD. A survey of such use case elements within any specified ODD can identify individual use case elements that correspond in type, to specific FMVSS requirements. For compliance testing, those use case elements can be structured so as to match the FMVSS requirement, the specific use case element can be stressed to replicate the FMVSS requirement; vehicle response can be measured and compared to the FMVSS acceptance criteria.

1. For example, consider the conditions of FMVSS 135 stopping distance requirements. The use case element is coming to a stop; under normal ADS-DV operating conditions, that is not a stressful challenge as the ADS-DV outlook must reliably detect, process data, and effectuate the control actions necessary and sufficient to bring the vehicle to a stop.
2. However FMVSS 135 is a braking requirement that demands maximum braking ("best effort" for a human driver) and measures maximum braking capacity in setting a stopping distance limit. In normal ODD functions, maximum braking effort is unlikely to be encountered.
3. For compliance testing, the sudden appearance of a target within the travel lane at a time-to-collision (TTC) that DEMANDS max brake application could be the stress

condition within the ODD that commands and delivers maximum braking effort and demonstrates compliance to FMVSS 135 stopping distance requirements.
4. The ADS-DV vehicle can be subjected to a sudden obstacle that stresses the use case element to which the ADS-DV had been trained. The response measure is stopping distance from target insertion into the lane of travel. The ADS-DV response would have to be constrained to travel straight in the blocked lane; steering avoidance would not be an allowed response to this stress condition applied to a standard use case element.
5. The condition would be equivalent to best effort for minimum stopping distance by a human driver now embedded into FMVSS 135.

Question. "Normal ADS–DV Operation" 12. "What design concepts are vehicle manufacturers considering relating to how an ADS–DV passenger/operator will interface with, or command (e.g., via verbal or manual input), the ADS to accomplish any driving task within its ODD? Please explain each design concept and exactly how each would be commanded to execute on-road trips."
Response: AV providers are positioned to respond.

Question. "Normal ADS–DV Operation" 14. "Will all ADS–DVs without traditional manual controls be capable of receiving and acting upon simple commands not consisting of a street address based destination, such as ''drive forward or backwards a distance of 10 feet and stop''; ''shift from park to drive and accelerate to 25 mph''; ''drive up onto a car hauler truck trailer''; etc.? Please explain projected challenges for ADS–DVs without traditional manual controls to complete discrete driving commands and tasks.
Response: The manner in which ADS-DVs without traditional manual controls receive and act upon simple commands will be determined by the individual AV providers. Some ADS – DV control system challenges that may benefit from additional consideration and research include:

General input/output model in L4/L5 vehicles: The relationships between external stimuli, driver/operator inputs, and vehicle responses in traditional vehicles will be replaced by something very different. Since knowledge and understanding of such relationships are crucial for safe driving, whatever replaces them will need to be well-designed from the start and learnable/learned by operators.

Communicating with an operator: What means/methods are available for communicating with an operator and how will these impact performance, acceptance, and trust?
Nature of inputs from an operator: Implications of possible methods of inputting commands into the system (e.g., voice, entry into a touch screen) vs. traditional steering wheel/pedal inputs.

Timing of inputs; when are commands entered relative to when they are executed by the system – may not be immediate. Smooth pursuit movements with traditional driving vs. the possibility

of allowing for continuous movement (forward/back), or discrete intervals (feet, yards, or other reference.)

Provision of feedback & response time from the vehicle: In a traditional vehicle, much of driving is essentially a self-paced tracking task. What will replace this, and what are the implications for performance, acceptance, and trust?

Control inputs vs. vehicle response compatibility: Potential lack of compatibility between operator's perception of the real-world, control movements, and corresponding changes in the vehicle's movement (e.g., an operator facing towards the rear of the vehicle).
Remote Control: Remote or teleoperation of L5 vehicles may present additional challenges.

Question. "Normal ADS–DV Operation" 15. "How would NHTSA ensure that the performance of the ADS–DV during testing is consistent with how the vehicle would perform during actual normal use?"
Response: See Exponent responses to Questions 4 and 13. Additionally, NHTSA might consider application of the general principles listed in "General Comments", supra: "demonstrable equivalence to current performance requirements; exercise of the entire AV system: sensors, communication bus, processing elements, control commands, control actuation, vehicle response." The key elements would seem to be execution of a use case element within the parametric requirements of a comparable FMVSS and exercise of the complete ADS-DV.

Question. "Test Mode With Pre-Programmed Execution (TMPE)" 16. "How could engineers responsible for performing FMVSS compliance assessments of an ADS–DV without manual controls be expected to access and interface with the compliance test library menu?"
Response: This approach would seem to risk a significant flaw if the "compliance library test menu" when accessed for compliance testing were active outside the ODD and exclusive to operation within the compliance library itself.

Should NHTSA care to pursue such an approach, a possible solution to access the "compliance library menu" could be a standard and common industry interface developed by, agreed upon, and adopted by an industry consortium formed in the manner of the "Collision Avoidance Metrics Partnership" or the like. A common access interface could be built into a specific tool with distribution limited to NHTSA, AV providers (including the supply base), and other authorized users with access tools that are coded to allow or deny access following exchange of encrypted challenge and response recognition messages; agreement of the challenge and response open access to the tool, in this case, the "compliance test library menu". Failure in the challenge and response exchange would prohibit access and keep the "compliance test library menu" locked. The tools could be serialized with electronic certificates of authenticity that expire and must be renewed for continued use. A trusted "owner" could be appointed to

supervise the tools and operational fees or licensing fees could be agreed upon to provide ongoing funding to sustain the tool control process.

In this approach, it would seem NHTSA would have to assure that the vehicle response while operating within the "compliance test library menu" relied upon standard operational algorithm features within the ODD. As part of a compliance demonstration, NHTSA may need to obtain documentation from the AV provider to ensure the sensing/communication/processing/control commands/control actuation/vehicle response is driven by the operational algorithm within the ODD and not an algorithm external to the ODD that is dedicated to FMVSS compliance tasks and activated only when the "compliance test library menu" is accessed, when the FMVSS task is selected, or in some other detection mode unique to the FMVSS use case. Possibly NHTSA could require production from the AV provider and audit of: system architecture documents including functional block diagram and, system logic block diagram, software requirements specification (SRS), software design specification (SDS), traceability analysis, detailed code review for actions unique to "library", detailed code review to ensure all FMVSS "library" elements are controlling within the ODD and not only in "library" mode . In this regard, please also see Exponent's General Comments regarding certification through simulation supra.

Question. "Test Mode With Pre-Programmed Execution (TMPE)" 17. "Would the FMVSS need to specify the libraries available to NHTSA to test the vehicle?"
Response: Yes, including requirements, test procedures and acceptance criteria. Absent those materials, an alternative mechanism would need to be established to define the requirements, procedures and criteria necessary for compliance. See answer to questions 4, 13, and 16 supra.

Question. "Test Mode With Pre-Programmed Execution (TMPE)" 19. "Can an ADS–DV be expected to perform within tight tolerance levels using the regular on-board sensors?"
Response: AV providers and sensor suppliers have profound knowledge in this domain and may be willing to share same with NHTSA. An industry consortium could research the issue and develop/establish common industry standards for sensor precision and response time that could possibly be matched to FMVSS requirements on a platform-by-platform basis. If a common standard were to be established, the responsible body may consider setting only minimum standards rather than minimum and maximum performance limits for precision and response time to enable technological advances without requiring standards changes. If standards are set at minimum performance limits, technology advances will be affected within that existing minimum standard framework. If standards include both minimum and maximum performance standards, technical advances in improved performance measures for precision and response time may be limited by the maximum performance limitations.

Question. "Test Mode With Pre-Programmed Execution (TMPE)" - 20. "How much variation in test results across various test locations (i.e., proving grounds) is expected to result from

testing an ADS–DV equipped with the same FMVSS compliance library at different locations? Could the ability to satisfy FMVSS performance requirements depend on the location the tests are performed?"
Response: Unknown. A similar question regarding laboratory-to-laboratory variations was successfully addressed (at least to the point of understanding) with round robin crash testing in the 1970s. AV providers may have insight as to performance variations with their own ODD when operating in differing test environments and may be willing to share such insights with NHTSA.

This could be a research project for an industry consortium. Such an industry consortium could develop, plan, and execute a project to address laboratory variations in a manner similar to the Alliance and Global Auto Maker projects of the 2000s to establish voluntary industry standards for: collision compatibility, side impact occupant-out-of- position test conditions and criteria, driver distraction, and so on. In those efforts, there were also generally voices from the public involved in the research efforts: NHTSA, CMOT, the IIHS, standards organizations, public health officials, and possibly State departments responsible for traffic safety. Public involvement and oversight could add to the value of industry common efforts in this domain.

Question. "Test Mode With Pre-Programmed Execution (TMPE) - 21. "Is it reasonable to assume any geofence-based operating restrictions could be suspended while the ADS–DV is operating in a ''test mode'' intended to assess FMVSS compliance?"
Response: Perhaps; AV providers could possibly include specific NHTSA specified and qualified test facilities within that AV provider's ODD. Determining the general feasibility and specific details of such an approach is best left for the AV provider community.

Question. "Test Mode With Pre-Programmed Execution (TMPE)" - 22. "How could vehicle-based electronically accessible libraries for conducting FMVSS testing be developed in a way that would allow NHTSA to access the system for compliance testing but not allow unauthorized access that could present a security or safety risk to an ADS–DV?"
Response: See answer to question 16 supra.

Question. "Test Mode With Pre-Programmed Execution (TMPE)" - 23. "Are there other considerations NHTSA should be aware of when contemplating the viability of programmed execution-based vehicle compliance verification?"
Response: See answers to questions 4, 16, and 19 supra. Additionally, some vehicles will not have passenger seating nor driver manual controls and some vehicles may not be sold or leased at retail in conformance with the current business model for distribution of motor vehicles. Alternative approaches to FMVSS compliance tests that do not comprehend these market conditions may not fully address the range of vehicles that will be subject to FMVSS

compliance. NHTSA may possibly wish to consider these controls limitations and distribution variations in crafting revisions to FMVSS 100 series requirements.

Question. "Test Mode With Pre-Programmed Execution (TMPE)" - 24. "When changes or updates are made to the ADS, how will the TMPE content be updated to reflect the changes and how often would it be updated?"
Response: Answers are likely unique and specific to each AV provider. NHTSA and industry may consider how to update regulatory certification documentation with change records and associated certification submissions. State institutions, Departments of Motor Vehicles, Secretary of State Offices, etc. now control and monitor human drivers. As the ADS-DV may be considered a driver, possibly there is an interest and a role for States in monitoring compliance records. An industry consortium could develop and adopt common standards for change record generation and associated certification documentation, enable variations sufficient for each AV provider to control their own system, and provide for a common reporting format to the appropriate regulatory authorities.

Additionally, NHTSA may consider requiring varying levels of TMPE certification modifications based on the nature of the changes the AV provider will have made to the ADS-DV. Such changes may vary from mild to major effects on vehicle behavior. The required changes to the TMPE certification documents could potentially be guided by risk analyses associated with different categories of updates. A similar approach is being proposed by the FDA for artificial intelligence and machine learning based software as a medical device. See https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device. An industry consortium could possibly research: update mechanisms planned by AV providers, TMPE content changes, risk quantification or characterization, update frequencies, and related issues. NHTSA participation in an institutional construct formed for consideration of such issues could inform NHTSA policy decisions in this domain.

Question. "Test Mode With External Control (TMEC)" - 25. "Is it reasonable to assume a common (universal) interface, translator, and/or communication protocol between an external controller and any ADS–DV will be developed?"
Response: Absent an industry effort to generate a common standard as OBD access ports or electrical charging ports, it is reasonable to conclude there may result a number of unique interface, translator, and/or communication protocols. This is a prime need for industry common action that could be supported by a consortium of the affected parties.

Question. "Test Mode With External Control (TMEC)" - 27. "Could a means of manual control be developed that would allow NHTSA to access the system for compliance testing but not allow unauthorized access that could present a security or safety risk to an ADS–DV?"

Response: Yes. See answer to question 16.

Question. "Test Mode With External Control (TMEC)" - 28. "Is it reasonable to assume any geofence-based operating restrictions could be suspended while an external controller intended to assess FMVSS compliance is connected to the ADS– DV?"
Response: It is not reasonable to assume that an ADS-DV will operate outside geofenced-based operating restrictions. It may be possible to include NHTSA selected and approved test facilities within an ADS' geo-fencing restrictions. However, to achieve this outcome, high definition (HD) maps would have to be supplied in an agreed-upon format or it would be necessary for each AV provider to develop its own HD map of the test facilities for inclusion within a geo-fenced ODD. Conceivably, an industry consortium could map the VRTC (or any other NHTSA selected/approved test site) and distribute the maps among consortium members.

Question. "Test Mode With External Control (TMEC)" - 29. "Are there other considerations NHTSA should be aware of when contemplating the viability of using an external controller-based vehicle certification?"
Response: Yes, as with the TMPE Process, there is a challenge in assuring the entire system is exercised if an external controller is applied and actuates an algorithm for FMVSS compliance. NHTSA will need to develop mechanisms to ensure the external access for FMVSS compliance testing does not enter into a control algorithm only active in FMVSS compliance mode. NHTSA will also need to ensure that the control algorithm active in the ODD is also activated in the external control mode, behaves exactly as it would when stressed in the ODD itself, and fully exercises every component and system of the ADS-DV. This seems difficult on its face should the external control simply command a response without initiation through the lookout sensors in the system, communications through the bus, processing, control command, actuation, and final vehicle response.

Common access mechanisms, tools, and security measures mirror those described for the "Test Mode With Pre-Programmed Execution (TMPE) Process" in our answer to Question 16 supra.

Question. "Simulation" - 30. "How can simulations be used to assess FMVSS compliance?"
Response: A simulation approach potentially offers great promise and multidimensional challenges. ADS-DV will be developed with significant prove out, operational stressing, and limit evaluations performed in simulations. Many, most, or perhaps all AV systems may be predominately trained using simulations as an algorithm can be subjected to many more miles of operation and many more stress conditions in simulation than is possible in closed course or public roadway driving. Since the systems are trained in simulations, it should be possible to stress systems in demonstration of FMVSS compliance in simulations also. Such an approach will likely require cooperation of the AV provider community. It is difficult to see how NHTSA

could develop the systems necessary to tax each ADS-DV system through simulation absent access to the algorithm and simulations input/output data.

Enforcement through simulation would routinize, and could possibly minimize, the demands on NHTSA resources. This approach could also possibly require a different set of analytical tools and skills than is now prevalent inside the Administration. NHTSA would have to develop the capacity and capability to exercise the simulations necessary and sufficient for FMVSS compliance testing. A simulation process likely could be structured so as not to require AV providers to share the proprietary control algorithms for the ADS-DV with NHTSA to enable the simulations. This could possibly present some advantage in avoiding exposure risk for AV providers' proprietary intellectual work product.

Simulations can be constructed to: model and exercise the entire ADS-DV system performance. Simulations can be exercised within or outside a geo-fenced environment. Simulations can stress the entire system at limit conditions by insertion of new data simulating a looming collision threat.

Please also see Exponent's "General Comments" supra.

Question. "Simulation" - 31. "Are there objective, practicable ways for the agency to validate simulation models to ensure their accuracy and repeatability?"
Response: Yes. NHTSA can exercise the simulations within the ODD. NHTSA can select operational use cases and set inputs to exercise ADS-DV within ODD but outside the training set that had been used to develop the ADS-DV. The control algorithm can be stressed to simulate the FMVSS dynamic requirements by insertion of a looming collision threat within the ODD at a point(s) where brakes (FMVSS 135) or steering (FMVSS 126) must be actuated for successful collision avoidance. Vehicle level performance can be obtained as output and compared to existing FMVSS criteria.

As with the "Test Mode With Pre-Programmed Execution (TMPE)" process and the "Test Mode With External Control (TMEC)" process, security could be provided through a standard and common industry interface developed by, agreed upon, and adopted by an industry consortium formed in the manner of the "Collision Avoidance Metrics Partnership" or the like. A common access interface could be built into a specific tool with distribution limited to NHTSA and AV providers (including the supply base) coded to allow or deny access following exchange of encrypted challenge and response recognition messages; agreement of the challenge and response open access to the simulation tool. Failure in the challenge and response exchange would prohibit access and keep the ADS-DV control algorithm locked. The tools could be serialized with electronic certificates of authenticity that expire and must be renewed for continued use. A trusted "owner" could be appointed to supervise the tools and operational fees

or licensing fees could be agreed upon to provide ongoing funding to sustain the tool control process. This process can be validated in a way that is consistent with the spirit of penetration testing to test vulnerability for computer systems. The validation test set could possibly be derived from or mirror typical penetration test strategies such as external/internal testing, blind testing, double blind testing, black box testing, white box testing, etc.

An industry consortium or contractor, working with NHTSA could develop a common industry certification simulation regimen. The SAE ORAD Committee has launched a Modeling and Simulation (M&S) Task Force with simulation validation methodology development intended as a major work product. NHTSA also may consider participation, monitoring, collaborating, and/or influencing this Task Force.

Please also see Exponent's "General Comments" supra.

Question. "Simulation" – - 32. "Is it feasible to perform hardware in-the-loop simulations to conduct FMVSS compliance verification testing for current FMVSS?" and "33. Is it feasible to perform software in-the-loop simulations to conduct FMVSS compliance verification testing?"
Question. "Simulation" – 33. "Is it feasible to perform software-in-the-loop simulations to conduct FMVSS compliance verification testing?"
Responses to Questions 32 and 33: Yes. See answer to question 30 supra. For example, consider simulations for FMVSS 135 or 126; at T=0, insert an obstacle to present a looming collision threat as new input for sensor recognition/response (FMVSS 126 requires multiple obstacle inputs for the double lane change maneuver), measure vehicle response as output. The simulation output can be compared to FMVSS response requirements for stopping distance or obstacle avoidance and other metrics as called for in the existing FMVSS. Under such conditions, the entire ADS-DV can be exercised.

Please also see Exponent's "General Comments" supra.

Question. "Technical Documentation for System Design and/or Performance Approach" - 34. "How can the documentation focused approach ensure compliance with FMVSS, considering it neither verifies that the vehicles on the road match the documentation nor confirms that the vehicles on the road comply with the FMVSSs?"
Response: Technical documentation of the ADS-DV can provide a reliable and accurate view of the ADS-DV control algorithm. The algorithm can be reviewed, audited, checked and validated against common industry standards (see list in General Comments section).

The AV providers could use third party entities to check and validate code features that appropriately control dynamic vehicle performance in response to specific use case scenarios that mimic conditions in an FMVSS compliance test procedure. NHTSA could conceivably staff

for and/or be provided such a third party audit review as its enforcement test(s) of ADS-DV vehicles. The algorithm review could involve: review of system block diagrams and software logic; industry accepted coding standards applications; static or dynamic analysis; walkthroughs; and as with a simulation process, applications of input/output for FMVSS test cases; reference answers 30-33 supra.

The Technical documentation approach could prove to be deeply intrusive to the AV provider Intellectual Work Product and proprietary concerns may significantly complicate AV provider receptiveness to submission of work product for NHTSA testing in compliance. Some of these concerns may be mitigated following standard practices in sensitive IP litigation matters, for example conducting reviews on air-gapped computers under supervision of neutral or otherwise qualified parties, AV providers no doubt will comment and might possibly address such concerns.

Please also see Exponent's "General Comments" supra.

Question. "Technical Documentation for System Design and/or Performance Approach" - 35. "If technical documentation were acceptable for compliance verification, how would the manufacturer assure the agency that the documentation accurately represents the ADS–DV and that the system is safe?"
Response: This is a very difficult question. At the most basic level, an AV provider (the "manufacturer" in the question) would be required to provide technical documentation regarding the ADS-DV algorithm and associated hardware. Conceivably NHTSA could access the control algorithm embedded in a commercial vehicle and the associated hardware, then check for compliance through matching hardware and software specifications from the technical documentation to the hardware/software on an exemplar vehicle. See also answers to questions: 4, 16, 30-33 supra.

Technical documentation could also include AV provider test method validation plans as they relate to meeting particular standards, allowing NHTSA or a third-party auditor to assess for example the repeatability, accuracy, and robustness of adherence to standards; NHTSA may wish to consider requirements not just for the ADS-DV itself but also the development, validation, and certification procedures applied to that specific product. These would be substantially different types of requirements than NHTSA has historically demanded from motor vehicle manufacturers to demonstrate certification but such requirements could possibly well serve NHTSA in meeting the safety need (as review of processes inform risk assessments).

Observations of process variations across the AV provider community may uncover certain elements that NHTSA could identify as necessary and sufficient to meet the need for motor vehicle safety and provide a solid basis for future rulemaking. A third party auditor could

provide such a role for AV-providers prior to certification to increase confidence in the ADS-DV and reduce risk in distribution of the ADS-DV into the stream of commerce.

While documentation alone may not be able to determine the full effectiveness of a crash avoidance algorithm, or assess coverage of corner near-crash cases in a highly complex highway scenario, there has been precedence in the medical device field that a proper, robust process can be established to minimize the risk of "bad" software. Possibly NHTSA would chose to consider AV provider process reviews for adequacy.

NHTSA may choose to incorporate for example, aspects of the FDA's Total Product Lifestyle (TPLC) pilot program approach to monitoring software products, specifically as they relate to demonstrating an AV provider's commitment to safety, quality, and organizational excellence (including appropriate role designations in validation testing). Additionally standard IEC 62304 outlines the document lifecycle requirements for the development of medical software and software within medical devices and the need to document the activities at each stage, including development plan, requirement specification, architecture, implementation and verification, integration and integration testing, system testing, release, maintenance process and risk management process. NHTSA could possibly develop analogous requirements.

In addition to technical documentation for compliance verification, NHTSA or third-party auditors could conduct a high-level review of an organization's software development program for best practices.

The fact that an AV vendor has taken steps to document its software development process, in many cases by itself, could demonstrate the existence of a framework that minimizes the common, low level errors that software engineers may make during the development process.

Documentation alone may not fully address ADS-DV safety performance, but it does achieve a first-pass, bottom-line sanity check of whether a software/firmware package within an ADS-DV is sufficiently robust and appropriate for further virtual, physical simulation and stress testing.

Conceivably elements of a technical documentation approach to certification of existing FMVSS could extend into a broader effort by an industry consortium with input from NHTSA and the public regarding certification elements for processes to deliver AV safety. Within an understanding of the limitations and the intended goals of documentation review, this could be a very powerful tool to effectively and efficiently evaluate ADS-DVs in the future.

However, this process, and all of the alternative processes considered by NHTSA in the ANPRM cannot establish that "…the ADS–DV…system is safe". FMVSS assure that the

system architectures integrated into a vehicle provide a mechanism that meets the safety need for use by human drivers.

1. The transport system in the US relies upon human drivers driving vehicles that had been engineered to meet FMVSS. It is the responsibility of those human drivers to operate those vehicles in a safe manner; and there is no FMVSS that assures safe performance by human drivers. ADS–DV systems will be engineered to improve on human driver performance as is now manifest in service, and the ADS-DVs will be engineered and certified to those same FMVSS performance requirements.
2. There is no FMVSS that controls human driver performance. Human driver performance is monitored and controlled by State authorities and to some extent by the personal liability insurance system in the U.S.
3. Similarly, there is no existing FMVSS that assures "…the ADS–DV…system is safe" beyond compliance to existing FMVSS requirements for systems intended to be operated by human drivers.
4. Assurance of ADS-DV safety performance will be yielded through the accumulated driving experience (on closed track, real roadways, and in training or system verification and validation simulations) that demonstrate the capability of an ADS-DV to: operate within an ODD, perceive and recognize prevailing and changing circumstantial conditions (including novel conditions and new stress events that fall outside the training set), process information about those conditions and events, plan and execute control responses to navigate the novel features newly presented in the ODD, and to avoid collision conflict through control applications. These are the precise actions human drivers apply in the driving task.
5. There is now no FMVSS to address an overarching requirement for safe driving performance in a vehicle AND it is the essential performance requirement to which ADS-DV engineering development efforts are focused by the AV provider community.
6. Should NHTSA determine a need for regulation in this domain (beyond its already substantial authority for defect investigations and recall orders), it would seem much additional collaborative work may be necessary.

The SAE ORAD Committee has convened a Verification and Validation (V&V) Task Force with the objective to define and develop methodologies necessary to build a safety assurance case that could be used to determine compliance with future (FMVSS or other) regulations for ADS-DVs. There may be multiple parallels between technical requirements in a validation set and in a certification set for new emerging regulations and certification methods to current FMVSS; NHTSA may wish to consider participation, monitoring, collaborating, and/or learning from this Task Force as work progresses.

Please also see Exponent's "General Comments" supra.

Question. "Technical Documentation for System Design and/or Performance Approach" - 36. "Exactly what kind of documentation could be submitted for each kind of FMVSS requirement? Provide specific examples with detailed explanation of the documentation required."
Response: See answer to question 34 supra. Documentation could include: third party audit results verifying conformance to common industry coding standards and methods; third party code review and verification/validation records, software requirements specification (SRS), software design specification (SDS), traceability analysis, block diagrams of software logic, simulation input/output for FMVSS test cases.

Please also see Exponent's "General Comments" supra.

Question. "Use of Surrogate Vehicle With Human Controls" - 37. "To what extent could equivalence of the vehicle components used for conventional and ADS–DVs be demonstrated to assure that surrogate vehicle performance would be indicative of that of a surrogate ADS–DV?"
Question. "Use of Surrogate Vehicle With Human Controls" - 38. "How can the agency confirm that the maneuver severity performed by a surrogate manually-drivable vehicle, during FMVSS compliance tests, is equal to that of the subject ADS–DV? For example, how can the characterization maneuvers and subsequent scaling factors in the FMVSS No. 126 ESC test on the surrogate vehicle be confirmed as equivalent on the ADS–DV?"
Responses to Question 37 & Question 38: Demonstrating equivalence would require some precise definitions of, and ways to measure such equivalence. It may be difficult to demonstrate equivalence in sensor and communication system performance in AVs with a conventional driver-in-the-loop. Performance with conventional controls reflects a relationship between human skill, biomechanics, and force; and the corresponding control mechanism and actuators. There is also a feedback loop that modulates human effort that may be missing in ADS-DVs.

Question. "Use of Surrogate Vehicle With Human Controls " - 39. "If results from FMVSS compliance tests of a conventional vehicle performed by its manufacturer differ from the results of NHTSA tests of an equivalent ADS–DV (particularly if the conventional vehicle complies with the agency's standards, but the ADS–DV does not), can the conflicting results be reconciled? If so, how?"
Response: In the current physical world of manufacturers self-certification, when a manufacturer's results differ from NHTSA results, manufacturers and NHTSA:

1. Initiate an investigation into cause; sometimes an investigation is opened as an enforcement action for non-compliance. In every case, the affected manufacturer would be expected to initiate its non-compliance investigation process.
2. The bases of the manufacturer's compliance claims are collected and reviewed buy NHTSA and the manufacturer.

3. Often, some element of re-testing is performed and data shared by the manufacturer and NHTSA.
4. The differences are resolved and a course of action is agreed upon by NHTSA and the manufacturer, OR,
5. If the dispute is not resolved, NHTSA will commence enforcement action through the Federal court system.

If disputes arise from engineering data, if the differences are eventually understood based upon fact data and information, and each party sees the data and information in the same way, the differences can be reconciled and a course of action agreed upon. If disputes arise from engineering data and if the differences are eventually understood based upon fact data and information, and each party interprets the data and information differently; the differences may not be reconciled among the parties and the dispute will be submitted to the Courts for resolution. NHTSA needn't change this dispute resolution system for disputes that may arise between Av providers' and NHTSA's test results with Surrogate Vehicle Human Controls or between those results and ADS-DV performance results.

Respectively Submitted on behalf of Exponent, Inc.; prepared by authors:

Robert C. Lange, M.S.
Senior Fellow, Principal, Vehicle Engineering Practice

John L. Campbell, PhD, CHFP, PMP
Senior Managing Scientist, Human Factors Practice

Elizabeth Groves, PhD
Managing Scientist, Electrical Engineering and Computer Science Practice

Ray K. Huang, PhD, PE, CFEI
Office Director & Principal Engineer, Electrical Engineering & Computer Science Practice

Chris Monk, PhD
Senior Managing Scientist, Human Factors Practice

Jeffrey Wishart, PhD
Manager, Vehicle Engineering Practice