Silent Majority Strategies

#NHTSA 2018-0092 December 10, 2018

National Highway Traffic Safety Administration
U.S. Department of Transportation (DOT)
1200 New Jersey Avenue S.E.
Washington, DC 20590

Response to the Advance Notice of Proposed Rulemaking: *Pilot Program for Collaborative Research on Motor Vehicles with High or Full Driving Automation/Comments of Silent Majority Strategies LLC*

Silent Majority Strategies (SMS) is a regulatory affairs consulting firm with a focus on technology, energy and the environment. Its principals, and signatories to this comment, have expertise in the regulatory process, administrative law and public policy.[1]

SMS is concerned that NHTSA and US DOT are not sufficiently focused on the critical issue of cyber-security in the development, testing and deployment of Automated Vehicles. The recent document, *Automated Vehicles 3.0 Preparing for the Future of Transportation*, declines to address cyber-security in favor of deferring to the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) and recommends only voluntary standards. Such a policy position is contradictory to NHTSA's genesis, its history and past practice and antithetical to NHTSA's statutory public mission. Should NHTSA commence with an AV pilot program, that program must have strong cyber-security requirements.

NHTSA was created in the 1960s as a reaction to the intolerable injury and death toll on our highways at that time. Since its creation, NHTSA has done an outstanding job implementing its mission to make America's roadways, drivers and driving safe. NHTSA, since its inception has emphasized and implemented its self-stated mission and vision which it has stated in several, similar ways such as:

- being the global leader in motor vehicle and highway safety;
- saving lives, preventing injuries and reducing economic costs due to road traffic crashes, through … safety standards and enforcement;
- to prevent and reduce vehicle crashes;

[1] SMS's principals, former Pennsylvania Department of Environmental Protection Secretary Mike Krancer and Keith Naughton, Ph.D., have extensive experience in politics, regulatory processes and legal affairs. Secretary Krancer is an expert in administrative law, regulatory processes and he has been involved at the highest level of government in highly complex and sometimes controversial matters. Mr. Krancer possesses over 30 years in the practice of law and has served as an Environmental Hearing Board Judge. Dr. Naughton has his Ph.D. in political science and has over 20 years' work experience in the arena of political strategy and communication in addition to expertise in the rulemaking process and public agenda-setting.

- dedicated to achieving the highest standards of excellence in motor vehicle and highway safety and striving to exceed the expectations of the American traveling public through its core values of integrity, service and leadership.

As NHTSA has recognized, "[t]oday, our country is on the verge of one of the most exciting and important innovations in transportation history— the development of Automated Driving Systems (ADSs), commonly referred to as automated or self-driving vehicles".

Necessity of Addressing Cyber-Security

Matters of AV and AV infrastructure safety and cyber integrity are centrally and inseparably intertwined and, thus, centrally and inseparably related to NHTSA's commitment to the Nation to insure highways, roadways and vehicles are safe**. For NHTSA to defer cyber integrity safety in AVs until later or defer to another agency whose primary mission is not highway safety, not only would be a mistake but violates NHTSA's statutorily-designated role, function and mission.** Such deferral would also be inconsistent with how NHTSA has stated its own role with respect to AVs where NHTSA stated that it pursues "a proactive safety approach" to AVs.[2]

Level 4 and 5 Automated Driving Systems will be connected directly with infrastructure, other vehicles and even remote-control centers. Levels 3, 4 and 5 ADS will also likely also be subject to over-the-air software updates. Unlike Level 0, 1 and 2 systems, Levels 3, 4 and 5 ADS will control vehicles without human input and thus errors in ADS operation will put other vehicles, their passengers and pedestrians at significant safety risk. As a result, vehicle software is a direct safety issue for NHTSA.

SMS is not aware of any precedent where NHTSA or any other safety-tasked Federal Agency) declined to act on identifiable safety risks.

NHTSA has shown itself through the years to be admirably nimble and proactive in protecting the American public the past when new technology, as it always does, comes on the scene. The iconic traffic safety engineer and past President of the Institute of Traffic Engineers, Matthew Sielski[3] in his landmark article, *Implementing the 1966 Highway Safety Acts* noted that, "the most important point and purposes of the Highway Safety Acts of the 60's is to promote the development of new counter-measures against accidents and their end results."[4] That AV technologies are developing quickly is exactly why NHTSA needs to act up-front on cyber integrity for AVs and AV infrastructure to provide for standards for the development of new counter-measures to protect the safety of the highways. NHTSA should be the

---

[2] https://www.transportation.gov/transition/nhtsa-top-policy-issues

[3] Mr. Sielski was in on the ground floor in the 1960s in the passage of the National Traffic and Motor Vehicle Safety Act of 1966 and the Federal Highway Safety Act of 1970 and one of the original commentators on those acts. He is past President of the Institute of Transportation Engineers. From 1938 to 1946 Mr. Sielski was Traffic Engineer of the Chicago Motor Club and from 1946 to 1963 was Director of the Safety and Traffic Engineering Department. In 1963 he became Director of the Traffic Engineering and Safety Department of AAA in Washington, DC. In 1967, Mr. Sielski joined the Federal Government as Director of the Office of Driving Environment Programs of the National Highway Safety Bureau and in 1968 went back to Chicago to become the Vice President for Safety and Traffic Engineering for the Chicago Motor Club. He was long active in the National Safety Council being Past Chairman of the Executive Committee of the Traffic Conference and a member of the Board of Directors of the Council. He was also active in the Highway (Transportation) Research Board.

[4] https://docs.lib.purdue.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=3150&context=roadschool

driving force and lead Federal Agency in that effort.

For NHTSA to confer with other agencies such as DHS is wise, but to decline and defer its primary regulatory role on this issue to another agency (especially agencies whose primary mission is not highway traffic safety) is at variance with the Agency's statutorily designated obligations, mission and creational function. Issues of cyber-security and cyber integrity within AV's and AV infrastructure goes significantly and importantly beyond the issue of external threats by malevolent actors. Cyber integrity and cyber-security for AVs and AV infrastructure goes right to the heart of highway traffic safety. This situation is analogous to the air transportation arena, where external threats are policed primarily by DHS but the overall operational safety of the air traffic system, i.e., air traffic safety, is not a DHS matter, but rather an FAA matter. For AVs and AV infrastructure, the analogue to the FAA would clearly be NHTSA. The issue is core to the safety and integrity of AVs themselves and AV transportation in general. Thus, the issue is squarely a NHTSA issue and ought to be regulated in the spirit of NHTSA's Vision, Core Values and Integrity.

SMS believes that NHTSA has a statutory duty and mission as well as the mandate of historical practice to make cyber-security a central part of its regulating and setting standards for Automated Vehicles and AV infrastructure. "NHTSA works every day to help Americans drive, ride and walk safely. We do this by promoting vehicle safety innovations, rooting out vehicle defects, setting safety standards for cars and trucks, and educating Americans to help them make safer choices when driving, riding, or walking."[5] **Any pilot program promulgated by NHTSA, US DOT or any other US DOT agency must include robust cyber-security requirements.**

Appropriate Cost-Benefit Analysis

In its ANPRM, NHTSA states that Executive Orders 12866 and 13563 are applicable. As such, it is incumbent on the Agency to pursue a cost-effective strategy in the development and promulgation of any pilot test program. Furthermore, as the adoption of any future regulatory requirements regarding the safety of AVs would certainly fall under the authority of EO 12866 and 13562, determining the cost-effectiveness of various safety measures would be necessary.

In view of the immediate and reasonably anticipated requirements of EO 12866 and 13563, SMS believes that NHTSA should engage in a rigorous cost-benefit analysis of proposed and potential safety measures, as well as the potential costs and benefits associated with the adoption of AV technology. SMS is concerned that the Agency has not and is not considering the correct empirical data for the statutorily-required cost-benefit calculations. Specifically, NTSA and other commenters have cited the figure that 94% of vehicle crashes are due wholly or in part to human error. The implication is that AV technology will reduce or even eliminate such errors in favor of error-free automated vehicles. The empirical evidence to date definitively contradicts this implication.

According the information placed on the public docket by Advocates for Highway and Auto Safety (Docket ID# DOT-OST-2018-0149-0059), the 2017 accident rate was one (1) traffic death per 86 million miles of (human-operated) driving, yet the fatal accident rate for one AV company testing high-level AVs (Level 4/5) is one (1) fatality per 3 million miles – nearly 29 times that of human operated vehicles. Therefore, the assumption that Level 4/5 eliminates human error and substitutes it with zero or very low error is, at this time, empirically disproven. The cost-benefit assumption that AV technology

[5] Transportation.gov - Understanding the NHTSA https://www.transportation.gov/transition/understanding-national-highway-traffic-safety-administration-nhtsa

will automatically result in safer transit should no longer be incorporated in NHTSA or other US DOT documents. Instead, US DOT and NHTSA should acknowledge that increased safety is not automatically assured without robust empirical (not theoretical) evidence.

AV's introduce cyber risk as a wholly new safety risk to transit, which not only has the potential to undermine potential benefits from automated vehicles but also has the potential to raise risks to a level at which the adoption of AVs results in a negative cost-benefit result. In addition, a collapse in public support and willingness to adopt AV technology that would come from cyber-security breaches would likely cause significant delays in adoption of AV technology and economic loss, thus delaying possible public safety, efficiency and productivity benefits from more mature and advanced AV platforms.

Given these facts, SMS recommends:

1) *NHTSA, US DOT and all US DOT agencies should make clear in any future documents that the citation of 94% human error in vehicle crashes does not state nor imply that the advent of automated vehicle technology which removes human decision-making (Levels 4 and 5) will result in a concomitant 94% fall in vehicle crashes, i.e. automated vehicle technology is not 100% risk-free.*
2) *NHTSA conduct a rigorous and comprehensive empirically-driven cost-benefit analysis in companion with any pilot test which will include cyber-security risks as a cost. Such a study should consider the costs of delayed adoption due to cyber-security incidents.*

Thank you for the opportunity to submit comments regarding this important public policy issue.

Submitted for Consideration

S/S

Keith Naughton, Ph.D.
Principal

S/S

Mike Krancer
Principal