U.S. Department of Transportation
National Highway Traffic Safety Administration

1200 New Jersey Avenue SE.
Washington, DC 20590

July 20, 2020

The Honorable Tackey Chan
House Chair, Joint Committee on Consumer Protection and Professional Licensure
State House, Room 42
Boston, MA 02133

The Honorable Paul R. Feeney
Senate Chair, Joint Committee on Consumer Protection and Professional Licensure
State House, Room 215
Boston, MA 02133

Dear Representative Chan and Senator Feeney:

Thank you for your June 17, 2020, letter to the National Highway Traffic Safety Administration (NHTSA) seeking written testimony on Massachusetts Initiative Number 19-06, Initiative Law to Enhance, Update and Protect the 2013 Motor Vehicle Right to Repair Law. The Agency appreciates the opportunity to provide a formal response to the questions posed in your letter.

It is worth noting that NHTSA does not take issue with efforts relating to data ownership, privacy, or serviceability, to the extent they do not affect motor vehicle safety. In fact, in NHTSA's published *Cybersecurity Best Practices for Modern Vehicles* document,[1] section 9 recommends that the automotive industry should provide strong vehicle cybersecurity protections that do not unduly restrict access by authorized alternative third-party repair services.[2]

As NHTSA understands it, this ballot initiative would require, beginning with the 2022 model year,[3] that all vehicle manufacturers selling new telematics-equipped vehicles into the State— including heavy duty vehicles with a gross vehicle weight rating of more than 14,000 lbs., in addition to passenger vehicles— design their systems in such a way that provides owners and

[1] https://www.nhtsa.gov/document/cybersecurity-best-practices-modern-vehicles.
[2] *See id*. at 21, "Serviceability. The automotive industry should also consider the serviceability of vehicle components and systems by individuals and third parties. The automotive industry should provide strong vehicle cybersecurity protections that do not unduly restrict access by authorized alternative third-party repair services."
[3] Model Year 2022 vehicles become broadly available for purchase in the Fall of 2021, with earliest models introduced as early as Spring 2021.

third-party repair facilities with access to the vehicle systems through an inter-operable, standardized, and open access telematics platform. The initiative would specifically require that telematics platforms be directly accessible through a mobile-based application, and that this access must include the ability to send commands to in-vehicle components (including, e.g., braking, acceleration, and steering controls). While the initiative requires the system to be "secure," it does not define what that vague term means, nor does it reflect any established best practices or other measures to address cybersecurity risks. Further, the initiative does not discuss the variety of telematics offerings available to consumers today, nor does it address feasibility, practicality, or availability of protocols or other measures that could appropriately protect against cybersecurity risks that would be introduced via proposed forms of third party telematics access.

You request information about whether aspects of the initiative might introduce additional cybersecurity risks to motor vehicles and public safety risks to road users, such as malicious hacking attempts. You also request information about whether the initiative might impact Federal motor vehicle safety efforts.

As this testimony will further elaborate, it is our view that the terms of the ballot initiative would prohibit manufacturers from complying with both existing Federal guidance and cybersecurity hygiene best practices.[4] NHTSA is also concerned about the increased safety-related cybersecurity risks of a requirement for remote, real-time, bi-directional (i.e., read/write capability) access to safety-critical vehicular systems. Given the multi-year automotive product development cycle, the deadline for compliance appears impossible for manufacturers to meet in a responsible manner, risking removal of existing cybersecurity controls over wireless access into vehicles as the ballot initiative directs, which increases the risk of cybersecurity attacks that could jeopardize public safety. Further, the requirement to establish universal and standardized access requirements increases the scale of risks of any potentially successful cybersecurity attack.

NHTSA's Cybersecurity Interests

As background, NHTSA's statutory authorities center on motor vehicle safety.[5] Accordingly, NHTSA's primary interest focuses on cybersecurity vulnerabilities that present potential vehicle safety consequences, which is a subset of the universe of cybersecurity. The increase in uses of software-intensive motor vehicle components, including telematics systems, introduces new and different risks to motor vehicle safety. Risks include the potential that the technological methods, tools, and capabilities could be compromised and used in ways that create unintended, and at times, unsafe outcomes. The specific possibility of a software vulnerability potentially being used by malicious actors to cause a crash or incident is the primary cybersecurity concern

[4] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf.
[5] 49 U.S.C. § 30101 et seq.

for NHTSA as the safety oversight agency for the automotive industry. NHTSA has authority to order vehicle recalls based on unreasonable risks to safety including those that may be caused by cybersecurity vulnerabilities.[6]

For years, NHTSA has worked to encourage industry to adopt improved cybersecurity practices, recognizing that cybersecurity risks are real, and that protection of safety-critical vehicle systems from malicious hacking attempts is vital to the safety of the motoring public. Telematics systems are an area of great concern to the agency, because such systems could allow actors to receive and/or send information to vehicles outside of the vehicle itself, and potentially interface with multiple vehicles at a time, and to do so without gaining physical access to the vehicle. In 2016, NHTSA published a *Cybersecurity Best Practices for Modern Vehicles* document to provide guidance to manufacturers and suppliers in developing strategies to make their vehicles more secure against malicious attacks and more resilient if such attacks are successful. This guidance encouraged manufacturers to harden safety-critical systems, identify and evaluate risk during system and vehicle development processes, and develop layers of protection throughout vehicles to protect against access by unauthorized third-parties and which are appropriate for the identified risks.

Cybersecurity Concerns with Massachusetts Initiative Number 19-06

One key recommendation in NHTSA's guidance is that manufacturers should control access to firmware that executes vehicle functions. This is particularly important for firmware controlling vehicle motion such as steering, acceleration, and braking. Such control and protection likely will be more challenging for manufacturers to administer if required to provide "the ability to send commands to in-vehicle components." We understand that in response to this requirement in the ballot initiative for *real-time, bi-directional access* that manufacturers have raised significant cybersecurity and consumer privacy concerns. Further, Section 2 of the ballot suggests that access to the telematics systems "… shall not require any authorization by the manufacturer, directly or indirectly…" "…unless the authorization system for access to vehicle networks and their on-board diagnostic systems is standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer."

NHTSA is not aware of any existing system architectures that would satisfy the requirements of the ballot initiative, and they are unlikely to be developed, tested, validated and deployed in the proposed timeframe. Therefore, manufacturers that offer telematics systems could find themselves in a situation that would require them to remove all access controls from their telematics systems, including controls designed to ensure the security of safety-critical systems. NHTSA has grave concerns with any proposed policy that would effectively prohibit wireless access controls in motor vehicles sold in the United States. This would raise substantial safety risks for American families.

[6] *See, e.g.*, NHTSA Recall Campaign Number 15V461000. This recall addressed a Fiat-Chrysler cybersecurity vulnerability involving 1.4 million vehicles.

Another key recommendation in NHTSA's guidance to the automotive industry, based on established cybersecurity practices, is for manufacturers to implement logical and physical isolation techniques—to the extent possible—to separate processors, vehicle networks, and external access points to limit and control pathways from external threat vectors to cyber-physical features of vehicles. This is important because the best way to prevent a malicious hacker from remotely taking control of a vehicle or manipulating its performance is to ensure that there is no pathway by which external connections can access and send commands to in-vehicle components. The ballot initiative would specifically *require* that vehicles be redesigned so that they are *not* isolated by mandating the ability to remotely "send commands to in-vehicle components" such as steering, braking, and acceleration systems, thus creating another direct conflict with existing Federal guidance. While the isolation recommendation does not prohibit a manufacturer from offering limited access to certain functionality, manufacturers currently have the flexibility and responsibility to design in layers of protections commensurate to their risk assessment, and to eliminate potential cybersecurity hazards where available techniques cannot lower overall risks to acceptable levels. The ballot initiative would require manufacturers to provide remote functionality that may potentially pose an unreasonable risk to safety, and further, eliminate their flexibility and ability to provide appropriate remote access controls.

We note the language in Section 2 of the ballot initiative, requiring that access to on-board diagnostic systems be standardized across all makes and models sold in Massachusetts, is ambiguous as to whether a uniform system architecture is required across *all* manufacturers or across makes and models sold within an individual manufacturer's portfolio. Either approach creates concerns. Vehicle manufacturers do not generally maintain a uniform system architecture across the industry, given market competition, antitrust laws, and intellectual property concerns. Even within manufacturers that produce multiple brands, they do not generally maintain a uniform system architecture across each make and model in their lineup, as the ballot initiative would require. A non-standardized approach provides cybersecurity benefits such that the scale and potential consequence of any specific cyberattack is inherently reduced. Having more vehicles with a common architecture—especially if that architecture provides a link between external connections and in-vehicle components—means that a single successful malicious cyberattack could have much wider scale of consequences because it can affect a larger number of vehicles.

Conclusion

Managing vehicles' lifetime cybersecurity risks is an extremely challenging undertaking: malicious actors, some of which are sponsored by hostile foreign governments, have the motivations, resources, and tools available to compromise access to safety-critical systems. A cyberattack on one or more motor vehicles has enormous potential safety consequences—a 4,000 to 80,000 lbs. vehicle operating at highway speeds can pose an incredible amount of danger to its surroundings if manipulated. This is why NHTSA continues to devote significant resources to the development and refinement of best practices and works with industry to identify techniques to harden vehicle systems. Two of the most important techniques—logical and physical isolation of vehicle control systems from external connections, and controlling access to firmware that

executes vehicle functions—may be rendered impossible by the provisions of this ballot initiative. The ballot initiative requires vehicle manufacturers to redesign their vehicles in a manner that necessarily introduces cybersecurity risks, and to do so in a timeframe that makes design, proof, and implementation of any meaningful countermeasure effectively impossible.

As stated earlier, NHTSA acknowledges the need for serviceability access by authorized third parties and has dedicated a section in its guidance document recommending that the industry not unduly restrict access by authorized alternative third-party repair services. However, steps proposed to ease access for serviceability cannot be allowed to compromise vehicle cybersecurity and public safety.

Additionally, you request information about whether aspects of the initiative might introduce consumer privacy risks to vehicle owners. NHTSA recommends that you contact the Federal Trade Commission, the Federal agency that primarily oversees privacy policy and enforcement,[7] for its assessment of any potential consumer privacy risks.

Sincerely,

James C. Owens
Deputy Administrator

[7] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security.