1300 Terra Bella Avenue, Suite 100 | Mountain View, CA 94043 | info@nuro.ai | www.nuro.ai

March 15, 2021

Cem Hatipoglu
Associate Administrator for Vehicle Safety Research
National Highway Traffic Safety Administration
U.S. Department of Transportation
1200 New Jersey Avenue S.E.
Washington, DC 20590

Docket No. NHTSA-2020-0087

Dr. Hatipoglu:

We write in response to the Request for Comment on Docket No. NHTSA-2020-0087, *Cybersecurity Best Practices for the Safety of Modern Vehicles*. Nuro commends your attention to this important topic and appreciates the opportunity to provide comment.

Nuro is developing autonomous vehicles (AVs) that are custom-built for local deliveries. We have partnerships with leading companies including Kroger, CVS Pharmacy, and Walmart to conduct deliveries of essential goods to customers. We have built a new class of vehicle from the ground up: our lightweight, electric, and occupantless vehicles are originally engineered and manufactured to be operated autonomously.

We agree with the approach that NHTSA has taken in providing flexible, non-binding, and voluntary guidance and best practices. This strategy, coupled with a culture that prioritizes cybersecurity within each company and across the entire industry, will help to guide the safe and secure operation of all motor vehicles on U.S. roadways. Given the varied approaches to vehicle designs, use cases, and business models — particularly those enabled by automated driving systems — it is essential for federal agencies' policies to reflect that there is not a uniform nor one-size-fits-all approach to cybersecurity. Prescriptive regulations and over-specification could inadvertently create new, unintended challenges.

It is the joint responsibility of vehicle manufacturers, technology companies, and parts suppliers to ensure that motor vehicles and their components are secure throughout the development, testing, and deployment phases. Vehicles are cyber-physical systems and it must be a priority to ensure each vehicle is secure.

As a business-to-business company, Nuro programs, operates, and maintains our fleet throughout the entire lifecycle of each vehicle. Nuro is mindful of the multitude of attack

vectors that must be considered for vehicles and their individual components. We monitor the physical, software, and network infrastructures to identify vulnerabilities and defend against potential attackers.

Federal regulators and industry — from automakers to technology companies to suppliers — have essential roles to play in mitigating cybersecurity risks. We appreciate NHTSA's attention to the importance of addressing cybersecurity throughout the entire supply chain. To this end, we share NHTSA's view that continued collaboration and communication between vehicle manufacturers and suppliers will ultimately make our roadways safer and more secure. Nuro communicates the importance of cybersecurity collaboration to our suppliers with the belief that this is essential for public safety.

Moving forward, we encourage NHTSA to also consider the diversity of applications in which AVs will be deployed and utilized. The new business models and vehicle form factors enabled by autonomy may merit different considerations than mass-market passenger vehicles. For example, Nuro's fleet-based delivery service uses occupantless AVs that only carry goods, and will never have human drivers or passengers.

Thank you for your continued attention to this important issue and the opportunity to provide comment. If you have any questions, please do not hesitate to contact us.

Regards,

David Estrada
Chief Legal Officer
Nuro