August 17, 2021

SUBMITTED ELECTRONICALLY VIA EMAIL

Dr. James Olthoff
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Re: Cybersecurity Labeling Programs for Consumers

Dear Dr. Olthoff:

The Alliance for Automotive Innovation ("Auto Innovators")[1] appreciates this opportunity to provide input to the National Institute for Standards and Technology ("NIST") in response to its request for papers on the challenges and practical approaches to consumer software labeling, pursuant to the directives in the Executive Order on Improving the Nation's Cybersecurity.

Auto Innovators was formed last year to serve as the singular, authoritative, and respected voice of the automotive industry in the United States. Our members include auto manufacturers producing nearly 99 percent of the cars and light trucks sold in the U.S., along with original equipment suppliers, technology companies, and other automotive-related value chain partners. In total, our industry supports roughly 10 million jobs in America, accounts for nearly 6 percent of our country's gross domestic product, and represents our country's largest manufacturing sector.

Auto Innovators welcomes the Administration's attention to critical cybersecurity challenges that confront our increasingly connected and digital world. Products and services that once only existed in the physical world are now part of our connected society. Automobiles are no exception. Innovative vehicle technologies, combined with the integration of vehicles into a broader ecosystem of connected infrastructure, devices, features, and stakeholders can unlock a wide range of benefits in safety, fuel efficiency, and convenience. This transformation also provides consumers with new and, increasingly,

[1] The Alliance for Automotive Innovation represents the manufacturers producing nearly 99 percent of cars and light trucks sold in the U.S. Its members are listed as follows: Aisin Group, Autoliv, APTIV, Argo AI, BMW Group, Bosch, Byton, Cruise, DENSO, Ferrari, Ford, GM, HARMAN, Honda, Hyundai, Infineon, Intel, Isuzu, Jaguar Land Rover, Karma, Kia, Luminar, Mazda, Mercedes-Benz, Mitsubishi Motors, Nissan, NXP, Panasonic, Porsche, RV Industry Association, Sirius XM, Stellantis, Subaru, Suzuki, Texas Instruments, Toyota, Volkswagen Group of America and Volvo.

remote ways of interacting and engaging with vehicles, spurring innovative businesses, technologies, and services.

The benefits of this transformation have the potential to be profound, driving us to a cleaner, safer, and smarter future. Yet, the technologies at the forefront of this evolution – including connectivity, electrification, automation– may also introduce new threats and risks. These increasingly digital, rather than mechanical, challenges are also no longer isolated to the confines of vehicles. They extend to the vast ecosystem of connections and external stakeholders, introducing factors outside an automaker's control.

The automotive industry understands the realities of a connected world and has been working proactively and collaboratively to build cybersecurity into the products and services that will define the future of transportation. In order to realize the safety, privacy, environmental and societal benefits of vehicles with advanced technologies, consumers must have confidence in the security of those products.

Providing consumers access to information about the security of consumer products is a worthwhile endeavor. The challenge is in determining how best to provide consumers with that information and in ensuring that the information provided is understandable and useful. As NIST begins to explore these important questions Auto Innovators offers the following auto industry perspective:

- Participation in any cybersecurity labeling program for consumer products should be voluntary. This enables the program to be more nimble and adaptable to a dynamic environment and encourages competition and innovation across industry.
- A cybersecurity labeling program for consumer products should account for the diversity of consumer products.
    - While certain types of consumer products may make sense for inclusion in a cybersecurity labeling program, it may be significantly more difficult to provide consumers with understandable and useful information about other consumer products – including those that are increasingly complex systems of connected components – through such a labeling program.
    - The safety of some consumer products is regulated by federal agencies or otherwise subject to existing security requirements or standards. In the interest of avoiding any inconsistencies or incompatibilities with existing regulatory guidance or requirements, it may be most appropriate to exclude these regulated products from a consumer product labeling program.
    - There are unique security considerations for different consumer products. For example, some consumer products have longer lifecycles, more complex supply chains and/or architectures, as well as connections with third party devices and services. To accommodate this variation, NIST should consider incorporating industry standards, including sector-specific security standards, into any voluntary cybersecurity labeling program.
- Given the dynamic and rapidly-evolving nature of cyber threats, an overly prescriptive approach to a cybersecurity labeling program may ultimately prove ineffective in keeping pace with the

security landscape. This runs the risks of labels become outdated – and thus of little use to consumers – in a relatively short period.

We appreciate the opportunity to provide input and perspective into these complex and important questions and look forward to further engagement with NIST on this issue.

Sincerely,

Hilary M. Cain
Vice President
Technology, Innovation, & Mobility Policy
Alliance for Automotive Innovation