Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
	)	PS Docket No. 23-239
Cybersecurity Labeling for Internet of Things	)	
	)	
	)	

COMMENTS OF THE ALLIANCE FOR AUTOMOTIVE INNOVATION

The Alliance for Automotive Innovation ("Auto Innovators") hereby submits the following comments in response to the Federal Communications Commission's ("Commission") Proposed Rule in the above-captioned proceeding. Auto Innovators appreciates that the Commission seeks to develop a voluntary cybersecurity labeling program that would help consumers compare Internet of Things ("IoT") devices and make informed purchasing decisions, drive consumers toward purchasing devices with greater security, incentivize manufacturers to meet higher cybersecurity standards to meet market demand, and encourage retailers to market secure devices.

I. INTRODUCTION

Auto Innovators represents the manufacturers that produce most of the cars and light trucks sold in the U.S., original equipment suppliers, battery makers, technology companies, and other value-chain partners within the automotive ecosystem. Representing approximately 5 percent of the country's GDP, responsible for supporting 10 million jobs, and driving $1 trillion in annual economic activity, the automotive industry is the nation's largest manufacturing sector.

II. THE AUTOMOTIVE INDUSTRY PRIORITIZES CYBERSECURITY IN AN INCREASINGLY INTERCONNECTED WORLD

An increasingly connected and digital world finds vehicles integrated into a broader ecosystem of connected infrastructure, devices, features, and stakeholders. Combined with innovative vehicle technologies, this integration can result in a wide array of safety, fuel efficiency, and transportation equity benefits. However, these opportunities also present new cybersecurity threats and risks, including some that are no longer isolated to the vehicle itself. Although the automotive industry continues to build cybersecurity proactively into its products and services, cybersecurity threats and risks can now extend to the vast ecosystem of connections, including the Internet of Things ("IoT"), and external stakeholders. To realize the safety, environmental, and societal benefits of vehicles with advanced and connected technologies, consumers should have confidence in the cybersecurity of this interconnected ecosystem.

III. PRODUCTS CURRENTLY REGULATED FOR CYBERSECURITY SHOULD BE EXEMPT

Providing consumers with access to information about the security of consumer products is a worthwhile endeavor. The creation of a voluntary cybersecurity labeling program for IoT consumer devices is helpful to that end. As the National Cybersecurity Strategy states, the ability of consumers to compare cybersecurity protections offered by different consumer IoT devices has the potential to incentivize security across the entire IoT ecosystem.[1] However, it is important to recognize the significant difficulty with providing consumers with

[1] National Cybersecurity Strategy, p. 20. National-Cybersecurity-Strategy-2023.pdf (whitehouse.gov)

understandable and useful information about the relative security of all consumer products. For example, some consumer products have longer lifecycles and more complex supply chains and/or architectures, as well as connections with third party devices and services. As such, the security considerations for such products are often unique and more nuanced.

In addition, the cybersecurity of some consumer products is already 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, the proposed voluntary cybersecurity labeling program should account for existing cybersecurity regulatory guidance or requirements and not apply to such regulated products.

IV. OTHER CONSIDERATIONS

Any voluntary cybersecurity labeling program should rely upon the definition of IoT device developed by the National Institute of Standards and Technology ("NIST") through its consultative, multistakeholder process.[2] Such a program should apply prospectively, allow for sufficient lead time, and be flexible and nimble to address both the wide range of consumer IoT devices on the market, as well as the evolving cybersecurity threat landscape impacting such devices. Furthermore, any labeling scheme should be clear and simple, avoid unnecessary information that may distract consumers from understanding important security considerations, and accommodate a range of formats. To help incentivize participation in the

---

[2] NIST defines "IoT device" as "one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution [LTE], Zigbee, Ultra-Wideband [UWB]) for interfacing with the digital world." See NIST IR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers (nist.gov).

voluntary program, obtaining a label and maintaining the IoT device's security measures consistent with the label over time, should provide a safe harbor or affirmative defense against liability for damages resulting from a cyber incident.

The Commission should consider periodic reviews of the labeling program to evaluate the impact of the labeling on improving cybersecurity and consumer decision-making, as well as the utility, effectiveness, and costs associated with the labeling. Another factor for the Commission's consideration is the interoperability of such labeling across jurisdictions, by grounding the program in international and sector-specific standards.

V. CONCLUSION

Auto Innovators appreciates the opportunity to provide the automotive industry's perspective on the proposed voluntary cybersecurity labeling for IoT devices program. We look forward to continued engagement with the Commission and other government stakeholders on this important effort.

Respectfully submitted,

/s/ Tara Hairston

Tara Hairston
Senior Director, Technology,
Innovation, and Mobility Policy

Alliance for Automotive Innovation
1050 K Street NW
Suite 650
Washington, DC 20001

October 6, 2023