October 15, 2021

SUBMITTED ELECTRONICALLY VIA EMAIL

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

Re: DRAFT Baseline Security Criteria for Consumer IoT Devices White Paper

Dear Dr. Olthoff:

The Alliance for Automotive Innovation ("Auto Innovators") appreciates this opportunity to provide input to the National Institute of Standards and Technology ("NIST") in response to the request for comments on its draft white paper entitled, "Baseline Security Criteria for Consumer IoT Devices," pursuant to its work as directed by Executive Order 14028 on Improving the Nation's Cybersecurity.[1]

Formed in 2020, Auto Innovators serves as the singular, authoritative, and respected voice of the automotive industry in the United States. Our members include auto manufacturers, original equipment suppliers, technology companies, and other automotive-related value chain partners. In total, our industry supports roughly 10 million U.S. jobs, accounts for nearly 6 percent of U.S. GDP, and represents the largest manufacturing sector in the country.

Auto Innovators welcomes the Administration's attention to the critical cybersecurity challenges confronting our increasingly connected and digital world. The integration of vehicles into a broader ecosystem of connected infrastructure, devices, features, and stakeholders – combined with innovative vehicle technologies – can unlock a wide array of benefits in safety, fuel efficiency, and transportation equity. This transformation in personal mobility also provides consumers with new ways of interacting and engaging with vehicles, spurring new business models, technologies, and services.

A cleaner, safer, and smarter transportation future is possible. However, these opportunities also present new cybersecurity threats and risks, including some that are no longer isolated to the confines of vehicles. Although the auto industry continues to build cybersecurity proactively into the products and services that will define the future of transportation, cybersecurity threats and risks can now extend to the vast ecosystem of connections and external stakeholders. To realize the safety, privacy, environmental, and societal benefits of vehicles with advanced and connected technologies, it is imperative that consumers have confidence in the cybersecurity of this interconnected ecosystem.

---

[1] Executive Order 14028 of 12 May 2021, "Improving the Nation's Cybersecurity," published in the *Federal Register* on 17 May 2021: https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf.

As Auto Innovators expressed in its response to NIST's call for papers in August, it is a worthwhile endeavor to provide consumers with access to information about the cybersecurity of consumer products. Nevertheless, the challenge is determining how to best provide this information, in terms of delivery and content (*i.e.*, is the information understandable and useful). With regards to the white paper on draft baseline security criteria for consumer IoT devices, Auto Innovators offers the following auto industry perspective:

- **Incentivizing Participation:** Executive Order 14028 directs NIST to "consider ways to incentivize manufacturers and developers to participate" in proposed labeling programs. In assessing the value of such a labeling program, NIST should also consider the market incentives, existing regulatory requirements, current standards and sectoral best practices, and other safety imperatives that manufacturers and developers already have to ensure the security of their products. In addition, any participation in a labeling program for consumer products should be voluntary, and manufacturers and developers should be able to self-attest to conforming with any labeling criteria and related technical requirements.

- **Clarifying Applicability:** Executive Order 14028 provides no definition for "consumer product" to ground NIST's work on baseline security criteria for "consumer" IoT devices. Auto Innovators maintains that the Safety Act's definition of "consumer product," as regulated by the Consumer Product Safety Commission ("CPSC")[2], could be a useful guidepost for this important exercise.

- **Excluding Regulated Products:** Existing regulatory requirements or standards for safety and cybersecurity may preclude products from demonstrating several of the proposed criteria related to product configuration, data deletion, update provisioning, and logical access to interfaces. To avoid the potential for such incompatibility, it may be prudent to exclude these regulated products from baseline security criteria and any related labeling regime.

- **Establishing Minimum Criteria:** Existing regulatory requirements or standards may also prevent certain products from demonstrating "increasingly comprehensive levels of testing or assessment." Under some regulatory or standards regimes, the product either meets the criteria or it does not. Also, given regulatory requirements, manufacturers or developers may not have "options regarding how their products' conformity with security criteria can be assessed." If these regulated products are not exempt from these baseline security criteria, then any externally facing consumer information that shows that the product has met minimum cybersecurity standards should be sufficient.

- **Avoiding an Overly Prescriptive Approach:** An overly prescriptive approach to baseline security criteria may prove ineffective in keeping pace with the dynamic and rapidly evolving nature of cybersecurity threats, and as a result, provide little informational value to, or cybersecurity state awareness for, consumers.

---

[2] See 15 U.S.C. §2052(a)(5).

- **<u>Accounting for Complexity:</u>** Baseline security criteria should account for the diversity of consumer products, particularly since it may be significantly more difficult to provide understandable and useful information about consumer IoT devices that are complex systems of connected components. The proposed documentation and information dissemination criteria do not seem to account for product complexity.

Auto Innovators appreciates the opportunity to provide input and perspective on these baseline security criteria and looks forward to further engagement with NIST on this important issue.

Sincerely,

Tara Hairston
Senior Director
Technology, Innovation, & Mobility Policy