ALLIANCE FOR AUTOMOTIVE INNOVATION

September 25, 2023

Ms. Barbara Cuthill
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Ms. Cuthill:

The Alliance for Automotive Innovation ("Auto Innovators") welcomes the opportunity to provide comments on *A Preliminary Update from the Internet of Things Federal Working Group* ("Preliminary Update"). We appreciate the ongoing effort to collaborate and coordinate across the federal government on the Internet of Things (IoT) and welcome the development of a comprehensive roadmap or strategy that can help promote and enable the IoT.

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.

We particularly appreciate the Federal Working Group's recognition of the benefits and opportunities of integrating IoT technologies into transportation. There is no doubt that transportation is a key part of the emerging IoT and that the auto industry is at the forefront of IoT-enabled innovation in the transportation sector. As the Preliminary Update notes, IoT can help improve the safety, reliability, and efficiency of cars. We welcome interest in this area of innovation and look forward to continued collaboration and engagement with the Federal Working Group to advance this shared priority.

STRATEGIC PILLARS

Auto Innovators is generally supportive of the strategic pillars laid out in the Preliminary Update. We seek to provide some additional perspective and context on how some of these pillars are currently addressed by the automotive sector and also recommend some areas of potential engagement for the Federal Working Group.

- **TRUST & DATA GOVERNANCE:** Auto Innovators agrees that privacy is essential to garnering consumer trust and confidence in IoT. Auto companies in the U.S. are committed to protecting consumer privacy and have long been trusted stewards of vehicle data. The groundbreaking Privacy Principles for Vehicle Technologies and Services (Privacy Principles), which are enforceable by the Federal Trade Commission, represent a proactive and unified commitment by automakers to protect identifiable information collected through in-vehicle technologies and continue to distinguish the auto industry from other industries as

one dedicated to safeguarding consumer privacy. The Federal Working Group may want to consider leveraging the baseline privacy protections contained in the Privacy Principles for other IoT sectors. These protections include:

- providing consumers with ready access to clear, meaningful notices about the collection, use, and sharing of identifiable information;
- obtaining affirmative consent before using sensitive information for marketing purposes;
- obtaining affirmative consent before sharing sensitive information with unaffiliated third parties;
- using and sharing identifiable information only in ways that are consistent with the context in which the information was collected;
- collecting and retaining identifiable information only as needed for legitimate business purposes; and
- implementing reasonable measures to protect identifiable information against loss and unauthorized access or use.

Auto Innovators also recognizes that cybersecurity is crucial to realizing the benefits of IoT, including automotive IoT. The auto industry is doing its part by proactively building cybersecurity into its products and services. However, the Working Group should recognize that the integration of vehicles into a broader ecosystem of connected infrastructure, devices, features, and stakeholders involves factors outside of the control of the auto industry. Ultimately, the entire ecosystem will need to work together to address IoT security in a holistic and comprehensive way. Moreover, as the cybersecurity threat environment is dynamic, it is important that the regulatory and policy environment governing automotive IoT remain nimble and adaptive.

It is also important for the Federal Working Group to recognize that cybersecurity risk cannot be eliminated, only managed and mitigated. The Federal Working Group should focus on promoting and building on well-respected cybersecurity risk management frameworks (such as National Institute of Standards and Technology Cybersecurity Framework) and industry standards and best practices (e.g., ISO/SAE 21434, best practice guides developed by the Automotive Information Sharing and Analysis Center, and the Cybersecurity Best Practices for Modern Vehicles from the National Highway Traffic Safety Administration).

Finally, the industry shares the Federal Working Group's interest in addressing counterfeits. The automotive industry's extensive investments in research and development and ongoing innovation to provide the safest and most energy-efficient vehicles for American drivers

must be protected from the growing threat of counterfeit automotive components. Motor vehicle safety critical components, if counterfeit, may not operate or perform as intended. Counterfeit motor vehicle parts not only infringe on valid intellectual property rights; they also give rise to serious public health and safety concerns and undermine the competitiveness of automotive manufacturing in the U.S. To supplement interdiction of infringing goods, the Federal Working Group should encourage statutory clarification regarding the ability of Customs and Border Protection (CBP) to share additional information with right holders and brand owners.

- **CONNECTIVITY:** Auto Innovators agrees with the Federal Working Group's focus on connectivity needs. There is no doubt that the auto industry will require additional spectrum to both bring new technologies to market and ensure that existing technology can reach more consumers. Indeed, as technology evolves, the automotive industry is now faced with a rapidly growing demand for spectrum.

  For example, the industry requires additional spectrum to both fully realize the promise of V2X and to develop next-generation V2X technologies. V2X technologies enable an array of traffic safety benefits for drivers, cyclists, and pedestrians alike. While the Federal Communications Commission (FCC) has allocated 30 megahertz of spectrum in the 5.9 GHz band for basic V2X technologies, this allotment does not support more advanced use cases, such as cooperative sensor sharing between vehicles. Put another way, the 30-megahertz allotment for V2X is insufficient bandwidth to meet the industry's full range of spectral needs. Moreover, there is no spectrum currently allocated for next generation V2X technologies.

  The automotive industry also lacks sufficient spectrum for wireless charging, which will help assist in more rapid production and deployment of EVs. While some automakers have previously urged the FCC to adopt power limits to accommodate high-power wireless power transfer systems for EV charging in the 79-90 kHz band, there is still no spectrum provided for such wireless EV charging. Providing spectrum for wireless charging will boost the EV market and move the automotive industry towards a cleaner and more sustainable future. In addition, it is crucial that the automotive industry maintain dedicated spectrum for both 60 GHz radar and obtain spectrum for ultra-wideband-enabled safety features that currently utilize unlicensed frequencies. For example, mobile automotive radar use of the 60 GHz band will help the industry deploy technology that monitors for children inadvertently left in cars, seatbelt reminders, air bag deployment control, gesture control, and even anti-theft technology. Moreover, freeing up ultra-wideband spectrum for a variety of automotive use cases will help unleash a new wave of automotive innovation and take further steps towards smarter, safer cars.

  As the Federal Working Group continues its work in this area, it is important that it account for both the lengthy and complex production cycle that automotive companies and their suppliers undergo to deliver new vehicles and technologies to market, as well as the fact that the vehicles themselves are on the road for far longer than a conventional consumer

electronic device is in use. It typically takes several years to bring new technology to market in a production vehicle, and up to ten years to phase in the technology across the entire product portfolio. The same is not true of a wireless router, cellphone, or other wireless device, all of which are updated on a nearly annual basis. Additionally, vehicles are on the road far longer than a mobile device is in use. According to a 2022 study by S&P Global Mobility, the average lifespan of a car in the U.S. is 12.2 years. New connected technologies cannot be integrated into vehicles and delivered to consumers overnight. Rather, new technologies must be able to rely on a reasonably foreseeable spectrum environment given elongated production cycles, and the reality that many such connected technologies will be used in the same vehicle for ten years or more.

MECHANISMS FOR SUPPORTING IoT PILLAR ADOPTION

Auto Innovators is also generally supportive of the mechanisms for supporting IoT pillar adoption identified in the report. Based on the current regulatory environment for automotive IoT, we are particularly enthusiastic about efforts to advance the federal guidance/policy mechanism. There are three specific areas where federal guidance/policy is particularly urgent in advancing automotive IoT innovation. These include:

- **AUTONOMOUS VEHICLES:** The ability of the U.S. to preserve its leadership in autonomous vehicle (AV) technology is in jeopardy due to the lack of a clear federal regulatory approach and framework that supports U.S.-based AV deployment at scale. To maintain the global competitiveness of the auto industry, the federal government must actively support and promote AV development and commercialization in the U.S. This includes rapidly accelerating efforts at the U.S. Department of Transportation to update existing motor vehicle safety standards to accommodate AVs, using its existing authority to grant targeted exemptions to AV developers that have demonstrated safety equivalence, and implementing the innovative AV STEP program announced earlier this year to provide an enhanced deployment pathway for AVs in the near-term. In addition, federal policymakers must expeditiously implement the remaining recommendations included in the AV Policy Roadmap that Auto Innovators released in December of 2020.

- **V2X:** A key reason that wide-scale deployment of V2X has not yet occurred in the U.S. is regulatory uncertainty. Although important progress has taken place in recent months, the auto industry and other V2X stakeholders, including state departments of transportation, continue to wait for final technical V2X rules from the FCC and a comprehensive national V2X vision and strategy from the US Department of Transportation. These important steps, as well as other recommendations contained within Auto Innovators' V2X Policy Agenda, are necessary for the industry to realize the full potential of V2X technology.

- **FEDERAL PRIVACY:** Auto Innovators recognizes that the best way to protect consumer privacy is through a single, national privacy law that provides consistent protections to consumers across the U.S. In recent years, a number of states have enacted state-level privacy regulations which create diverse and – in some cases – inconsistent requirements.

This emerging patchwork of state laws is particularly challenging for automakers that have customers in every state and produce a product that regularly crosses state lines. A patchwork of state privacy laws creates confusion among consumers about their privacy rights and makes compliance unnecessarily difficult. It also creates situations where state privacy laws may conflict with federal requirements or policy objectives. A federal privacy law will provide uniformity and consistent protections to consumers across the U.S., while also simplifying compliance for companies that operate in multiple states.

Auto Innovators welcomes the opportunity to provide the perspective of the auto industry on the Preliminary Update. We look forward to continuing to work with the Federal Working Group as it continues its work to advance social and economic prosperity through improved adoption of IoT technology.

Sincerely.

Hilary M. Cain
Vice President
Technology, Innovation, and Mobility Policy