June 17, 2021

SUBMITTED ELECTRONICALLY VIA REGULATIONS.GOV

Ms. Evelyn L. Remaley
Acting Administrator
National Telecommunications and Information Administration
Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington D.C. 20230

Re: National Telecommunications and Information Administration Request for Information on Software Bill of Materials Elements and Considerations, Docket No. 210527-0117, 86 Fed. Reg. 29568 (June 2, 2021)

Acting Administrator Remaley:

The Alliance for Automotive Innovation ("Auto Innovators")[1] appreciates this opportunity to provide input to the National Telecommunications and Information Administration (NTIA) in response to its request for comments on the elements and considerations for a Software Bill of Materials (SBOM), pursuant to the directive to the Department of Commerce, in coordination with NTIA, 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 38 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, in addition to those who are employed in the technology and mobility sectors directly. We account for nearly 6 percent of our country's gross domestic product and represent our country's largest manufacturing sector.

[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, APTIV, Argo AI, BMW Group, Bosch, Byton, Cruise, DENSO, Ferrari, Ford, GM, HARMAN, Honda, Hyundai, Infineon, Intel, Isuzu, Jaguar Land Rover, Karma, Kia, Local Motors, 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.

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.

As physical machines evolve into increasingly software-dependent and connected platforms, technology is reshaping the relationship between vehicles and their users. In the past, the main, or only, external input for a vehicle was the driver or occupants of the vehicle. That is no longer the case. 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, 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.

Cybersecurity is crucial to realizing the safety, privacy, environmental and societal benefits of vehicles with advanced technologies. The automotive industry understands the realities of a connected world and takes cybersecurity risks seriously. The automotive industry has been working proactively and collaboratively to build cybersecurity into the products and services that will define the future of transportation.

Supply chain management is a critical element of the automotive industry. This industry operates some the most complex and expansive supply chains of any sector of the economy, and for good reason. Motor vehicles are incredibly complex machines. A single vehicle brings together more than 10,000 parts, that must all work in concert – safely, efficiently, and reliably - in harsh environmental conditions, often for the useful life of the vehicle, at a price that is affordable to consumers.

As technology evolves, so too have the industry's supply chains. As software has become integral to the future of motor vehicles, the industry recognizes the importance and benefits of establishing an appropriate level of visibility and awareness of the software, and associated supply chains. This will assist automakers, suppliers, and other stakeholders in the supply chain when it comes to the identification, mitigation, and, as necessary, remediation of software vulnerabilities throughout the lifecycle of the vehicle. This becomes increasingly relevant as vehicles become more connected.

Auto Innovators offers the following recommendations to NTIA on elements and factors for an SBOM:

- **Leverage Industry Collaboration:** Earlier this year, the members of the auto industry, building on the work of the healthcare sector, began developing an SBOM proof of concept for the auto

industry. This work is being led by the Suppliers Working Group at the Auto-ISAC, in collaboration with NTIA and other stakeholders. The goal is to develop an auto-specific model for SBOM, including implementation, that is tested and refined over the coming year to achieve full industry agreement.[2] These industry-led efforts should be supported and leveraged by NTIA. To that end, the auto industry appreciates NTIA's support on this endeavor and looks forward to continued collaboration.

- **Account for Sector-Specific Variations:** We encourage NTIA to carefully consider how implementation of an SBOM across different industry sectors or verticals may have different implications or require different approaches. NTIA should continue to support and facilitate efforts that examine different sector use cases and models. We believe these ongoing efforts by the auto industry and other sectors will provide valuable insights into how core elements of an SBOM are best and most effectively implemented in different sectors. In addition, NTIA should enable an adaptable approach to support the unique challenges associated with the automotive industry, including cyber-physical systems that have a diverse supply base. For example, there needs to be flexibility in the assignment of responsibility across multiple entities in a way that preserves confidentiality and intellectual property, but also provides sufficient detail to manage system-level risk.

- **Consider Implications of SBOM Communication and Disclosure:** We encourage NTIA – and the administration – to carefully examine the implications of how an SBOM, including the ingredient and/or vulnerability list, is communicated or shared. For example, a product may contain a component with a known vulnerability, but that vulnerability is not exploitable due to countermeasures or other factors. Public communication or disclosure of "vulnerabilities" without this additional and important context risks unnecessarily undermining public confidence. In addition, the structure of any SBOM should take into consideration the risk benefit or level of detail necessary to achieve the objective of the SBOM without unintentionally impacting the analysis of software structure, attack path or other opportunities for compromise or unnecessarily stifling innovation.

- **Establish Definitions that Provide Clarity on Scope and Expectations:** We urge NTIA to consider incorporating definitions that provide clarity on scope and clearly outline expectations for an SBOM. For example, NTIA could clarify that an SBOM is a subset of a general Bill of Materials, focusing on software elements, for use in supply chain management and that the

[2] https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_energy_automotive.pdf

purpose of an SBOM is to foster efficiency and accuracy in traceability activities supporting risk analysis, vulnerability management, and the remediation processes.

Conclusion

In the pantheon of tools necessary to keep pace with the dynamic nature of cyber threats, the auto industry sees significant promise in the concept of a SBOM. We look forward to continuing to work with NTIA and other stakeholders on this important issue.

Sincerely,

John Ohly
Senior Director, Strategy, Advocacy, and Technology Policy
Alliance for Automotive Innovation