Autos Drive America®
Jobs. Trade. Growth.

April 30, 2024

Ms. Elizabeth L.D. Cannon
Executive Director
Office of Information and Communications Technology and Services
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Re: ***Docket No. BIS–2024–0005, "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles"***

Dear Executive Director Cannon:

Autos Drive America writes in response to the Bureau of Industry and Security's ("BIS") call for public comment on the *Securing the Information and Communications Technology and Services Supply Chain: Connected Car Advance Notice of Proposed Rulemaking* (the "ANPRM"). The ANPRM seeks public comment on issues and questions related to transactions involving connected vehicle information and communications technology and services ("ICTS") that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries.

Autos Drive America represents 12 international automakers that have made America their home, investing over $107 billion into their American operations, directly employing over 156,000 Americans, and supporting an additional 2.3 million jobs. The association's members operate 75 research and development facilities and support innovation all throughout the supply chain. Over the last two years, international automakers have committed over $25 billion toward their electrification efforts, which include additional resources committed to R&D toward advanced vehicles, with more investments expected.

While each of the association's members approach the advancement of the automotive industry differently, each plays an important role in the U.S. automotive market. As consumer preferences and technological capabilities advance, Autos Drive America's members will be here providing industry-leading vehicles that increase road safety, contribute to environmental sustainability, and provide options to a diverse array of consumers. These companies support the country's need for both a U.S. manufacturing workforce and skilled research and development careers.

Autos Drive America's members are developing various levels of connected vehicle platforms, and cybersecurity and the integrity of the ecosystem is of the utmost importance to each of them. As BIS has recognized in its ANPRM, many technological interfaces and data play key roles in the systems required to enable the functionality of connected vehicles. Information is collected through numerous sensors, processed in internal vehicle networks, and can, in some cases, be made available to other road traffic components, which can react accordingly. This data is also transmitted from the vehicle to the auto manufacturer. To prevent data leakage, manipulation, and technical failures—while simultaneously meeting customer demands for

801 Pennsylvania Ave, NW, Ste 620
Washington, DC 20004

AutosDriveAmerica.org

increased connectivity and functionality in the digital age—it is necessary to protect the relevant vehicle functions with security measures, including applying cybersecurity, encryption and other data protection efforts.

Therefore, Autos Drive America urges that BIS focus its efforts on working with the industry to ensure that automakers and their supply chains apply appropriate security concepts or standards that offer comprehensive protection for vehicles and the systems that data can be extracted from, whether through software or hardware security. As vehicles increasingly rely on digital capabilities, efforts to provide cybersecurity and risk mitigation are top priorities for the association's members, regardless of the origins of the vehicles' components and ICTS.

It is critical that the United States and its allies remain leaders in advanced and connected vehicle technologies. Maintaining such leadership requires continued access to cutting-edge systems and the best technologies from all over the world, as well as continued investment in the United States' educational and technical training, manufacturing/industrial, and research and development capacity.

As automotive development cycles typically span 5–7-years, any transition in the existing ICTS supply chain will require supplier qualification and supply chain shift that will take significant time to complete. The same is true for new or proposed projects under development as they may require a revision and re-focus to a future supplier-base.

To avoid disruption in the U.S. automotive marketplace and to provide the necessary development time for ICTS systems in future products, first and foremost, development and deployment of cutting-edge standards and best practices for risk mitigation must continue. In the event risks will not be adequately minimized through standards, then any proposed transition in the ICTS supply chain must be constructed with the industry to create appropriate lead-times and phase-out schedules to appropriately analyze any concerns, and subsequently, to develop and deploy an alternative supply chain that meets all relevant regulations.

BIS should work with the industry to develop new ways in which automakers can demonstrate their adherence to cybersecurity and how cyberthreats may be appropriately mitigated without the need for a complete supply chain overhaul that may set back U.S. leadership in advanced vehicle technologies.

One option that BIS should consider is a program modeled after the Customs Trade Partnership Against Terrorism ("CTPAT") Trade Compliance Program. CTPAT Trade Compliance is a voluntary U.S. Customs and Border Protection ("CBP") program for U.S. importers who have made a substantial commitment of resources to assume responsibility for monitoring their own adherence to expansive customs and other trade regulatory requirements in exchange for certain benefits. Membership in the CTPAT Trade Compliance program requires meeting various rigorous eligibility criteria, as well as the provision of extensive documentation to CBP. Autos Drive America's member companies are active members of CTPAT and are familiar with its requirements and processes, which would in part reduce the compliance learning curves associated with this type of certification process.

Such a program would provide an objective and clear pathway for trusted automotive partners to maintain ongoing commerce and operations in the United States as BIS implements appropriate cybersecurity risk mitigation measures. The program would also facilitate ongoing

collaboration between the automotive industry and BIS as connected vehicle technologies develop.

Another ongoing forum where BIS may find valuable discussion, information, and best practices is the Automotive Information Sharing and Analysis Center (Auto-ISAC). This group is an "industry-driven community to share and analyze intelligence about emerging cybersecurity risks to the vehicle, and to collectively enhance vehicle cybersecurity capabilities across the global automotive industry, including light- and heavy-duty vehicle OEMs, suppliers and the commercial vehicle sector."[1]

BIS should also consider the benefits of the adoption of global standards, like UN Regulation No. 155 on Cyber Security and Cyber Security Management Systems and UN Regulation No. 156 on Software Updates and Software Updates Management Systems. These standards are applicable in the European Union and Japan and are important to ensuring vehicle data and cyber security.

Response to Questions 9 and 10

The automotive supply chain, including the supply chain for ICTS, consists of multiple tiers, each with numerous potential suppliers for hardware components that service automotive manufacturing operations in the U.S. and global markets.

Autos Drive America's members are already beginning to restructure supply chains away from foreign entities of concern, but these changes cannot happen overnight. As with many of the structural components, selecting and testing connected vehicle components requires multiple years to source and qualify suppliers—in part due to numerous regulatory and safety requirements across the jurisdictions in which international automakers operate—such that alternatives to existing suppliers are difficult to integrate in a short timeframe.

Moreover, given the complexity and variety of the technologies involved, no automotive manufacturer will be able to own and maintain complete software stacks, and therefore the required ECUs and semiconductors, by itself. Should re-designs be required as a result of a proposed rulemaking, changing currently existing components and semiconductors retroactively would require substantial time and investments to ensure full compliance with any proposed rules. Importantly, such changes could affect not only new vehicle projects, but also ongoing support for legacy vehicle models, significantly expanding the potential expense.

Response to Questions 27-30

As previously mentioned, Autos Drive America recommends that BIS work with the automotive industry to create a program that allows automakers to verify their supply chains using a trusted-trader-like program to support connected vehicle cybersecurity. As previously mentioned, using the CTPAT Trade Compliance Program as a model may help to avoid disruptions while making sure that automakers and their suppliers are using acceptable standards.

[1] https://automotiveisac.com/.

CTPAT Trade Compliance is a voluntary program for U.S. importers who have made a substantial commitment of resources to assume responsibility for monitoring their own customs with regulatory trade requirements imposed by CBP and other agencies. To qualify for CTPAT Trade Compliance membership, U.S. importers must meet specific eligibility criteria, complete a detailed application and trade compliance questionnaire supported by extensive documentation, and commit to continuing responsibilities and annual updates.

Such a program will be focused on the needs of U.S.-based vehicle OEMs and/or suppliers who are active in the U.S. market. A trusted-trader-like program will provide an objective and clear pathway for trusted automotive partners to maintain ongoing operations in the U.S. as BIS implements its rulemaking.

Response to Questions 31-33:

Any wholesale ban against ICTS with foreign adversary touch points would require substantial efforts and resources for the U.S.-based automotive industry. Given the global nature of automotive supply chains, it would be exceedingly difficult for OEMs to fully ensure the absence of any foreign adversary-based suppliers in all ICTS parts or components. This includes costs associated with vetting and contracting with new suppliers, but also costs associated with higher-cost components, availability of supply, and, in some cases, ensuring equivalent quality and functionality. Rising costs will ultimately have an impact on vehicle prices and as such be detrimental for the U.S. customer. In a worst-case scenario, customers will face both higher prices and restrictions on choice and quality.

Also, the competitive positioning of a manufacturer using lower-quality or performing components vis-à-vis other auto manufacturers—particularly those that will maintain access to the higher quality or better-performing component—may be impacted. In this way, BIS must take care to ensure that any policy approach enables the continued competitiveness of the U.S. automotive industry against competitors who remain able to access parts and technologies that may have foreign adversary touchpoints. At the same time, the economic competitiveness of the auto industry in the U.S. will be harmed if connected vehicles that are heavily subsidized by foreign adversaries are sold at below-market prices to U.S. consumers.

Response to Question 34:

Autos Drive America recommends that BIS work closely with the automotive industry to strike the right policy balance on the complex and urgent issue of foreign adversaries in ICTS. In particular, the prioritization, scope, and timing of any regulation—while avoiding unintended consequences that may inadvertently harm the U.S. industry and its competitiveness or limit the availability of advanced automotive technologies—is critical.

To the extent that ICTS systems from persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary are integral to vehicles, we recommend that BIS work with the automotive industry to develop best practices and standards that mitigate risk. BIS should also provide sufficient lead time to automotive manufacturers to enable the development and procurement of alternative sources that can be integrated into the existing and future architectures. Without sufficient lead-time, manufacturers would be unable to keep their production lines active, and vehicle sales could even be stopped immediately depending on the

scope of potential restrictions. This could cause widespread financial impact, prompt consumer claims, and engender consumer distrust against the entire automotive industry.

Conclusion

Autos Drive America recommends that as BIS and the Department of Commerce works with the automotive industry to develop effective ICTS system security standards that the U.S. government as a whole supports policies that ensure that alternative ICTS automotive supply chains are available to U.S.-based vehicle OEMs and suppliers. These policies should include trade agreements with allies and trusted partners, reducing technical barriers to trade, and incentivizing the establishment of supply chains domestically and with trusted partners to provide technologically competitive products.

As part of the response to the threat outlined in this ANPRM, the United States should work to bring together allies and partners to institute a coordinated response that will effectively counter the national security threats that may be posed by the ICTS systems. Autos Drive America looks forward to engaging with BIS on this proposed rule in the future.

Sincerely,

Jennifer M. Safavian
President and CEO
Autos Drive America