1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

October 28, 2024

BY ELECTRONIC SUBMISSION

Elizabeth L.D. Cannon
Executive Director
Office of Information and Communications Technology and Services
1401 Constitution Ave. NW
Washington, DC 20230

Re: Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles
Docket No. 240919-0245

Dear Executive Director Cannon:

The Consumer Technology Association (CTA) appreciates the opportunity to submit the following comments in response to the Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles Notice of Proposed Rulemaking (NPRM) issued by the U.S. Department of Commerce (Department) Bureau of Industry and Security (BIS or Agency). BIS is soliciting public comment on its proposed rule to prohibit information and communications technology and services (ICTS) transactions that involve certain software and hardware designed, developed, manufactured, or supplied by persons owned, controlled, or subject to the jurisdiction or direction of the People's Republic of China (PRC) or the Russian Federation (Russia).[1]

CTA is North America's largest technology trade association and represents the $505 billion U.S. consumer technology industry, which supports more than 18 million U.S. jobs. Members of CTA are diverse and include companies at the forefront of vehicle technology, including vehicle and component manufacturers, software developers, transportation platforms, and companies engaged in a multidisciplinary approach within this evolving industry. As the trade association representing American and Canadian technology companies, including makers and suppliers of vehicles and their components, and led almost entirely by U.S. citizens and composed solely of U.S. and Canadian companies, CTA is well positioned to comment on these issues and supports the evident goal of this rulemaking: to ensure Americans are protected from attempts by Russia and China to harm American citizens using connected vehicles. This worthy goal led President Trump to sign E.O. 13873, "Securing the Information and Communications Technology and Services Supply Chain," to delegate to the Secretary of

[1] Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 89 Fed. Reg. 79088 (Sept. 26, 2024) ("Notice").

Commerce the authorities granted under the Emergency Economic Powers Act (IEEPA) "to deal with any unusual and extraordinary" foreign threat.[2] To use emergency powers under the IEEPA to deal with a threat, a new declaration of national emergency must be made.

CTA appreciates the serious and vital work of this rulemaking to address undue or unacceptable risks associated with the inclusion in connected vehicles of certain ICTS associated with persons owned, controlled, or subject to the jurisdiction of certain foreign adversaries. We recognize BIS staff's efforts to quickly, diligently, and carefully seek facts to develop this proposed rule, which is thoughtful, comprehensive, and important. However, CTA believes the rule can be refined and clarified to provide a smoother transition that reflects industry economic realities and American consumer desires to keep and maintain existing vehicles. In issuing final rules using notice and comment rulemaking,[3] the Department of Commerce must consider not only the rule's primary goal in the context of its granting authority, but also must consider and respond to significant comments received during the period for public comment.[4] We appreciate the continued efforts of BIS to incorporate these serious comments.

At the outset, CTA agrees that no government role is more important than national security. Part of our national security requires a growing economy, strong automotive industry, and robust and competitive transportation infrastructure. With rapid changes in technology, including electric vehicles and self-driving cars, the U.S. is in a global economic competition with other nations. This competition will likely determine our national economic success, which directly affects the U.S.'s ability to fund and maintain a strong national security and defense apparatus.

The U.S. auto industry is important to Americans on many levels. In 2021, Americans bought some 11.8 million new vehicles. The U.S. automotive industry employed over 4.3 million people in 2023, employing nearly 2.1% of the U.S. working age population.[5][6] The automotive industry is so central to the U.S. economy that Congress has repeatedly acted to maintain its strength as a national priority. In doing so, Congress and the Executive Branch have also made automotive safety and security a priority. E.O. 13873 seeks to support these objectives by minimizing the risk that Russia or China can gather information from, control, or harm occupants of connected cars or other road users. We support this.

To this end, CTA's comments focus on: (1) adjusting the compliance timelines for covered hardware and software to align with industry capabilities; (2) cost estimates for compliance; (3) submission of confidential business information; (4) clarifying definitions used in the NPRM; (5) improving the process and requirements for Declarations of Conformity; and (6)

---

[2] Exec. Order No. 13873, 84 Fed. Reg. 22689 (2019); 50 U.S.C. 1701, et seq.
[3] 5 U.S.C. § 553.
[4] See *Citizens to Pres. Overton Park, Inc. v. Volpe,* 401 U.S. 402, 416 (1971); *United States v. Nova Scotia Food Prod. Corp.*, 568 F.2d 240, 252 (2d Cir. 1977) (finding agencies must respond to all well supported comments which are of "cogent materiality").
[5] *See* BUREAU OF LABOR STATISTICS, AUTOMOTIVE INDUSTRY: EMPLOYMENT, EARNINGS, AND HOURS, https://www.bls.gov/iag/tgs/iagauto.htm.
6 SEE FEDERAL RESERVE ECONOMIC DATA, INFRA-ANNUAL LABOR STATISTICS: WORKING-AGE POPULATION TOTAL: FROM 15 TO 64 YEARS FOR UNITED STATES, HTTPS://FRED.STLOUISFED.ORG/SERIES/LFWA64TTUSM647S

expanding authorizations and advisory opinions to support U.S. manufacturing and to mitigate disruptions to supply chains.

CTA's specific modifications to the proposed rule are as follows:

I. Implementation Timeline

CTA recognizes the urgency of these issues and considers matters of national security a priority. The concerns that are the focus of this rulemaking are shared by connected vehicle manufacturers and Vehicle Connectivity System (VCS) hardware importers.

In its NPRM, BIS proposes making requirements for VCS hardware importers effective for all VCS hardware associated with a vehicle model year of 2030 or later. This imposes a four-year timeline that may not offer some VCS hardware importers enough time to vet their current supply chains and, if necessary, identify and source reasonable alternatives while remaining competitive in the global connected vehicle industry.[7] BIS also proposes applying prohibitions on the import or sale of completed connected vehicles that incorporate covered software starting with transactions associated with Model Year 2027. This provides a one-year timeline that may not offer some VCS software stakeholders enough time to transition.[8]

The final rule should consider the practical realities that connected vehicle importers and VCS hardware developers face, and acknowledge potential risks related to security validation and development that a quick transition might create or exacerbate. The time required for the industry to develop, test, certify, release, and validate covered hardware and software is long, between five and seven years for some industry participants.

Software product development is a lengthy process that begins at least five years prior to the Model Year production. Further, Model Years begin to roll off the production lines up to six months before the calendar year starts. For example, Model Year 2027 production will begin in mid-2026 and affected companies are already three years into the development of technology. In many cases, contracts and system requirements have already been established. Not only would regulated companies have to potentially break their contracts to comply with the proposed timeline, which is costly and damaging to business relationships, but they would now also have to undertake identifying and qualifying new suppliers, which will take time.

For these reasons, CTA respectfully recommends BIS extend these timelines from one to three years for software, and from four to six years for hardware, as these timelines would be better aligned with the realities of automotive manufacturing.

II. Cost Estimates

CTA respectfully asks that BIS revisit its proposed cost estimates. BIS assesses that there are 42 to 281 entities potentially impacted by the proposed rule and that the initial cost burden for these entities is between $30,964 and $38,554.[9]

Based on industry stakeholders' knowledge of their own supply chains and the complex steps involved in the development, re-design, testing, regulatory carrier certifications, import,

[7] Notice at 79120.
[8] *Id.*
[9] Notice at 79113.

and sale of covered software and VCS hardware, as well as the due diligence requirements imposed upon companies using even domestic sources, CTA finds it likely that these cost estimates are dramatically understated. Anecdotal reports from industry experts expect a mid-six-digit to low-seven-digit cost burden.

BIS's cost assessment fails to consider potential unintended downstream impact. The Department has stated that the proposed rule is drafted to "address the national security risks posed by Connected Vehicles" and that it seeks to strike a balance by "focusing the rule only on those systems that most directly facilitate the transmission of data both into and from the vehicle." This statement fails to address the relationship between these systems and the broader mobile wireless ecosystem. The technology that comprises automotive connectivity systems is not unique or exclusive to connected vehicles. Instead, the proposed rule could unintentionally sweep in a broad range of wireless technologies that are essential to connected vehicles but were not originally designed for automotive applications. The proposed rule therefore fails to consider the unintended downstream impact on the importation of other wireless connectivity technologies, regardless of the industry or end-use in which they are used.

It is impossible to estimate to an accurate amount the true cost-impact this rulemaking would have in the 30-day window of this comment period. At a minimum, BIS must revisit its assumptions about the likely reach of this NPRM to reasonably and fully consider the costs it would impose.

III. Confidential Business Information

CTA acknowledges that a certain level of confidential business information sharing is required for BIS to adequately assess and mitigate national security risks identified in the NPRM. To assist companies in preparing to disclose the necessary information to comply with Declarations of Conformity and/or apply for a Special Authorization, BIS should provide detailed information about how it will give certainty to companies sharing extremely confidential and proprietary intellectual, product, or supply chain data. Gathering the valuable information BIS requests in this rulemaking in a single location risks creating a highly valuable and nationally sensitive target that could enhance—rather than reduce—the national security risks that BIS intends to address through this rule. BIS should explain how it will ensure that such data will not be shared or made publicly available and will be protected from incidental or malicious data breaches. Further, BIS should identify how suppliers' specific confidential business information will be protected in the reporting process from other companies in the interconnected supply chain.

CTA recommends BIS align and exchange information with its own Department of Commerce (DOC), as well as the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), Environmental Protection Agency (EPA), Federal Trade Commission (FTC), and other relevant agencies on best practices concerning information sharing, data protection, and preventing duplicative burdens across government and industry.

Regarding FOIA requests specifically, the U.S. Customs and Border Protection (CBP) issued Directive 2120-010A, which provides guidance for the agency and its personnel to withhold information falling under the categories that include, but are not limited to, trade secrets and confidential commercial information.[10] CTA encourages BIS to refer to these directives and

[10] U.S. CUSTOMS AND BORDER PROTECTION, DIRECTIVE 2120-010A, PRIVACY POLICY, COMPLIANCE, AND IMPLEMENTATION (June 29, 2022).

other similar directives to ensure that the highest level of confidentiality possible is preserved in the U.S. commercial space.

IV. Definitions

The definitions included in the proposed rule require additional detail to prevent confusion, clarify the standards with which regulated entities must conform, and facilitate compliance.

- **Knowingly.** BIS proposes to prohibit certain transactions in which the regulated entity "knowingly" imports or sells a restricted item.[11] The intent threshold ("knowingly") includes "an awareness of a high probability of its existence or future occurrence." It is unclear how far down the supply chain an entity is expected to determine if an imported VCS contains a prohibited component, such as to Tier 2 or 3 suppliers. Further, BIS should provide clarification as to how this threshold applies to regulated entities who rely on foreign automotive suppliers. To resolve these ambiguities, BIS should consider establishing an approved vendor list that contains foreign VCS hardware vendors from which a U.S. entity can import from without the need for additional compliance requirements.

- **Designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.** BIS proposes to define the scope of prohibited transactions as applying to VCS hardware and covered software that is, "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia."[12] Relatedly, BIS proposes to define the phrase "persons owned by, controlled by, or subject to the jurisdiction of a foreign adversary" as including any person, corporation, partnership, association or other organization that is "owned or controlled by" a foreign adversary.[13] Consistent in both of these definitions is the language "owned or controlled by," which may be subject to multiple interpretations.

  This language can be made more precise by incorporating criteria from the Department of Justice's advanced notice of proposed rulemaking, "National Security Division; Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern." Specifically:

  > Persons who are owned by, controlled by, or subject to the jurisdiction or direction of a country of concern may enable the government of that country to indirectly access such data. For example, countries of concern may have cyber, national security, and intelligence laws that, without sufficient legal safeguards, can obligate such persons to provide that country's intelligence services access to U.S. persons' bulk sensitive personal data and government-related data.[14]

  Further, BIS should provide clarification or examples on how the actions "designed, developed, manufactured, or supplied by" apply in the context of hardware or covered software development in the global automotive supply chain where multiple entities may

[11] Notice at 79117.
[12] *Id.*
[13] Notice at 79116.
[14] 89 Fed. Reg. 15780 (March 5, 2024) at 15781.

play a role in the design, development, or production from the initial conception to sale or import. BIS should also consider providing examples to clarify the difference between "design" and "development."

CTA also recommends BIS add specific language that clarifies when a person or business is considered to be "controlled by" a foreign entity.

- **Country of citizenship.** The proposal suggests a natural person who is a citizen of China or Russia and who "is not a U.S. citizen or permanent resident of the U.S." is a person controlled by a foreign adversary.[15] BIS should alter this language such that Chinese nationals who are authorized through an established U.S. visa program (e.g., H-1B), are not considered foreign adversaries.

- **U.S. person.** BIS defines "VCS hardware importer" and "connected vehicle manufacturer" by reference to "a U.S. person" but does not define this term.[16] For added clarity, CTA recommends that BIS use the definition of "U.S. person" in the Export Administration Regulations ("EAR"), which includes "protected individuals." "Protected individuals" are individuals who are U.S. citizens, U.S. nationals, lawful permanent residents, asylees and refugees as defined by 8 U.S.C. § 1324b (a)(3).[17]

- **Foreign interest.** CTA generally supports BIS's proposal not to require a Declaration of Conformity for the sale of completed connected vehicles manufactured in the United States when there is no foreign interest in the covered software. However, BIS proposes to define "foreign interest" as "any interest in property of any nature whatsoever, whether direct or indirect, by a non-U.S. person."[18] For clarity, we recommend that BIS add the examples included in the supplementary information section as illustrative examples of "foreign interest" in the regulation itself. Namely "an interest through ownership, intellectual property, contract, . . . profit-sharing or fee arrangement," all of which are legally cognizable interests. Further, the foreign interest qualifier should be added to the definition of VCS hardware for consistency, given that the prohibitions on hardware will be implemented for the same national security-based reasons as the prohibitions on covered software.

  The scope of "foreign interest" should be narrowed to allow for a person in an allied country to be treated the same as a U.S. citizen because these individuals are unlikely to pose the type of threats this rulemaking aims to mitigate. The definition of an allied country is best defined as the group of countries listed as "Country Group A" within the Export Administration Regulations.[19]

  CTA emphasizes that it is in the U.S. interest for U.S. companies and companies headquartered in close democratic allies to lead global auto markets. This leadership sustains innovation, and it drives adoption of trusted technology and trusted technology standards. If we retreat, these standards and markets will be led by others who do not share our values or commitment to customers.

[15] Notice at 79104.
[16] Notice at 79116.
[17] 22 C.F.R. § 120.62.
[18] Notice at 79116.
[19] Supplement No. 1 to Part 740, Title 15.

- **Connected vehicle.** CTA recommends that BIS modify its definition of "connected vehicle" to better reflect vehicles that are exempt from the regulation. CTA suggests the following language be added, as indicated by italics:

> *Connected vehicle* means a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways, that integrates onboard networked hardware with automotive software systems to communicate via dedicated short-range communication, cellular telecommunications connectivity, satellite communication, or other wireless spectrum connectivity with any other network or device. Vehicles operated only on a rail line*, as well as other vehicles not manufactured primarily for use on public streets, roads, and highways such as agricultural, construction, and mining vehicles, are not included in this definition*.

  This change would support BIS's expressed intent that the proposed rule would exclude vehicles "not used on public roads like agricultural or mining vehicles."[20] Further, the NPRM stipulates that on-road vehicles driven by mechanical power are within the scope of this rule.[21] BIS should clarify that this scope does not include micromobility devices such as bicycles, which can also be considered connected vehicles if propelled by mechanical power and driven on roadways.

- **Automated Driving Systems (ADS).** CTA appreciates that BIS's definition of ADS "corresponds to automation levels 3, 4, and 5 as defined by SAE International Standard J3016."[22] The SAE Standard J3016 is widely accepted by industry stakeholders and accurately describes the range of autonomy levels in existence. For added clarity and consistency with industry's understanding of what ADS is, CTA recommends that BIS directly reference J3016 in its definition for ADS and clarify within the definition the applicable levels to which this regulation is intended to apply.

- **Vehicle Connectivity System (VCS).** BIS proposes defining VCS as hardware or software with transmission, receipt, conversion, or processing capabilities at frequencies over 450 megahertz. CTA recommends that the frequency range be limited to 450 to 7125 megahertz.

  CTA is generally appreciative of BIS's emphasis on connectivity when defining which technologies are within the scope of this rulemaking.[23] CTA is thus supportive of BIS's decision to focus on systems with a higher risk of connectivity and transmission functions, and to exclude systems such as Operating Systems (OS), Advanced Driver Assistance Systems (ADAS), or Battery Management Systems (BMS) unless they specifically contain VCS components.[24] However, the current definition of VCS may still

---

[20] *Commerce Announces Proposed Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats*, DEPT. OF COMMERCE (Sept. 23, 2024), https://www.bis.gov/press-release/commerce-announces-proposed-rule-secure-connected-vehicle-supply-chains-foreign#:~:text=Washington%2C%20D.C.%20%E2%80%93%20Today%2C%20the,sold%20separately%2C%20with%20a%20sufficient.

[21] Notice at 79116.

[22] Notice at 79102.

[23] Notice at 79092.

[24] *Id.*

be overly broad and extends beyond the two-way communication systems described in the ANPRM.

The NPRM seeks to focus "the rule only on those systems that most directly facilitate the transmission of data *both* into *and* from the vehicle."[25] In support of BIS's emphasis on the importance of connectivity capability, CTA respectfully recommends that BIS further clarify its definition of VCS to exclude systems that are connected internally to the vehicle, but which are not capable of communication beyond the vehicle regardless of their connectivity to a system with external communication capabilities. Another consideration would be to exclude VCS hardware, like Bluetooth, used solely to connect a vehicle occupant's devices to infotainment systems. Infotainment systems are largely contained within their own ecosystem in the vehicle, and the ability to connect a mobile device, gaming controller, headphones, or other Bluetooth-enabled device brought into the vehicle by the occupant does not represent a national security risk that necessitates a covered use for purposes of this regulation.

In addition, BIS should focus the definition of VCS on Transmission Control Unit (TCU) components rather than specific or single parts, to avoid encompassing replacement parts in its definition. If replacement parts were covered by this definition, it would have a substantial impact on cost and technical changes for vehicles already in the market. For example, should a particular replacement part not be allowed to be imported, a used vehicle owner would not be able to repair the vehicle, causing harm to the consumer who owned the vehicle prior to any ban being imposed. CTA urges BIS to consider these potential impacts when reassessing the proposed rule's attendant costs. To prevent these additional burdens, BIS should consider grandfathering in a legacy fleet that can be, "repaired as produced."

- **VCS hardware.** BIS proposes to define VCS hardware as "software-enabled or programmable components and subcomponents" that support the function of VCS.[26] This definition is expansive and may create compliance difficulties in several areas. CTA respectfully makes the following recommendations:

    - **BIS should remove the language "that supports" from the definition of VCS hardware.** The phrase "that supports the function of VCS" is broad and could capture a range of technology that BIS has indicated it does not intend to regulate in this rulemaking, such as vehicle charging systems and infotainment systems. CTA suggests striking "that supports" and replacing it with "that directly enables." Without this clarifying language, this ambiguity could effectively sweep in a broad scope of software-based components, thereby creating additional supply chain disruptions that would negatively impact the U.S. automotive industry in a manner not intended by the proposed rule.

    - **Satellite navigation systems should be excluded from the definition of VCS hardware.** The NPRM states that "BIS proposes to achieve this balance by focusing the rule only on those systems that most directly facilitate the transmission of data both into and from the vehicle, rather than focusing on all systems." However, the definition of VCS hardware includes satellite navigation systems. As Global Navigation Satellite System (GNSS) receivers do not

[25] *See* Notice at 79092 (emphasis added).
[26] Notice at 79117.

transmit information and simply receive information that is not directly used to control the vehicle, we believe they should be excluded from the rule. This would make the treatment of GNSS consistent with the treatment of LiDAR within the NPRM: “BIS's further technical analysis found that LiDAR generally lacks the ability to transmit from the vehicle and does not, as a standalone system, control the vehicle.”

- **Radar systems.** Similarly, radar systems should be excluded from the definition of VCS hardware for similar reasons. Radar systems do not transmit information from the vehicle and are not, as a standalone system, directly used to control the vehicle.

- **Harmless hardware that does not independently have connectivity functions should be excluded from the definition of VCS hardware.** CTA supports BIS’s explicit exclusion from the definition of VCS hardware component parts that do not contribute to the communication function of VCS hardware. To add clarity to this definition, BIS should add examples to the list of covered hardware components that are included and excluded, including rationale for each item included. For example, the definition of VCS hardware should explicitly exclude coax cables and other harness hardware that do not independently perform any connectivity-related functions or control or add to the vehicle’s connectivity capability but could be considered to be “contributing” to vehicle connectivity. However, CTA does not intend for this example to be limiting or exhaustive in nature.

- **Aftermarket Telematics (AMT) devices should be removed from the definition of VCS hardware.** CTA respectfully recommends BIS revise its determination that aftermarket telematics devices are consistent with this definition and are covered by the proposed rule. The inclusion of AMT devices in the definition of VCS hardware is not necessary from a national security perspective, will cause an extreme burden on a large number of U.S. small businesses, and may also prove to be a burden on BIS.

  Unlike telematics products specifically designed and manufactured for integration into a vehicle during the original manufacturing process, AMT devices are designed to be installed after the vehicle has been manufactured and sold. They are often more modular, designed to be easily installed and removed, and do not have the same level of integration with a vehicle's original systems.

  AMT devices generally pose a reduced security risk compared to integrated VCS hardware. AMT devices primarily have “read only” rights with passive telematics and limited access to critical vehicle systems, can be easily removed or replaced if compromised, and operate in a diverse ecosystem that inherently reduces the potential impact of any single vulnerability.

  The AMT industry in the U.S. is highly fragmented. There are hundreds of telematics companies selling products and services in the U.S., with many additional participating companies in the value chain, and multiple segments and product offerings, including fleet management, commercial trucking, and non-trucking industries like construction, government, and private transportation.

If AMT devices remain covered, hundreds of small businesses will be subject to the requirements of the proposed rule. These small businesses do not have, and cannot afford, legal and compliance departments (or outside counsel) to ensure that they satisfy the rule's requirements. CTA urges BIS to carefully consider the burdens the additional regulatory impacts will have on small business when reassessing the burdens this rulemaking would impose. In addition, potential delays caused by required Declarations of Conformity could cause economic harm, with a risk of damages claims.

- **Prohibited VCS hardware and covered software transactions.** CTA supports BIS's description of "prohibited VCS hardware transactions," and "prohibited software transactions," which states that a transaction will not be "prohibited" solely based on the country of citizenship of natural persons employed or contracted to design, develop, manufacture, or supply VCS hardware.[27] CTA encourages BIS to retain this provision in the final rule, regardless of whether or not it is for hardware or software, or for conventional or ADS vehicles, in order to protect employees and contracted individuals from unfair treatment based on their nationality.

  On this note, BIS should amend the VCS hardware and covered software prohibitions to confirm, as suggested in its corresponding discussion in Example 19, that such hardware or software is not subject to the rule's restrictions when Chinese and/or Russian nationals participate in the design and/or manufacture from *outside* of the PRC or Russia.[28]

- **Covered software.** To avoid capturing technologies that do not directly facilitate VCS or ADS at the vehicle level, CTA recommends that BIS remove the phase "that supports" and replace it with "that directly enables" within its definition of "covered software." CTA also recommends that BIS offer clarity on whether software imported as a stand-alone import outside of a completed connected vehicle would be considered covered software. Generally, the complexity of software systems may create a challenge for differentiating between the various layers in the software stack. To the extent that BIS can provide further explanation of what is intended and not intended to be included in the software stack (i.e., firmware, embedded software, middleware, or other layers) further detail would be appreciated.

  CTA supports BIS's decision not to include firmware and open-source software in the definition of covered software. We urge BIS to amend the proposed rule's language to explicitly state that the rule's prohibitions do not apply to open-source software that is not directly tied to the VCS or operation of the vehicle, even if that open-source software uses VCS for communications. CTA specifically proposes that BIS add the following language to the end of the definition of "covered software":

  > *Covered software also does not include automotive open-source software that resides on an in-vehicle infotainment unit or centralized head unit and relies on communications through a VCS.*

  We request BIS provide clarity that ADS software that is not connected to a covered entity and that is added to a completed connected vehicle is not considered "covered

[27] Notice at 79117.
[28] Notice at 79107.

software." Specifically, BIS should reconcile the proposed rule's definition of "covered software" with the stated intent in the preamble, which states that, "open-source software that has been modified is only considered "covered software" if the entity doing the modifications has a nexus to the PRC or Russia;" and "ADS software that is not designed, developed, manufactured, or supplied by persons owned, controlled, or subject to the jurisdiction or direction of the People's Republic of China (PRC) or the Russian Federation (Russia) and which is added to a completed connected vehicle, is not considered a manufacturing operation and as such would not be covered."[29]

This can be achieved with the following edits to the definition, indicated in italics, which would bring the text of the proposed rule in line with BIS's stated goals and provide clarity for regulated entities:

> "Covered software also does not include open-source software that can be freely used, modified, and distributed by anyone, with both access to the source code and the ability to contribute to the software's development and improvement unless that open-source software has been modified *by someone owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia* for proprietary purposes and not redistributed or shared. *ADS software that is not designed, developed, manufactured, or supplied by persons owned, controlled, or subject to the jurisdiction or direction of the People's Republic of China (PRC) or the Russian Federation (Russia) and which is added to a completed connected vehicle, is not considered a manufacturing operation and as such would not be covered."*

To further reduce confusion and help stakeholders comply, CTA recommends BIS define "open source" and "firmware" as follows:

- **Open source.** BIS should define "open source software" independently of "covered software" in alignment with the definition included in Pub. L. 115-232 (the FY 2019 National Defense Authorization Act):

  > "The term ''open source software'' means software for which the human-readable source code is available for use, study, re-use, modification, enhancement, and re-distribution by the users of such software."

  This definition is well-accepted amongst industry stakeholders, and a similar definition is used by the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS).[30]

  In addition, BIS proposes that if licensed open-source software is modified to create proprietary enterprise software for a specific use not meant for redistribution, the resulting software could be subject to prohibition if the person modifying the open-source software is owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.[31] BIS should provide additional

[29] Notice at 79102.
[30] *See Cybersecurity and Infrastructure Security and Resilience*, CISA Open Source Software Security Roadmap, (Sept. 2023) at 3, https://www.cisa.gov/sites/default/files/2024-02/CISA-Open-Source-Software-Security-Roadmap-508c.pdf.
[31] Notice at 79102.

clarification for, or consider striking, this general exclusion for open-source software.

- **Firmware.** In its definition of covered software, BIS characterizes firmware as software with the primary purpose of controlling hardware.[32] CTA agrees that firmware is distinct from software and is more comparable in function to hardware and recommends BIS retain this definition in its final rule. That said, for purposes of ensuring alignment between BIS and industry, CTA encourages BIS to adopt a more precise definition for firmware that will help industry appropriately scope the application of the firmware exclusion.

  In addition to firmware, "embedded software," which is not addressed in the NPRM, is key to the functioning of connected vehicle hardware, but does not itself control a particular connected vehicle. Like firmware, embedded software is commonly provided by the hardware supplier as an integral part of the hardware component and is not generally divisible or distinguishable from hardware for purposes of supply chain management. Embedded software is specialized programming on non-primary processor devices that controls specific functions of the device. It has fixed hardware requirements and capabilities, and because of that, the addition of third-party hardware or software is strictly controlled. In the case of communications semiconductors (e.g. cellular modems, Wi-Fi chips, Bluetooth chips, wired ethernet chips), the software that runs directly on those chips, and controls the ability to set up connections to allow for the transfer of information, is frequently considered to be embedded software.

  The embedded software does not facilitate the collection of data or control the vehicle. It does not make decisions on what to communicate, when to communicate, or to whom to communicate; it is told that information by the application-level software running on the primary processor. CTA therefore recommends that BIS consider excluding from any final rule "embedded software," defined as "specialized programming on non-primary processor devices that controls specific functions of the device, has fixed hardware requirements and capabilities, and as a result, enables strict controls around the addition of third-party hardware or software."

Finally, BIS should clarify that legacy software code developed prior to the effective date of the Connected Vehicle rule is not prohibited. The technology that the NPRM seeks to regulate is linked to technology primarily developed for other use cases, such as mobile cellular communications, implicating lines of historical code that is essential to connected vehicles but that were not originally designed for automotive applications. Today's automobiles leverage technologies based on decades worth of research and development from other sectors such as the mobile telephone and telecommunication industries. The software code for 3G, 4G, and 5G telecommunications is developed by software engineering teams from around the world, including from China, and built on top of legacy code developed for other use cases.

As such, the global nature of software development and industry's reliance on existing legacy code—including code developed in China—will likely create significant compliance challenges with respect to the Proposed Rule's definition of covered

[32] Notice at 79116.

software. Determining retroactively whether a person "owned by, controlled by, or subject to the jurisdiction or direction of [China] or Russia" was ever involved in the development of software, particularly with respect to software incorporated into semiconductor components that are not specific or unique to vehicle connectivity systems or automated driving systems, is nearly impossible given the decades of history related to the development of connectivity technology and the global nature of such development. Even if such determinations were possible as a technical matter, disaggregating historical software code from connected vehicle-specific code would not be economically viable. Requiring semiconductor suppliers to rewrite legacy code that has otherwise already been tested and certified for quality, and used securely worldwide for decades, would impose further costs on semiconductor industry players, particularly in the mature-node segment of the industry which is facing additional pressures due to non-market policies and practices.

Given that the NPRM neither defines nor considers the reliance on legacy code as part of a connected vehicle's system and given the associated compliance challenges it would impose on companies, we encourage BIS to clarify that legacy software code is not prohibited under the final rule.

- **Hardware Bill of Materials (HBOM) and Software Bill of Materials (SBOM):** As will be explained in greater detail in the section below, CTA recommends that BIS not require SBOMs or HBOMs be submitted in Declarations of Conformity. Apart from this recommendation, CTA also recommends that BIS amend its definition of HBOM to align with existing government definitions. BIS defines an HBOM as "a comprehensive list of parts, assemblies, documents, drawings, and components required to create a physical product" that includes information identifying the manufacturer like firmware, technical information, and descriptive information.

  This definition includes information that cannot be mapped at this time and would risk revealing trade secrets and confidential business information. BIS's use of "documents" and "drawings" in the HBOM definition does not align with other governmental definitions of HBOM, would be a significant burden, and would provide information that would not be useful to BIS without additional explanation from experts in the field. Further, BIS's definition of HBOM requires submitting firmware information, but BIS has not explained within its definitions for hardware why firmware information would also need to be disclosed. BIS should modify its definition of HBOM to address these concerns and align more closely with CISA's HBOM Framework for Supply Chain Risk Management. For example, CTA recommends an HBOM include: HBOM header information, entity name, entity location, finished good product details, component part information, and component part details.

V. Declaration of Conformity

- **Timeline.** CTA believes that BIS can obtain up-to-date information without requiring companies to submit annual Declarations of Conformity. Instead, CTA recommends BIS remove this requirement in favor of a streamlined attestation or self-certification that states the regulated entity is not knowingly engaged in a prohibited transaction. In the alternative, if updates directly to BIS are deemed necessary, BIS should require updates to Declarations of Conformity only when the Model Year in question has undergone material changes. Since contracting occurs well in advance of the Model Year, it is not productive to require Declarations annually for the same Model Year if nothing has

changed. This reasonable alternative would further BIS's goals of ensuring compliance while avoiding the imposition of unnecessary burdens on regulated entities.

- **Material Change**. BIS proposes to require VCS hardware importers or connected vehicle manufacturers to submit an updated Declaration of Conformity and an updated HBOM or SBOM within 30 days of a material change that impacts the contents of a Declaration of Conformity.[33] CTA recommends that BIS change this requirement to make updates annual. CTA also recommends that BIS add a time limitation to the material change requirement because minor software updates could result in numerous changes to the SBOM that would not be useful to BIS and that would make this requirement overly burdensome. For example, even a new author, or a slight software update, would constitute a change to an SBOM, even for vehicles that are 15 years old. CTA recommends BIS limit this requirement to vehicles that are 10-years old or newer, a timeframe which aligns with BIS's intent to maintain up-to-date information without being overly burdensome.

  On this note, CTA emphasizes that software for connected vehicle applications is updated on a constant basis for safety and performance reasons. These updates address myriad safety concerns that this rulemaking is concerned with guarding against, such as through software patching to address cybersecurity risks or threats.

  CTA recommends BIS not require connected vehicle manufactures to submit an updated Declaration of Conformity for Firmware Over the Air (FOTA) or Software Over the Air (SOTA) updates so that these important safety precautions can continue in a responsive manner. The administrative burden of submitting a new Declaration for each of these updates would be overwhelming and may force connected vehicle manufacturers to reduce the number of updates they perform.

  In addition, CTA recommends that BIS take into account that VCS hardware importers and connected vehicle manufacturers face constraints in their ability to know when a change has occurred at high levels of the supply chain. For example, a company may not know when a Tier 5 supplier changes its Tier 6 supplier. Companies may be restricted in their ability to comply with the material change requirement based on the information available to them.

- **Recordkeeping Requirement.** CTA asks that BIS consider revising the 10-year retention requirement to a lower standard, such as five years. If BIS chooses not to revise the 10-year requirement, CTA urges BIS to narrow the scope of records that must be retained. The current language regarding what records must be retained includes "business records related to the execution of a transaction, such as contracts, import records, bills of sale, relevant correspondence, and all other files specified in sections 791.312 and 791.313 to assess compliance with the rule." BIS should consider reducing these requirements to only essential records relating to the key concerns this rulemaking is focused on, namely contracts, import records, and bills of sale. CTA also requests further clarification on the specific requirements for storing compliance data throughout the process, such as the permissible location for data centers.

[33] Notice at 79109.

- **SBOM and HBOM Requirement.** SBOMs and HBOMs pose considerable threats to confidential business information. CTA asks BIS to address this risk by removing the requirement that SBOMs and HBOMs be submitted as part of the Declaration of Conformity. Instead, BIS should require that this information be made available at the agency's request for investigations and audits, by the vehicle importer, vehicle manufacturer, or the equipment manufacturer, for any ADS/VCS software or VCS hardware. Doing so would mitigate costs, reduce paperwork, and minimize risk that proprietary information will be shared, including the national security concerns that could exist if the information were subject to a cybersecurity attack. It would also minimize the risk that sensitive IP from suppliers of advanced systems would have to be shared with vehicle importers—who could be future competitors—so that the vehicle importers themselves could satisfy their own Declaration of Conformity requirements. At a minimum, if BIS declines to remove this requirement, CTA recommends that BIS delete the HBOMs and SBOMs from their system after their analysis is complete to prevent possible leakage of sensitive information afterwards.

- **Definition of "Due Diligence."** BIS proposes to require that Declarations of Conformity for both covered software and VCS hardware include documentation of due diligence efforts but does not define "due diligence."[34] This creates a risk to BIS that it may not get the information it needs, and a risk for regulated companies that they may not be in compliance even after completing reasonable due diligence. We recommend BIS state in the final rule that the due diligence requirement is satisfied if a company provides third-party or independent research in its Declaration, but that the use of such third-party or independent research is not required.

  CTA recommends that BIS consider alternatives to the import prohibition for VCS hardware or covered software that is not owned by or controlled by a foreign adversary interest. BIS should consider allowing importers to conduct their own due diligence or evaluation to ensure their imports do not pose a risk or are exploitable. As an example, BIS could consider whether industry processes or standards could be adopted that would allow for import of a restricted component while maintaining the necessary security. CTA suggests that BIS consider NHTSA's Federal Motor Vehicle Safety Standards (FMVSS) self-certification process as a potential model for the self-certification process included in the Declarations of Conformity.[35]

- **Other requirements.** BIS proposes to only require connected vehicle manufacturers to provide information regarding the make, model, and trim of imported completed connected vehicles for which VCS hardware is intended if that information is known.[36] This definition does not address instances when the purpose of the use for the hardware could evolve but would pose no new risk. We recommend modifying the text as indicated in italics, to address this definitional gap:

---

[34] Notice at 79117-8.
[35] *Understanding NHTSA's Regulatory Tools*, NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION, https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/understanding_nhtsas_current_regulatory_tools-tag.pdf.
[36] Notice at 79117.

(v) if known *at first submission*, the make, model, and trim of the completed connected vehicles for which the VCS hardware is intended.

BIS also proposes to require companies to submit, as part of the Declaration of Conformity, a list of third-party external endpoints to which the VCS hardware connects, including the country, identity, and location of the service.[37] The proposed rule's reference to these endpoints and connections is overly broad. BIS has stated that the focus of this rule is on VCS hardware "that integrate various radio frequency communication technologies and enable Connected Vehicles to access external data sources." While it appears that BIS meant to exclude connections to tethered devices such as electric vehicle supply equipment (EVSE) (EV chargers) and aftermarket diagnostic scan tools which have connectivity and enable the transfer of data on and off of the vehicle, CTA recommends BIS clarify that tethered devices are excluded as "endpoints" in this rulemaking.

Further, the number of third-party external endpoints a modern infotainment system can connect to is extensive and continuously changing, since users can download external applications which have their own freely changing connections and endpoints. There is no certainty that network hosting will remain static throughout time, and the manufacturer of the VCS hardware is not usually notified of this changing information. For this reason, providers often will not be able to provide detailed information about third-party external endpoints, and CTA recommends that BIS remove the third-party external endpoint requirement entirely. Alternatively, VCS hardware manufacturers could provide a Declaration as to the regional data connectively possibilities for the respective hardware, such as by providing a statement to BIS listing the general region in which the hardware will function. Another alternative would be for BIS to require endpoint hosts for connected vehicle applications to provide Declarations concerning the nature of their entity and the location of the associated data transacted.

In general, much of the information BIS requests that companies submit in the Declaration of Conformity would be time consuming and costly to gather, package into a digestible format, and report to BIS, and would create new cybersecurity and information risks. Rather than require this information at the onset, BIS should instead require that it be made available for review by the agency as needed.

VI. General Authorizations

CTA supports BIS's proposal to provide General Authorizations under a self-certification regime for transactions that would otherwise be prohibited but that meet specific requirements. CTA believes the scope of transactions that qualify for a General Authorization should be broadened to include the following:

- **Amend General Authorization No. 4.** BIS has stated that General Authorizations are intended for transactions "where any undue or unacceptable risks to national security can be reasonably mitigated."[38] VCS hardware imports intended to be assembled into vehicles solely for export to China or other jurisdictions fall within this description, as these imports' final intended market is outside the United States. To address this, CTA

[37] *Id.*
[38] Notice at 79116.

recommends that BIS amend General Authorization (4) by adding "assembly" as indicated in italics:

> 4) The completed connected vehicle that incorporates covered software or the VCS hardware is imported solely for purposes of repair, alteration, *assembly,* or competition off public roads and will be reexported within one year from the time of import.

- **Additional General Authorization for re-imported hardware.** CTA recommends that BIS add a General Authorization for re-imported VCS hardware (and components thereof) that are manufactured in the United States, temporarily exported from the United States for integration purposes, and then re-imported into the United States ("General Authorization for re-imported VCS hardware").

  The proposed rule's importation test for VCS hardware is broad and could unnecessarily disrupt manufacturing and trade by interfering with the existing multi-national supply chains (that do not involve the PRC or Russia) of automotive OEMs and their primary suppliers. To address this, CTA recommends that BIS provide a General Authorization for VCS hardware that is made in the U.S., temporarily exported, and then re-imported.

  The U.S. government should seek to encourage U.S. production of vehicles and their components. By focusing on importation of VCS hardware regardless of its country of manufacture, the rule as drafted discourages production of VCS hardware in the United States. It is counterproductive and contrary to the interests of U.S. industry and the U.S. public to require automotive manufacturers to establish alternative supply chains in cases where the hardware is 'Made in the USA.'

  The proposed rule may cause U.S.-headquartered automotive manufacturers to become less competitive against their foreign competitors. It also may deny all automotive manufacturers serving the U.S. market the opportunity to take advantage of cost-saving technological developments in the production and assembly of vehicles and their component systems, thus disadvantaging the U.S. public that utilizes automobiles through higher prices or the inability to offer reduced prices.

  BIS should add an additional General Authorization to cover VCS hardware that is made in America. CTA recommends the following language:

  > The imported VCS Hardware (or component thereof) was (i) manufactured in the United States, (ii) exported temporarily for purposes of incorporation into a VCS or a completed connected vehicle to a country other than the PRC and Russia and not to any persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, and (iii) then re-imported into the United States.

VII. Specific Authorizations

CTA supports the inclusion in this rulemaking of a Specific Authorization process that permits connected vehicle manufacturers and VCS hardware importers to continue forward with otherwise prohibited transactions when it has been determined that national security risks can be mitigated to an acceptable degree.

Specifically, CTA supports the proposal that applicants independently perform a threat analysis regarding their ability to limit PRC or Russian government access to, or influence over, the design, development, manufacture or supply of the VCS hardware or covered software.

Lastly, BIS should also clarify whether there are specific requirements for conducting proof of content testing in the U.S. with Chinese network access device technologies only available from China.

VIII. Advisory Opinions

CTA appreciates BIS's willingness to offer advisory opinions to allow VCS hardware importers and connected vehicle manufacturers to seek guidance from BIS on whether a prospective transaction may be prohibited.[39] BIS has stated it will only consider advisory opinion requests for actual, as opposed to hypothetical, transactions. To assist companies with compliance, CTA recommends BIS institute a period where they will accept hypothetical advisory opinions, to help industry navigate these rules before they are put into effect.

CTA recommends that BIS develop a process by which it would pre-clear the continued use of certain covered software or hardware by trusted suppliers. Pre-clearance could be conditioned on companies meeting specified cybersecurity standards and implementing appropriate risk mitigation measures.

IX. Appeals

CTA supports BIS's proposal to create a mechanism by which any person whose application for a special authorization is defined may appeal the decision to the Under Secretary.[40] CTA recommends that BIS expand on this appeals option and create a detailed framework process, which all parties, including suppliers and manufacturers, can use as a guide to navigate through the appeals process effectively.

Thank you for the opportunity to provide these comments. CTA looks forward to continued collaboration with the Government on these important issues.

Sincerely,

/s/ Michael Petricone
Michael Petricone
Senior Vice President, Government and Regulatory Affairs
Consumer Technology Association
1919 S Eads St. Arlington, VA 22206

[39] Notice at 79090.
[40] Notice at 78111.

/s/ Ed Brzytwa
Ed Brzytwa
Vice President, International Trade
Consumer Technology Association
1919 S Eads St. Arlington, VA 22206

/s/ India Herdman
India Herdman
Senior Manager, Policy Affairs
Consumer Technology Association
1919 S Eads St.
Arlington, VA 22206

/s/ Finch Fulton
Finch Fulton
K&L Gates LLP
1601 K St., NW
Washington, DC 20006