US-China Business Council Comments on Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles (Docket No. 240919-0245) (RIN 0694-AJ56)

The US-China Business Council (USCBC) appreciates the opportunity to submit feedback to the Department of Commerce regarding the notice of proposed rulemaking (NPRM) on "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles."[1] USCBC represents more than 270 American companies engaged in business with China. Our membership covers a wide range of industries and sectors and includes many automotive and technology companies. Our members include some of the most recognizable American brands and small-and medium-sized enterprises.

USCBC supports the administration's whole of government approach to protect Americans from foreign adversaries that may exploit vulnerabilities in information and communications technology and services (ICTS). Our businesses are stronger and more resilient, whether it be in the United States or abroad, when connected systems are secure. We acknowledge the legitimacy of the national security risks associated with connected vehicles (CVs) identified and described in the NRPM and acknowledge BIS's responsibility to address those risks to protect US national security. We understand that China[2] and other countries have similar concerns.

USCBC strives to act as a constructive partner to the administration in ensuring US national security and the competitiveness of US companies. USCBC member companies have at significant expense, taken measures to assess the security of Chinese suppliers' products and evaluate connections to known malicious actors maintained on lists such as the Entity List and SDN list. In some cases, they have abrogated commercial relationships beyond what is required under US law, often at the detriment of their global competitiveness and to their reputations as reliable business partners. As BIS moves to finalize the rule, USCBC requests additional clarity around certain definitions and aspects of implementation.

USCBC is concerned that implementation of these rules could create friction with allied countries that do not yet have similar controls and could disadvantage US firms that compete with international suppliers in China. Additionally, there is a chance that such measures could invite retaliation. The United States should use the final rule as a template to pursue a multilateral and harmonized regulatory framework through plurilateral forums, such as the US-EU Trade and Technology Council (TTC) and US-Canada-Mexico Agreement (USMCA).

---

[1] [1] https://www.federalregister.gov/documents/2024/09/26/2024-21903/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles

[2] https://mp.weixin.qq.com/s/404yJjpaM7a6anAxE7FuFg

Executive Summary

To facilitate smooth implementation and compliance with the final rule, and to inform potential future invocations of ICTS authorities, USCBC makes the following recommendations. Our recommendations are centered around improving clarity, creating consistency, and easing implementation for regulators and industry alike.

Definitional concerns

- BIS should define and provide illustrative examples of the terms *assemble*; *design; develop; manufacture; material change; supply; and U.S. person*.
- BIS should clarify the definitions of the terms *automated driving system*; *covered software*; *person owned by, controlled by, or subject to the jurisdiction of a foreign adversary*; *vehicle connectivity system (VCS)*; and *VCS hardware*.

Recommendations

- BIS should clarify that the rule does not apply to VCS hardware importers and CV manufacturers that import covered hardware intended for assembly into vehicles that are not covered by the definition of *connected vehicle*.
- BIS should clarify that the rule does not apply to VCS hardware importers and CV manufacturers that import covered hardware intended for assembly into vehicles for reexport to China or elsewhere.
- BIS should develop a preclearance procedure to ensure automakers and suppliers have advance approval for continued use of certain covered software, with appropriate risk mitigation.
- BIS should publicize approvals, denials, and appeals decisions issued under specific authorizations, consistent with the government's obligations to protect companies' sensitive proprietary information and intellectual property.
- BIS should issue guidance for completing declarations of conformity, which would provide clear and standard directions to VCS hardware importers and CV manufacturers undergoing the declaration of conformity process.

Additional suggestions

- BIS should align its rules on ICTS supply chains and infrastructure to the extent feasible with other allied and partner countries that have developed similar measures. The administration should work with other countries to harmonize regulations and best practices to secure ICTS supply chains and infrastructure better while minimizing adverse impacts on US company competitiveness.
- BIS should communicate its objectives with China's commercial regulators and Chinese companies to prevent misunderstandings and provide a more permissive environment for US companies to conduct due diligence into their supply chains.
- BIS should clarify whether there are specific requirements for conducting proof of concept testing in the United States with Chinese network access device technologies only available from China.

I. BIS should address the following definitional concerns

Meaning of assemble, designed, developed, manufactured, and supplied

As written, BIS proposes to apply restrictions to products that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. The term *assembled* is also used several times in the NPRM, in an example of a prohibited transaction (Example 15), to describe situations in which a CV manufacturer would not need to submit a declaration of conformity, and to describe requirements that BIS may include in specific authorizations for CV manufacturers that products that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of China. BIS does not, however, define *assembled*, *designed*, *developed*, *manufactured, or supplied*.

The meaning of some of these terms, such as manufactured, are relatively straightforward, but others, such as developed can apply to several different business scenarios, particularly with respect to software. For example, it is unclear whether the utilization of a software module from China as part of a larger ADAS suite means that the final software is considered "designed" or "developed" by a person owned by, controlled by, or subject to the jurisdiction or direction of China. Further, the application of these terms could be interpreted so broadly as to capture both hardware and software items designed, developed, or manufactured historically in China prior to the rule taking effect. 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 that is not specific or unique to vehicle connectivity systems or automated driving systems, but is nonetheless foundational to vehicle connectivity systems, is impossible.

To minimize confusion among importers, BIS should specify business processes that constitute assembly, design, development, manufacture, and supply, and provide specialized definitions for each of these terms where applicable to vehicles, software, and systems, respectively. Doing so will provide much needed clarity to CV manufacturers and VCS hardware importers and provide a more even playing field for companies with varying levels of sophistication when it comes to compliance resources.

Person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary § 791.301

BIS should clarify the definition *of person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary*. The term is defined in part in subparagraph (1) as

> [A]ny person, wherever located, who acts as an agent, representative, or employee, or any person who acts in any other capacity at the order, request, direction or control, of a foreign adversary or of a person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary.

For the vast majority of CV manufacturers and VCS hardware importers, it is not immediately apparent how to determine whether certain elements of this definition, such as subsidization, are applicable to their business partners. BIS should provide additional guidance on how CV manufacturers and VCS hardware importers can determine whether their suppliers are subsidized, financed, controlled, or are acting "in any other capacity." Absent further guidance, making such determinations will be especially challenging for non-publicly traded companies where information relating to ownership structures and subsidization is not readily available.

It is essential that BIS furnish additional material, including certification templates, that CV manufacturers and VCS hardware importers can use to determine whether suppliers meet these definitions and to help importers qualify suppliers.

Automated driving system § 791.301

BIS should clarify whether it intends for there to be any distinction between the definition of automated driving system as proposed in the proposed rule and the definition in SAE Levels 3-5.[3]

Covered software § 791.303

BIS should amend the definition of *foreign interest* under *covered software* to apply only to cases where a foreign person retains a legal ownership or control interest over software. This definition (particularly given the reference to OFAC's use of the same term) may be misinterpreted as being so broad as to sweep in virtually any software code a non-US person has ever developed. The proposed rule and the underlying executive order, which are limited in scope to restricting technologies that pose an "undue" or "unacceptable" risk to national security, should not be read so broadly as to encompass code subject to these safeguards.

Firmware

BIS should define *firmware* under *covered software* by referencing industry standards. BIS should also consider excluding "embedded software," which is not addressed in the proposed rule, but like firmware, 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.

Infotainment software

In the NPRM, BIS discusses extensively its intent to exclude operating systems unless they have VCS components and fall within the proposed rule's definition of VCS hardware. However, at one point in the text BIS mentions, "At a minimum, this definition of covered software would include operating systems such as a real-time operating system (RTOS), and general-purpose operating systems." (FR 79102). The NPRM has otherwise been clear that in-vehicle infotainment software that does not have its own connectivity and requires communication through a VCS is not within the NPRM's scope [see FR 79092]. But the phrasing on FR 79102 creates some confusion and could be misinterpreted to more broadly catch all general-purpose operating systems, contravening what the NPRM has otherwise articulated about automotive software systems like BMS and automotive OS that do not have their own connectivity.

For this reason, we urge BIS to explicitly exclude OS software that is not directly tied to the function of the VCS or operation of the vehicle even if that OS software uses the VCS for communications and include an expanded definition of covered software that states, "Covered software also does not include automotive OS software that resides on an in-vehicle infotainment unit or centralized head unit and relies on communications through a VCS."

Open-source software

BIS should consider adopting the definition of *open-source software* used in the 2019 National Defense Authorization Act[4] (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)

[3] https://www.iso.org/standard/73766.html

[4] https://crsreports.congress.gov/product/pdf/R/R45816

or the Department of Homeland Security Cybersecurity and Infrastructure Security Agency's[5] definition (software for which the human readable source code is made available to the public for use, study, re-use, modification, enhancement, and re-distribution). Doing so will streamline future compliance with the proposed regulations.

Material change § 791.305

As written, CV manufacturers and VCS hardware importers are required to file follow up declarations any time there is a "material change" that makes a prior declaration no longer accurate. BIS should define *material change* and provide examples of changes which would trigger a CV manufacturer or VCS hardware importer's obligation to submit an updated declaration of conformity and an updated hardware bill of materials (HBOM) or software bill of materials (SBOM).

U.S. person § 791.301

BIS should define *U.S. person* under the rule and harmonize it with the definition of *U.S. person* under the EAR[6] by including protected individuals.

VCS hardware § 791.301

BIS should amend the definition of *VCS hardware* to only include hardware in which there is a *foreign interest*. As under the definition of *covered software*, *foreign interest* under the definition of *covered software* should apply only to cases where a foreign person retains a legal ownership or control interest over software.

Aftermarket devices

BIS should provide greater clarity on the scope of coverage for aftermarket devices. While BIS notes that aftermarket device coverage is intended, in the explanation, BIS notes that the VCS hardware definition is intended to "include aftermarket devices not contained in a completed connected vehicle at sale but that could be later integrated into or attached to the vehicle to perform VCS functions." The requirement that the device be "integrated into or attached to the vehicle" is not clear in the VCS definition.

BIS should revise the phrase "support the function of [VCSs] or that are part of an item that supports the functions of VCSs" to make clear that the device must be integrated into or attached to the vehicle to be covered. Further, BIS should define what "integrated into or attached to the vehicle" means in this context. As written, it is broad enough to include aftermarket devices not contained in a completed CV at sale but that could later be temporarily attached to the vehicle to perform VCS functions, e.g., mobile phones. We understand the intention from the notes to be more permanent attachments, like fleet tracking devices. However, even in that space, there are devices that can be temporarily installed, e.g., attached with a few screws, that would track single or multiple shipments, rather than being installed for permanent use on the vehicle. While these devices may provide limited data on the location of a vehicle for some period of time, they do not provide any connectivity to the vehicle's operational functions.

Automotive radar

[5] https://www.cisa.gov/sites/default/files/2023-09/CISA-Open-Source-Software-Security-Roadmap-508c%20%281%29.pdf

[6] https://www.bis.gov/ear/title-15/subtitle-b/chapter-vii/subchapter-c/part-772/ss-7721-definitions-terms-used-export

BIS should explicitly exclude automotive radar, which like LiDAR lacks the ability to transmit from the vehicle and does not, as a standalone system, control a vehicle.

Harness hardware

BIS should clarify that 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 which contribute to vehicle connectivity are not covered hardware.

II. BIS should clarify that importing covered VCS hardware for assembly into vehicles that are either not covered by the definition of CV or intended for reexport is not prohibited

BIS should clarify that the import of covered VCS hardware for assembly into vehicles that are not covered by the definition of *connected vehicle* or intended for reexport is not prohibited. This should be true regardless of whether vehicle assembly occurs in a foreign trade zone. Motor vehicles are a key export for the United States. In 2023, US motor vehicle exports to the world exceeded $78.5 billion and exports to China exceeded $6 billion.[7] Automotive manufacturing supports over 2 million US jobs[8] and it is imperative that the United States remain a competitive location for automotive manufacturing. Allowing VCS hardware importers and CV manufacturers to continue importing covered VCS hardware intended for assembly into vehicles that are not covered by the definition of *connected vehicle* or intended for reexport would help the United States maintain its position as a leading automotive manufacturing country.

III. BIS should clarify that importing covered VCS hardware as service or warranty parts is not prohibited

BIS should clarify that the import of VCS hardware as service or warranty parts for vehicles placed in service prior to January 1, 2029, is not prohibited. Automakers typically have warranty obligations for past model years that may run up to 10 years or longer following a given model year. Such VCS hardware may or may not be specific to a given model year. BIS should clarify that VCS hardware imported as service or warranty parts after January 1, 2029, are not captured by the prohibitions in *§* 791.302 and/or are authorized by the exemptions in *§* 791.308 provided that such VCS hardware units are intended for use solely as service or warranty parts for vehicles placed in service prior to January 1, 2029.

IV. BIS should develop a preclearance procedure to ensure automakers and suppliers have advance approval for continued use of certain covered software, with appropriate risk mitigation

Code for automotive use is built on top of legacy code for other use cases, like mobile phones and personal computers. It is not feasible to require automakers or suppliers to eradicate or rewrite this legacy code because it may have prior development in China. Because the automotive industry relies on this prior development for non-CV use cases, it could result in significant disruptions if companies are required to wait for a specific authorization to continue to use certain legacy code portions in automotive applications.

Under the proposed rule it is likely that requests for specific authorization will be reviewed on a case-by-case basis and may require varying lengths of time depending on the complexity of the case. At the same time, a timely decision by BIS to grant or deny a specific authorization request

[7] https://usatrade.census.gov/

[8] https://www.autosinnovate.org/resources/papers-reports/Driving%20Force%20Annual%20Report.pdf

will be critical for business and product planning purposes. We note that such authorizations must be made at least three to four years before any model year enters production. Automotive suppliers, particularly of high-technology vehicle connectivity systems and components, cannot make investments in design and development of automotive products years before the vehicles enter the market for sale without certainty that their products and activities will be permitted in the US market. BIS should therefore consider a preclearance process that would provide advance approval for the continued use of certain covered software and hardware in connected vehicles sold in the United States.

A preclearance procedure would mitigate the risk of undue harm to industry while still also addressing the supply chain integrity concerns related to CV software. In addition to allowing preclearance with respect to certain covered software, BIS could require companies seeking preclearance to meet specified cybersecurity standards and risk mitigation measures specific to ensuring the integrity of the relevant code, including third party vulnerability testing as applicable. Sufficient time must be built into the rule so that preclearance can be granted before any prohibitions are anticipated to affect the market.

V. BIS should improve the specific authorization mechanism by publicizing approvals, denials, and appeals decisions

BIS should improve the specific authorization mechanism by publicizing approvals, denials, and appeals decisions for specific authorizations. Applicants' business confidential information should be redacted when BIS publishes approvals, denials, and appeals decisions. By making approvals, denials, and appeals decisions public, BIS would help to facilitate compliance by informing companies of the nature and structure of transactions BIS is willing to grant specific exclusions for. VCS hardware importers and CV manufacturers would be able to make better informed decisions about whether to request a specific authorization and BIS would likely receive fewer applications for specific authorizations. BIS should also issue guidance for submitting appeals applications, outlining the format of the written appeal application and identifying supporting documents that will help BIS make its decision. This would allow BIS to devote more resources to the timely review of applications that are submitted.

VI. BIS should issue guidance for completing declarations of conformity

The supply chains required to produce connectivity technologies in vehicles are highly complex, often involving numerous suppliers and intricate relationships across multiple tiers and countries. With the various inputs needed to assemble these technologies, it can be challenging for companies to fully trace their supply chains. Therefore, it is essential that BIS issue guidance on declarations of conformity for VCS hardware importers, CV manufacturers, and other stakeholders. Doing so will help companies to meet their compliance obligations and do so efficiently and cost-effectively.

In the guidance, BIS should tell VCS hardware importers and CV manufacturers how far back in their supply chain, from raw material input to finished product, they must trace to comply with the final rule. BIS should also outline and provide samples of the documents needed to submit a complete declaration of conformity. The US Customs and Border Protection Agency (CBP) provides similar guidance to importers who are seeking to undergo the applicability review process to dispute a detainment of goods under the Uyghur Forced Labor Prevention Act (UFLPA).[9] This guidance, though not exhaustive, identifies documents that facilitate the review process and

[9] [9]https://www.cbp.gov/sites/default/files/assets/documents/2023-Feb/Best%20Practices%20for%20Applicability%20Reviews_Importer%20Responsibilities_0.pdf

provides a template for affected importers to follow as they undergo the process. We suggest that BIS provide a similar standing guidance for the declaration of conformity process to illustrate exactly what VCS importers and CV manufacturers can submit in order to demonstrate the absence of prohibited transactions in their supply chain, how information should be organized, how records of these documents should be stored, and any best practices for VCS importers and CV manufacturers as they attempt to comply with the rule in a way that minimizes disruptions to industry.

VII. **Impacts on US company competitiveness**

USCBC encourages BIS to align its rules on ICTS supply chains and infrastructure to the extent feasible with allied and partner countries. The United States should use the final rule as a template to pursue a multilateral and harmonized regulatory framework through plurilateral forums, such as the US-EU Trade and Technology Council (TTC) and US-Canada-Mexico Agreement (USMCA). A multilateral and harmonized regulatory framework would better protect ICTS supply chains and infrastructure while minimizing adverse impacts on US company competitiveness. US companies would be less likely to be singled out for Chinese retaliation or seen by their Chinese customers as less reliable than other foreign companies. 45 percent of USCBC's 2024 Member Survey respondents reported that their company had lost sales due to uncertainty of continued supply while 29 percent of respondents reported that their company faced increased scrutiny from regulators in China.[10] These numbers are likely to increase should the US not pursue a multilateral and harmonized regulatory framework. USCBC applauds the administration's effort to work with partners and allies on CVs risks[11] and encourages the administration to communicate its objectives with China's commercial regulators and Chinese companies to prevent misunderstandings and provide a more permissive environment for US companies to conduct due diligence into their supply chains.

VIII. **Conclusion**

USCBC appreciates this opportunity to submit feedback on the proposed rule. Our goal is to support US industry, and we aim to advance this objective while simultaneously assisting the US government in taking appropriate action to address legitimate national security concerns. We hope that this feedback will help BIS continue to balance these two goals. We hope that our comments will lead BIS to clarify ambiguities, provide clear and standard guidance around conformity declarations, and address other concerns outlined in this submission.

[10] [10] https://www.uschina.org/sites/default/files/uscbc_member_survey_2024_en.pdf

[11] https://www.state.gov/first-multinational-meeting-to-address-connected-vehicle-risks/