October 28, 2024

Elizabeth Cannon, Executive Director
Office of Information and Communications and Technology Supply Chain
Bureau of Industry and Security
U.S. Department of Commerce

"Securing the Information and Communications and Technology Supply Chain: Connected Vehicles" [Docket No. 240919-0245]

RIN 0694-AJ56

Dear Executive Director Cannon:

The National Foreign Trade Council (NFTC) appreciates this opportunity to respond to the Notice of Proposed Rulemaking (NPRM) "Securing the Information and Communications and Technology Supply Chain: Connected Vehicles" [Docket No. 240919-0245]. This proposed rule seeks to mitigate national security risks associated with the importation of vehicles from foreign adversaries, principally China and Russia, with certain connected technologies, specifically hardware and software used in Vehicle Connectivity Systems (VCS) and software used in Autonomous Driving Systems (ADS).

NFTC acknowledges the importance and supports the objectives of this rule to address concerns regarding data privacy as well as to deter and prevent the ability of malign foreign actors to disrupt critical transportation infrastructure in the United States. In meeting these objectives, rules on connected vehicles must be narrowly constructed, provide definitional clarity, and where feasible, build on existing mechanisms. We must also consider how to measure the effectiveness of these measures --- what will success look like, particularly as the pace of technological advancements continues to accelerate? How will BIS ensure the durability of these rules? For example, are the Model Year timelines stated in this proposed rule the best way to implement these requirements and are they realistically attainable given the complexity of supply chains and manufacturing schedules? And perhaps most importantly of all, how will the U.S. government address the leakage of ICTS-controlled items described in this proposed rule into the U.S. market, whether intentionally or unintentionally? What mechanisms are being set up to detect this, and how will this be enforced?

Definitional and Scope Concerns

We are concerned by BIS' definition of a person subject to the jurisdiction of this proposed rule to include "… any person who acts in any other capacity at the order, request, or under the **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 party by a foreign adversary… ***[emphasis added].*** The inclusion of "direction" extends beyond

long-standing policies and practices of assessing ownership and control, not defined in this regulation. Moreover, "direction" can be a one-time event as well as episodic; without clear guardrails, the term "direction" can become a "catch-all" for initiating enforcement actions without foundation. NFTC respectfully seeks clarification and limitations on how "direction" will be defined for purposes of implementing a final rule on connected vehicles.

NFTC appreciates the concern given to minimizing supply chain disruptions including phased implementation beginning with MY2027. However, that this proposed rule was developed "…irrespective of any other automobile-related trade actions taken by the U.S. government" precludes the ability to leverage existing processes administered by other agencies to streamline compliance. For example, the Federal Communications Commission also administers regulations affecting underlying telecommunications technology and software.

Proposed hardware and software controls

NFTC appreciates BIS' effort to limit the scope to the specific hardware and software that enable wireless connectivity without including other systems that may make use of connectivity. However, in its definition of VCS, the proposed rule does not specify what hardware, and software falls out of scope. We therefore respectfully suggest that VCS specifically excludes a hardware or software item that merely exchanges data with a VCS without affecting the ability of the VCS to transmit, receive, concert or process radio frequency communications. This would achieve the desired national security outcomes whilst avoiding overreach.

NFTC notes that a single chip can serve multiple purposes and be used in multiple systems. In many cases, chips are designed to serve multiple use cases, including other than in a connected vehicle. We respectfully request that the OICTS exclude chips where the primary or intended use case is not automotive. We also seek clarification on the treatment of legacy chips as well as other hardware and software that was developed prior to a final rule on connected vehicles, particularly in cases where Chinese content cannot be definitively ruled out. It is a normal expectation that an automobile can require repair and servicing for well over a decade and that parts and components containing legacy chips may need to be replaced as part of routine maintenance or repairs. Lastly, we ask OICTS to examine instances where products are primarily "designed, developed and manufactured" either in the U.S. or other non-foreign adversary location, yet elements of the supply chain for hardware or software may "pass through" a foreign adversary (e.g., China), and consider applying an exclusion or de minimis threshold for such cases.

NFTC seeks clarification on how the OICTS plans to protect proprietary information contained in HBOMs (Hardware Build of Materials) and SBOMs (Software Build of Materials). H/SBOMs may contain detailed specifications and other information that can be considered intellectual property. Moreover, this information is also subject to change and frequently will only reflect OEMs and tier 1 and possibly tier 2 suppliers. Will companies be required to resubmit every time an HBOM or SBOM changes for any reason? NFTC respectfully urges consideration of the utility and extent of information contained in BOMs as they relate to the national security concerns articulated in this proposed rule.

NFTC notes that the definition of VCS hardware is intended to capture items that are software-enabled or programmable. However, the NPRM contains examples of static VCS hardware like antennas and printed circuit boards, not all of which are software-enabled or programmable.

We strongly suggest that hardware and software must directly enable functionality in order to be captured by this rule and seek greater definitional clarity including specifying excluded items.

NFTC notes the ubiquity of software that has been developed by persons representing many nationalities including those from foreign adversaries. It is impossible to isolate pieces of code according to the nationality(ies) of the developer(s), particularly retrospectively. We note with appreciate BIS' Example 19, which concludes that a U.S. person who is a connected vehicle manufacturer working with VCS and ADS software developers around the world including those who are citizens of the People's Republic of China ("China" "PRC") and Russia would NOT meet the definition of a "person owned by, controlled by, or subject to the direction of a foreign adversary" and thus any sale of a completed connected vehicle in the U.S. using this software would also NOT be considered a Prohibited Transaction. We agree that the nationality of a natural person who is a direct employee of a connected vehicle manufacturer or an employee of a party in the supply chain including VCS and ADS, must not be the sole determining factor as to the applicability of any prohibition.

Declaration of Conformity

The NPRM proposes to implement a requirement at the time of entry to certify compliance through a Declaration of Conformity submitted to BIS by VCS hardware importers and connected vehicle manufacturers. The requirement for these declarations appears to be tied, in part, to the primary use of the connected vehicle being for passenger transport on public roads. This requirement seems to envision that the ultimate use of connected vehicles will be known at the time of manufacture and the use of hardware components in connected vehicles is known at the time of import. This will not always be the case. It is also concerning that BIS has indicated in the NPRM that it will not identify industry standards as informative or determinative in complying with the requirements of this NPRM. Identifying such standards could prove beneficial in demonstrating due diligence and reasonable care in the importation of subject products.

The importation of VCS hardware may not always be clearly intended for the use in a connected vehicle. One example might involve the importation of a Bluetooth transmitter that could be incorporated into a vehicle or a home audio system with wireless speakers. In either case, the involvement of PRC and/or Russian nationals in the development of source code and the development of firmware (including over-the-air updates that have not yet occurred) are almost unknowable to the level of certainty that seems to be envisioned by the Declaration of Conformity. Further, adding the requirement of a Declaration of Conformity or similar requirement at the time of entry for a finished connected vehicle is a burdensome administration of this requirement. NFTC seeks clarification on the requirements for a Declaration of Conformity for a connected vehicle to understand if there is a more efficient way to administer this rule.

Noting the important commitment in the NPRM to "*narrowly address, pursuant to E.O. 13873, the acute national security concerns posed by certain foreign adversary ICTS in connected vehicle supply chains while minimizing any unnecessary disruptions in manufacturing and trade*" BIS should give greater urgency and consideration to the impacts on industries other than VCS hardware importers and connected vehicle manufacturers. Many of the components identified as subject to Declaration requirements are closely related to components used in other industries. In addition to the Bluetooth example above, Wi-Fi and motion detector technology have uses in many applications. This pervasiveness of the technology identified as

subject to this proposed rule is derived from generations of iterative development in the global telecommunications industry. To avoid a deluge of advisory opinion requests related to import declaration requirements for products that may be within the scope of the NPRM as drafted, BIS should consider how it can clarify the applicability of this requirement for import purposes.

Recommendations

NFTC respectfully makes the following recommendations to more closely align the implementation of this rule to its stated national security objectives and provide greater clarity to affected industries:

1) Clarify the definition of "connected vehicles" within the context of this proposed rule to specifically exclude vehicles used primarily for agricultural or construction purposes.
2) Consult closely with industry to reach a more precise and actionable definition of "foreign interest". This would reduce variances in compliance activities across countries and would not degrade the national security objectives of this proposed rule.
3) Persons from allied countries and compliant and reliable trading partners should be exempt from the meaning of "foreign interest". NFTC also respectfully recommends further close consultation with industry to reach a more precise and actionable definition of "foreign interest".
4) Exclude business entities formed as Wholly Formed Foreign Entities (WOFEs) as well as employees of WOFEs who are citizens of foreign adversaries. Generally speaking, non-Chinese owner(s) exercise(s) substantial control and direction over the operations of the entity in China. Particularly in cases where a WOFE is formed to solidify supply chains for U.S.-domiciled automakers, it appears counterproductive to include this in the definition of a person subject to the jurisdiction of this proposed rule "any corporation, partnership, association, or other organization with a principal place of business in, headquartered in, incorporated in, or otherwise organized under the laws of a foreign adversary or country controlled by a foreign adversary". Additionally, as mechanisms exist to seek authorization to share controlled technical data including software, source and object code, with non-U.S. persons, we respectfully suggest that the OICTS expand coordination with other parts of BIS to provide similar authorizations for covered software and hardware. For example, this could be achieved through the creation of an authorization similar to a Validated End-User program that "whitelists" trusted suppliers including software development partners.
5) Incorporate the taxonomy used by SAE for L3, L4 and L5 in defining ADS. This would exclude lower levels of automation as defined by SAE's J3016 standard.
6) Delay the application of this proposed rule until at least 2030 (preferably later). While using the model year rather than the date of importation is helpful, a delay in the implementation date would facilitate compliance and an orderly transition. The supply chains of finished connected vehicles and their components, including VCS hardware, are long and involve many suppliers. In many cases, purchase orders for components and parts are placed several years before manufacturing of a particular model year vehicle begins.

NFTC greatly appreciates this opportunity to provide recommendations from across industry sectors affected by this proposed rule. We welcome opportunities to provide additional information and data as the OICTS continues to finalize this rule.

About NFTC

The NFTC, organized in 1914, is an association of U.S. business enterprises engaged in all aspects of international trade and investment. Our membership covers the full spectrum of industrial, commercial, financial, and service activities The NFTC supports open, rules-based trade, including a level and competitive playing field. Our goal is to protect national security and economic security interests and strengthen global supply chains critical to the U.S. competitiveness.

Robust trade relationships are central to economic and national security. NFTC's National Security Policy Initiative brings the voice of business to policymakers on global security issues affecting international trade. Companies play a vital role in promoting American values, including human rights and democracy. Our data driven recommendations support American competitiveness and technology leadership that is central to our national security.

Thank you again for this opportunity to comment on this NPRM. We welcome the opportunity to discuss this important matter and answer any questions that you may have regarding these comments or recommendations. I can be reached at (202) 887-0278 or via email at jchu@nftc.org.

Sincerely,

Jeannette L. Chu
Vice President for National Security Policy