Comments of the
Semiconductor Industry Association

On

The Proposed Rule Entitled
"Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles"

89 Fed. Reg. 79088 (September 26, 2024)
RIN 0694-AJ56
Docket No. 2024-21903

Submitted October 28, 2024

The Semiconductor Industry Association ("SIA") submits these comments in response to the request from the Bureau of Industry and Security ("BIS") within the Department of Commerce ("Commerce") in the Notice of Proposed Rulemaking ("NPRM" or the "Proposed Rule") to address the undue or unacceptable risks, as identified in Executive Order ("E.O.") 13873, posed by a class of transactions that involve information and communications technology and services ("ICTS") designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary and integral to Connected Vehicles ("CVs"), 89 Fed. Reg. 79088.

Part I contains introductory and background comments about SIA and semiconductors. Part II contains comments, questions, and requests about specific provisions in the Proposed Rule for BIS's consideration.

Part I – Introduction and Background

SIA has been the voice of the U.S. semiconductor industry for almost 50 years. SIA member companies represent more than 99% of the U.S. semiconductor industry by revenue and nearly two-thirds of non-U.S. firms, and are engaged in the research, design, and manufacture of semiconductors. The U.S. is the global leader in the semiconductor industry today. Continued U.S. leadership in semiconductor technology will drive economic strength, national security, and global competitiveness. More information about SIA and the semiconductor industry is available at https://www.semiconductors.org/.

Semiconductors are complex products critical to the functioning of everyday consumer electronics, communications, and computing devices in the automotive, industrial, financial, medical, retail, and many other sectors of the economy. They are also critical components for future technologies, such as artificial intelligence, quantum computing, and 5G/6G telecommunications.

As stated in both the House and Senate versions of the 2021 National Defense Authorization Act: "*The leadership of the United States in semiconductor technology and innovation is critical to the economic growth and national security of the United States*."[1] Given how important the economic vitality and competitiveness of the U.S. semiconductor industry is to national security, as a general matter, it is critical to ensure that any connected vehicle regulatory regime is narrowly tailored and designed to achieve specific, clearly articulated national security objectives. See E.O. 13874 (regulating transactions that pose "undue" or "unacceptable" risks to U.S. national security).

We appreciate that BIS has sought to "narrowly address the acute national security concerns posed by certain foreign adversary information and communications technology and services in connected vehicle supply chains while minimizing any unnecessary disruptions in manufacturing and trade." However, should the Proposed Rule be published without important clarifications to the scope of certain definitions and requirements, SIA member companies could face a significant increase in burdensome requirements that will increase their costs and reduce their global competitiveness. And, given that roughly 65 percent of annual auto chip demand involves chips of 90nm and above,[2] the additional burdens resulting from the Proposed Rule could disproportionately (though not exclusively) impact companies in the so-called "mature-node" or "legacy" chips segment – a segment that is already facing other pressures globally.

SIA and its member companies therefore appreciate the opportunity to provide comments, questions, and requests with respect to the Proposed Rule, and respectfully requests that BIS consider revising the NPRM on the basis of these comments.

Part II – Comments on Specific Provisions of the Connected Vehicle Proposed Rule

Comment II.A: BIS should narrow the definitions of "VCS Hardware" and "VCS Hardware Importer" under the Proposed Rule.

Under § 791.301 in the Proposed Rule, VCS hardware is defined as "software-enabled or programmable components and subcomponents that support the function of Vehicle Connectivity Systems or that are part of an item that supports the function of Vehicle Connectivity Systems: microcontroller, microcomputers or modules, systems on a chip, networking or telematics units, cellular modem/modules, Wi-Fi microcontrollers or modules, Bluetooth microcontrollers or modules, satellite navigation systems, satellite communication systems, other wireless communication microcontrollers or modules,

[1] H.R. 6395 § 1824(b) and S. 4049 § 1098(b).
[2] McKinsey & Company. (n.d.). *Will the supply-demand mismatch persist for automotive semiconductors?* McKinsey & Company. October 2022, from https://www.mckinsey.com/industries/industrials-and-electronics/our-insights/will-the-supply-demand-mismatch-persist-for-automotive-semiconductors

and external antennas." Furthermore, BIS notes in the NPRM that the definition of VCS hardware "would 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" [emphasis added].

It is important to note that a single chip can serve multiple purposes and can be incorporated into multiple systems within a vehicle or integrated into devices or systems in other end markets beyond automotive. For further clarity, the microelectronics components included in the definition of VCS hardware are not exclusive to VCS. For example, a "microcontroller or module" that can support a VCS system could also be incorporated into a wide variety of other vehicle systems such as vehicle charging or infotainment systems, and within systems incorporated into products sold in other end markets. In fact, in 2023, the automotive end market accounted for only 39.5 % of microcontroller unit (MCU) sales in the United States.[3] Bluetooth microcontrollers, for example, can be used for communication interface to infrastructure such as smart meters, surveillance cameras, or battery storage systems as well as for use in home automation sensors, appliances, power tools, and television remote controls. Similarly, general-purpose MCUs can be used across several different industries, including consumer electronics (e.g., fitness monitors and televisions), computers and peripherals (e.g., desktops and storage devices), communications (e.g., two-way radios and cordless phones), industrial applications (Internet of Things devices and robotics), as well as smart cards (e.g., SIM cards and bank cards).[4]

In addition, the inclusion in the VCS hardware definition of aftermarket devices "that could be" later integrated into or attached to the vehicle to perform VCS functions, as noted above, will likely pose a significant compliance challenge for chipmakers. Pursuant to § 791.305(b)(2), a VCS hardware importer is required to submit a Declaration of Conformity 60 days prior to the first import of VCS hardware for each model year for units associated with a vehicle model year, or calendar year for units not associated with a vehicle model year. This presumes that the ultimate use for connected vehicle systems will be known at the time of import, which is likely not the case given the multi-purpose use of chips, as referenced above.

The Proposed Rule also defines "*VCS hardware importer"* as "a U.S. person importing VCS hardware for further manufacturing, integration, resale, or distribution." However, as noted above, the components included in the definition are not [exclusively, or even primarily,] used in vehicle connectivity systems or vehicles as detailed above.[5] Given

---

[3] This figure is based on the annual value of MCU shipments in the Americas by end-use. Source: World Semiconductor Trade Statistics and SIA analysis.

[4] In 2023, global MCU sales were distributed by end-use as follows: automotive: 39.2%; industrial and other; 27.4%; smart cards: 15.4%; consumer goods: 9.3%; communications, 5.5%; and computers and peripherals: 3.2%. Source: World Semiconductor Trade Statistics and SIA analysis.

[5] Infotainment and ADAS systems accounted for approximately 35% of the MCU and general-purpose logic components used by the Americas automotive industry. Gartner, "Semiconductor Forecast 3Q-2024," September 24, 2024.

this, the definition of "*VCS hardware importer*" is likely to sweep in a range of entities/importers that intend to incorporate the covered components into systems not intended for integration into a vehicle, and therefore do not appear to be within the intended scope of the Proposed Rule.

Pursuant to § 791.305(a)(1) of the Proposed Rule, a VCS hardware importer may not import VCS hardware into the United States without first submitting a Declaration of Conformity to BIS. But, as explained above, this requirement will impact a much broader set of transactions than BIS likely intended given the wide range of non-vehicle applications of the components included in the VCS hardware definition. These requirements will flow down to SIA member companies and could cause significant disruptions to the automotive supply chain, including reduced supply of compliant hardware components to dealers and consumers.

SIA therefore requests that BIS narrow the scope of 1) the definition of "VCS hardware" in § 791.301 to include only those components that "directly enable" the functioning of VCS and 2) the definition of "VCS hardware importer" to ensure that only those companies that import covered hardware for incorporation into a VCS and not other end applications, including aftermarket devices, are subject to the compliance requirements pursuant to § 791.305(a)(1). We also recommend that the definition of VCS Hardware should be limited to components "in which there is a foreign interest" to be consistent with the definition of "covered software".

Comment II.B: The proposed requirement for VCS hardware importers to submit a Hardware Bill of Materials as part of a Declaration of Conformity creates risk to proprietary and business confidential information.

As noted above, before importing *any* VCS hardware into the United States, VCS hardware importers are required to submit a Declaration of Conformity, which must include a Hardware Bill of Materials ("HBOM") comprised of a comprehensive list of parts, assemblies, documents, drawings, and components required to create a physical product, including information identifying the manufacturer, related firmware, technical information, and descriptive information.

As detailed in SIA's comments[6] in response to Federal Acquisition Regulation ("FAR") Case 2023-008, titled *Prohibition on Certain Semiconductor Products and Services*, 89 Fed. Reg. 36738 (May 3, 2024), semiconductor companies consider information about their supply chain – including materials suppliers and other vendors – as sensitive information and intellectual property, and have expressed serious concern about providing such business proprietary information – to their customers, who may also be their competitors, or distributors that also serve their direct competitors.

[6] Comments of the Semiconductor Industry Association (SIA) on "Prohibition on Certain Semiconductor Products and Services," (89 Fed. Reg. 36738 (May 3, 2024)), August 1, 2024, https://www.regulations.gov/comment/FAR-2023-0008-0014.

How would proprietary and confidential business information be protected? The protection of intellectual property and other business confidential information is essential to U.S. technological advantage and continued semiconductor competitiveness. As a result, we encourage BIS to ensure the rule clearly articulates federal requirements for each agency to protect and limit the dissemination of business confidential information.

Comment II.C: BIS should narrow the definition of "foreign interest" to clarify the scope of covered software and limit the scope of VCS hardware.

Under § 791.301 of the Proposed Rule, "covered software" is defined to mean "the software-based components, **in which there is a foreign interest,** executed by the primary processing unit of the respective systems that are part of an item that supports the function of Vehicle Connectivity Systems or Automated Driving Systems at the vehicle level." [emphasis added] "Foreign interest" is in turn defined as "any interest in property, of any nature whatsoever, whether direct or indirect, held by a non-U.S. person." BIS explains that foreign interest "can include, but is not limited to, an interest through ownership, intellectual property, contract – e.g., ongoing supply commitments such as maintenance, any license agreement related to the use of intellectual property – profit-sharing or fee arrangement, as well as any other cognizable interest." According to the supplementary information section of the NPRM, this definition is intended to be consistent with the definition of "interest" used in the context of OFAC sanctions.

Further, Section § 791.303 of the Proposed Rule prohibits the knowing import or sale in the United States of completed connected vehicles that incorporate covered software, designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of China or Russia. Pursuant to § 791.305(a)(2) and (a)(3) of the Proposed Rule, a connected vehicle containing covered software cannot be imported or sold as part of a transaction that is not otherwise prohibited unless the connected vehicle manufacturer submits a Declaration of Conformity to BIS.

Read broadly, this application of "foreign interest" could include a U.S. headquartered company's in-house engineer team that is operating, and developing code, in a country that is a partner or ally of the United States. Does BIS intend to exempt or carveout from the proposed regulations in-house staff such as engineering teams that work for a U.S. headquartered company but are located in an allied or partner country, and ensure that these same employees would not be treated differently than what is currently captured in deemed export rules and license procedures? Are these in-house engineering teams also considered to have an "interest in the property" solely based on their development of the code as part of their job responsibilities and duties?

To help minimize the compliance burden without compromising the national security goals of the rule, we recommend that the "foreign interest" definition be modified such that an interest in the software held by a foreign person or foreign entity that has no cognizable legal interest would not fall within the meaning of a foreign interest, severing

any link to the broad definition adopted by OFAC, for a very different context. 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, as noted above, 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.

We further encourage BIS to consider excluding wholly owned subsidiaries of U.S. companies and employees of such subsidiaries.

Comment II.D: BIS should clarify that legacy software code developed prior to the effective date of the Connected Vehicle Proposed Rule is not prohibited.

The technology that the Proposed Rule seeks to regulate is inextricably linked to technology primarily developed for other use cases, such as mobile cellular communications, implicating inestimable lines of historical code worked on by engineers across the globe that remain 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 globally by software engineering teams from around the world, including from China, and built on top of legacy code developed for other use cases. It is important to note that the involvement of China-based engineers in the development of mobile hardware and software reflects the realities of the mobile communications industry more broadly. China is the world's largest mobile market, with 70% of the world's mobile phones made in China. China is also the largest single-country end market for mobile phones. In addition, mobile technology is based around global standards for a global market, so that, for example, a U.S. mobile device can function in China and vice versa.

As such, the global nature of software development and industry's reliance on existing legacy code – including code developed, for example, by a Chinese citizen with a valid permanent residence in the U.S. – will likely create significant compliance challenges with respect to the Proposed Rule's definition of covered 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 Proposed Rule neither defines nor considers the reliance on legacy code as part of a connected vehicle's system, and associated compliance challenges it would impose on companies, we encourage BIS to clarify that legacy software code is not prohibited under the Proposed Rule.

Comment II.E: BIS should develop a preclearance procedure to ensure auto manufacturers and suppliers have advance approval for continued use of certain covered software, with appropriate risk mitigation.

As discussed above in Comment II.D, because the automotive industry relies on this legacy software code designed for non-automotive use cases, even a temporary delay in receiving a specific authorization to use certain legacy code in automotive applications could have significant impacts on semiconductor company operations.

For the proposed specific authorization process to be effective, such authorizations must be made at least three to four years before any newly designed model year vehicle enters production. Semiconductor suppliers that produce VCS hardware, which, as discussed above, can be sold into many other end market verticals, cannot be expected to invest in designing and developing automotive chips years before newly designed vehicles enter the market for sale without certainty that their products will be permitted in the U.S. market.

We therefore encourage BIS to establish a process for companies to obtain preclearance for certain covered software items, such as base code that is not specifically designed or developed for automotive applications. Sufficient time must be built into the final rule so that pre-clearance can be granted before any prohibitions may impact the broader market.

Comment II.F: BIS should extend the timeline for auto manufacturers and their suppliers to implement software and hardware restrictions.

A new connected vehicle model, on average, takes about four to five years to develop from ideation to vehicle launch, though sometimes longer. Auto OEMs and their Tier 1 suppliers typically make supply chain and technology sourcing decisions years *before* a particular model year vehicle is set to enter production, and decisions by manufacturers and suppliers about what technologies and features to pursue and which vendors to select must therefore occur at least four or five years before a particular model year vehicle is set to enter production. Further, the automotive product development cycle does not permit late changes in suppliers, components, or systems because any such changes require new rounds of testing, validation, and certification.

In other words, the timeframe during which a connected vehicle manufacturer could change its VCS or ADS software supplier or system, while still achieving its intended start of regular production in accordance with the proposed implementation timeline under the Proposed Rule, has already passed. The Proposed Rule, if implemented as drafted, would require impacted manufacturers to identify new suppliers, negotiate new contracts, and potentially redesign software and hardware to meet the same performance specifications, while ensuring compliance with the broad prohibitions.

Most automotive manufacturers source semiconductor components to be integrated into a new model year vehicle three to four years before manufacturing production begins to build in enough time to integrate and validate components at the vehicle level.

In addition, vehicle models do not generally undergo major redesigns or architecture changes every model year. Rather, it is only once every four to six years that a manufacturer will undertake a major redesign of a specific vehicle model. Major redesigns are when vehicle models are completely or nearly completely reengineered. In the interim, a particular vehicle model will only experience minor refreshes, which includes smaller changes such as updated headlights, new wheel designs, or new paint color options. Technologies and suppliers remain largely unchanged when a vehicle model undergoes a refresh and software in such vehicles must continue to be supported and maintained.

To avoid substantial industry disruption, we encourage BIS to extend the timeline for software and hardware restrictions to begin for hardware and software at least an additional 2 years following the effective date of the rule, to ensure the U.S. connected vehicle industry has adequate time to transition their supply chains and comply with the rule.

* * *

Thank you for the opportunity to comment on the Proposed Rule. SIA looks forward to continued partnership with BIS and other agencies in providing support and feedback.

Uploaded to www.regulations.gov. ID – BIS-2024-0005-0059