KIRKLAND & ELLIS

Kirkland Alert

Bureau of Industry and Security Proposes Rulemaking Impacting Importation and Sale of Hardware and Software for Connected Vehicles with a Nexus to China and Russia

06 November 2024

Introduction

On September 26, 2024, the U.S. Department of Commerce's Bureau of Industry and Security ("BIS"), Office of Information and Communications Technology Services ("ICTS") published a Notice of Proposed Rulemaking ("Proposed Rule") regarding sweeping new restrictions on imports of Vehicle Connectivity System ("VCS") hardware and vehicles incorporating such hardware, and imports and sales of connected vehicles incorporating covered VCS and/or Automated Driving Systems ("ADS") software. This Proposed Rule follows BIS's Advance Notice of Proposed Rulemaking ("ANPRM"), dated March 1, 2024, and demonstrates the muscularity of the ICTS authorities granted to BIS.

The Proposed Rule may significantly alter automotive and vehicle technology and supply chains, encourage automotive sectoral U.S. decoupling from China and Russia, and create substantial compliance hurdles for automakers and associated industries.

We summarize the key aspects of the Proposed Rule as follows: (i) the rationale and scope of the restrictions; (ii) key definitions; (iii) the four prohibitions on VCS and ADS technology; (iv) compliance and exemptions; and (v) key takeaways from the Proposed Rule.

Comments on the Proposed Rule were due October 28, 2024, and can be found at https://www.regulations.gov/document/BIS-2024-0005-0059/comment.

Rationale and Scope of Restrictions

VCS and ADS are key efficiency and safety advances in surface transportation. Further, they are increasingly ubiquitous components of modern vehicles — so-called *connected vehicles* — commonly known as "smart cars" in the passenger vehicle context. With the rise of complex driver assistance and autonomous vehicles, BIS sees VCS and ADS as potential threat vectors for foreign adversaries seeking digital or physical control of these devices. VCS and ADS exercise control over basic mechanical functions in vehicles from ignition to braking. Malicious interference with their functionality could disable or damage a vehicle in transit. Additionally, intervehicle communications and sensing are governed through these systems. Vehicle data exfiltration could yield a trove of information about U.S. drivers and their environments. Therefore, VCS and ADS susceptibility to foreign interference may pose threats to the integrity and safety of U.S. transportation infrastructure and U.S. citizens, especially in the event of infrastructural cyberattacks under conditions of Great Power Competition.

The purported objective of the Proposed Rule is to isolate connected vehicles from potential Chinese or Russian influence or control for national security reasons.

Significantly, BIS admits, with "very few exceptions, all new vehicles sold in the United States will fall under its "connected vehicles" definition. McKinsey estimates that 95 percent of new vehicles will be "connected" by 2030. Connected vehicles rely on "vehicle-to-everything" ("V2X") communications such as "short-range communication, cellular telecommunications connectivity, satellite communication, or other wireless spectrum connectivity with any other network or device" for enhanced safety and mobility. Autonomous vehicles, for example, rely on this technology to communicate with their surroundings and with other vehicles. Major automakers continue to integrate more V2X technology across many vehicle classes.

Key Definitions

Connected Vehicles and Connected Vehicle Manufacturers

After some narrowing attributed to initial comments on the ANPRM, BIS defines "connected vehicle" (still broadly) as:

> [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, and other wireless spectrum connectivity with any other network or device.

This expansive category captures most surface transportation vehicles, such as passenger vehicles, motorcycles, buses, small and medium trucks, class 8 commercial trucks, and recreational vehicles. BIS currently excludes rail line vehicles ("rolling stock"), unmanned aerial vehicles, and (likely) new agricultural vehicles, such as tractors, which rely heavily on V2X.

Meanwhile, "connected vehicle manufacturers" include U.S. persons either assembling/manufacturing completed connected vehicles in the U.S. or importing such vehicles into the U.S. for sale.

Covered VCS and ADS

The Proposed Rule prohibits transactions involving two main categories of VCS/ADS components/technologies: software and hardware. VCS refers to either a "hardware or software item for a completed vehicle that has the function of enabling the transmission, receipt, conversion, or processing of radio frequency communications at a frequency over 450 megahertz."

ADS are solely software-focused. Specifically, BIS aligns its ADS definition with Level 3, 4 and 5 systems as defined by regulatory and industry standards NHTSA and SAE J3016, focusing on more advanced systems with autonomous capabilities.

- **Covered Software: VCS and ADS**. BIS defines "covered software" as "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 VCS or ADS at the vehicle level." BIS includes "machine learning software" if part of the ADS, while excluding open-source software. It states that a principal rationale for software restrictions is the "persistent connectivity" of VCS and ADS as well as their "essential functions" for vehicle operation.

Here, BIS essentially imports the Office of Foreign Asset Control's broad "interest in property" definition for purposes of assessing whether there is "foreign interest" in covered software, meaning that a "foreign interest can include, but is not limited to, an interest through ownership, intellectual property, contract . . . as well as any other cognizable interest."

- **Covered Hardware: VCS Only**. The Proposed Rule includes only VCS, rather than ADS, hardware in the scope of the Proposed Rule. VCS hardware is defined to include the following 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, and external antennas. BIS has determined that aftermarket telematics devices, including fleet tracking devices and systems, that fulfill functions consistent with the definition of VCS hardware also are covered.

  VCS hardware importers are expected to include "OEMs [original equipment manufacturers] and tier 1 and tier 2 suppliers importing VCS hardware into the United States," including imports of connected vehicles with VCS hardware already installed.

Persons Owned by, Controlled by, or Subject to the Jurisdiction or Direction of Foreign Adversary

BIS has taken an expansive view of the persons and entities that might trigger the below-described restrictions. Specifically, BIS has defined "Persons Owned by, Controlled by, or Subject to the Jurisdiction or Direction of Foreign Adversary" as:

- any person, wherever located, who acts as an agent, representative, or employee, or 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 part by a foreign adversary;

- any person, wherever located, who is a citizen or resident of a foreign adversary or a country controlled by a foreign adversary, and is not a U.S. citizen or permanent resident of the U.S.;
- 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 a country controlled by a foreign adversary; or
- any corporation, partnership, association or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary, to include circumstances in which any person identified in any of the aforementioned bullet points possesses the power, direct or indirect, whether or not exercised, through the ownership of a majority or a dominant minority of the total outstanding voting interest in an entity, board representation, proxy voting, a special share, contractual arrangements, formal or informal arrangements to act in concert, or other means, to determine, direct, or decide important matters affecting an entity.

For example, if a U.S. corporation is a "wholly owned subsidiary" of a Chinese or Russian state-owned enterprise or state-owned investment funds, then the U.S. corporation would be "considered 'owned by'" China or Russia, respectively. Further, if a U.S. corporation is a subsidiary of a *private* company incorporated in China or Russia with its principal place of business in either of those countries, then the U.S. corporation would be considered "controlled by" and "subject to the direction of" China or Russia. In addition, wholly owned subsidiaries of U.S companies that are organized in China or Russia are considered to the "subject to the jurisdiction of" China or Russia, respectively. Finally, the sweep of the BIS designation extends far beyond a traditional parent-subsidiary relationship. BIS explains, for example, that even a one percent special management share held by the Chinese or Russian government, if it grants directorship or veto rights, is sufficient to establish that the firm is "controlled by" either China or Russia. In this way, the Proposed Rule features CFIUS-type control concepts. While the Proposed Rule does not specifically address private equity funds and the participation of the persons described above as limited partners in private funds, we expect that a case-by-case assessment of any control or governance rights afforded to such investors will be required to assess whether the fund and/or its portfolio companies might be considered to be "controlled by" or "subject to the direction of" a foreign adversary.

Expansive Sweep of Definitional Coverage

Thus, the Proposed Rule covers: (i) almost all vehicles; and (ii) almost all corporate connections to China or Russia.

Four Prohibitions

The Proposed Rule identifies four main categories of prohibited activities:

- **First**, the Proposed Rule prohibits VCS hardware importers from importing covered VCS hardware, including as integrated into a completed connected vehicle. This includes VCS hardware "designed, developed, manufactured, or supplied by persons subject to the jurisdiction or direction" of China or Russia.
- **Second**, the Proposed Rule prohibits manufacturers of connected vehicles from "knowingly importing into the United States completed connected vehicles" that incorporate covered VCS and ADS software.
- **Third**, the Proposed Rule prohibits connected vehicle manufacturers from "knowingly [s]elling" any completed connected vehicles that incorporate "VCS hardware or covered software." This prohibition applies "even if the vehicle was made in the United States."
- **Fourth**, the Proposed Rule prohibits any connected vehicle manufacturers "owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia" from selling completed connected vehicles with VCS hardware or covered software in the U.S.

The Proposed Rule could affect domestic U.S. concerns of OEMs or automakers with partial or complete Chinese or Russian ownership, not just the importation of overseas-originated VCS and ADS technology for assembly in the U.S. This provision applies even if the Chinese- or Russian-affiliated manufacturers are "not involved in the design or development of the VCS Hardware and Covered Software," but merely built the vehicles.

Functionally, the Proposed Rule advances a quasi-prohibition on the importation of completed Chinese and Russian vehicles containing Chinese or Russian VCS and ADS technology and partial decoupling in the automotive market.

Compliance

The Proposed Rule includes three compliance mechanisms: (i) **Declarations of Conformity**; (ii) **general authorizations**; and (iii) **specific authorizations**.

- **Declarations of Conformity** include a yearly certification to BIS that the submitter has not engaged in any prohibited transactions as well as providing information on the import of VCS hardware and/or import or sale of completed connected vehicles. Declarations also are to include "technical information regarding the hardware or software in question and a Bill of Materials for applicable software, hardware, or both."
- **General authorizations** are available for VCS hardware importers and/or connected vehicle manufactures seeking to engage in otherwise prohibited transactions. These are narrow and include justifications for testing or for driving limited to fewer than thirty calendar days.
- **Specific authorizations** permit case-by-case determinations on VCS hardware and covered software if the otherwise prohibited transaction "does not present an undue or unacceptable risk to U.S. national security." Specific authorizations require "ISO/SAE 21434 Threat Analysis and Risk Assessments" to ascertain applicant ability to, amongst others, "limit PRC or Russian government access to, or influence over the design, development, manufacture or supply of the VCS hardware or covered software…." BIS may also require additional mitigation measures.

Bills of Materials ("BOM")

The Proposed Rule requires comprehensive, onerous BOMs to meet compliance standards under the Declarations of Conformity, which may prove difficult to obtain from unaffiliated suppliers.

- The Hardware BOM includes extensive lists of assemblies, components and parts for the creation of a physical product, including firmware, technical information and descriptive information.
- The Software BOM is a "formal and dynamic, machine-readable inventory" explaining software supply chain relationships and software dependencies in detail.

Key Takeaways

- **This Proposed Rule to regulate and prohibit automotive technology imports is part of BIS's heightened emphasis on ICTS supply chain security**. BIS's June

2024 ban of Kaspersky Lab antivirus and cybersecurity products was its first ICTS Final Determination. This follows BIS's establishment of an ICTS Transaction review process in January 2021. The Department of Commerce has stepped up its scrutiny of information and communications transactions in light of Executive Orders 13873 in 2019 and 14034 in 2021, which focused attention on data and software security. The current Proposed Rule may augur more ICTS-driven BIS action in non-traditional-technology sectors. Further, the Proposed Rule is consistent with recent efforts to excise adversarial parties from critical supply chains, including pertaining to telecommunications network equipment and biologics/pharmaceuticals.

- **The Proposed Rule also has a political valence**. Congress has expressed concern over automotive-related national security matters. Recently, several members of Congress sent a letter to the new president of Mexico, Claudia Sheinbaum Pardo, expressing concern over the expanding presence of Chinese automakers in Mexico. As it prepares for revisions to the USMCA, the Mexican government has noted and voiced some similar concerns over Chinese imports, though more recently has suggested that the Proposed Rule violates the USMCA. Domestically, the anticipated renegotiation of the USMCA prompted the United Auto Workers to seek higher tariffs on passenger cars and parts from the Biden Administration. It is unclear what effect the results of the U.S. election may have on the development of final rules, but several major vehicle manufacturing states — such as Michigan — and UAW strongholds are key electoral battlegrounds and the next president is not likely to encourage any action that could be construed as weakening the proposed restrictions.
- **Violators could be subject to serious civil or even criminal penalties under the International Emergency Economic Powers Act ("IEEPA")**. Under the IEEPA, civil and criminal penalties are available for violations. The maximum civil penalty currently is the greater of $368,136 or twice the value of the underlying transaction (subject to annual inflationary adjustments). The maximum criminal penalty is a fine of $1 million and/or 20 years imprisonment. BIS may also issue administrative responses to violations such as a cease-and-desist order. Interestingly, BIS has proposed an advisory opinion mechanism to enable parties to obtain pre-transaction clarifications regarding the applicability of the rulemaking but has not established a post-transaction voluntary disclosure mechanism as exists for export controls and sanctions compliance matters (most sanctions regimes, for example, are IEEPA-authorized).
- **BIS signals increasing regulatory convergence between low-sensitivity manufactured goods and sensitive high-technology goods due to networking and the Internet of Things**. As this Proposed Rule indicates, interconnectivity between devices prompts national security concerns. In 2023, the U.S. imported $426 billion in goods from China. The top two categories were electrical/electronic

equipment and machinery. More than ever, U.S. and global firms will need to consider how intensified U.S. restrictions against information and communications technology from China in particular will implicate an increasing swathe of bilateral trade in manufactured goods.

- **Proposed Effective Date**. The Proposed Rule states that prohibitions for software systems will take effect for Model Year 2027. Prohibitions on hardware would take effect for Model Year 2030, or January 1, 2029, if the vehicle units lack a model year. Notwithstanding these elongated affective dates, which are referred to as exemptions in the Proposed Rule, given the complexity of global automotive supply chains measures should be taken in the near term to assess supply chains and remediate potential risks.

Related Professionals

Zachary S. Brez, P.C.

Partner / New York

Cori A. Lable, P.C.

Partner / Los Angeles – Century City

Kim B. Nemirow, P.C.

Partner / Chicago

Ivan A. Schlager, P.C.

Partner / Washington, D.C.

Daniel J. Gerkin

Partner / Washington, D.C.

Jodi Wu

Registered Foreign Lawyer (Kirkland & Ellis, Hong Kong) and Partner (Kirkland & Ellis LLP, U.S.) / Hong Kong

Nick Niles

Partner / Chicago

Weng Keong Kok

Registered Foreign Lawyer / Hong Kong

Joe Kiernan

Associate / Dallas

Related Services

Practices

- International Trade & National Security
- Government, Regulatory & Internal Investigations

Suggested Reading

- 15 November 2024 Award Kirkland Recognized in GIR 30 2024
- 07 November 2024 Award Three Kirkland Partners Named to Securities Docket's Enforcement Elite 2024
- 04 November 2024 Press Release Kirkland Counsels Pelican Energy Partners on Final Closing of Oversubscribed Inaugural Nuclear Energy Fund