Morgan Lewis

REPORT

SMARTPHONES ON WHEELS

COMMERCE ISSUES GAME-CHANGING FINAL RULE ON SECURING THE ICTS SUPPLY CHAIN IN CONNECTED VEHICLES

FEBRUARY 2025

SMARTPHONES ON WHEELS: COMMERCE ISSUES GAME-CHANGING FINAL RULE ON SECURING THE ICTS SUPPLY CHAIN IN CONNECTED VEHICLES

The US Department of Commerce's Bureau of Industry and Security (BIS) published a Final Rule on January 16, 2025 that prohibits the import, sale, and manufacture of vehicles equipped with Vehicle Connectivity System (VCS) or Automated Driving System (ADS) hardware and software that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of nations identified as "foreign adversaries" by the Final Rule, which includes China and Russia. The Final Rule, as crafted, will significantly impact entities up and down connected vehicle supply chains that fall within the definitions of VCS Hardware importers and/or Connected Vehicle Manufacturers. These regulated entities may include legacy automakers, technology companies, and component suppliers of VCS Hardware and Connected Vehicle systems.

This Final Rule follows a Notice of Proposed Rulemaking (NPRM) published on September 26, 2024, an Advance Notice of Proposed Rulemaking (ANPRM) issued on March 1, 2024, and consideration of robust public comments by BIS. The Final Rule was slated to take effect in 60 days from issuance, or approximately March 17, 2025. However, on January 20, 2025, President Donald Trump signed a Presidential Memorandum titled Regulatory Freeze Pending Review. This Regulatory Freeze is effective through approximately March 24, 2025, and therefore will likely cause a slight delay in the effective date of the Final Rule. All indications suggest, however, that the Final Rule is likely to be adopted in its current form after the Regulatory Freeze ends. Notably, the original Information and Communications Technology and Services (ICTS) Executive Order—which was a major catalyst for the issuance of the Final Rule and forms the jurisdiction basis of the Final Rule—was issued by President Trump in 2019. Since then, bipartisan support for safeguarding perceived threats to US citizens' personal data and national security concerns stemming from connected technologies has grown in strength. In addition, on January 20, 2025, President Trump signed the America First Trade Policy Presidential Memorandum, which among other things directs the secretary of commerce to explore the possibility of extending the ICTS directive to other consumer products with connected technologies and that pose similar national security risk.

This report summarizes the Final Rule's primary prohibitions, key definitions, compliance pathways for regulated entities, the exemptions, advisory opinions, "is-informed" notices, appeals, and finally our views on the road ahead for the connected vehicle industry.

PROHIBITED TRANSACTIONS

BIS adopted the following prohibitions for transactions involving VCS Hardware or Covered Software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a "foreign adversary," as used in the Final Rule, which includes China and Russia:

- The knowing importation of certain VCS Hardware into the United States by VCS Hardware importers (Section 791.302, "Prohibited VCS hardware transactions")
- The knowing sale within the United States, or importing into the United States, by Connected Vehicle Manufacturers of completed connected vehicles that incorporate Covered Software (Section 791.303, "Prohibited covered software transactions")
- The knowing sale in the United States, by Connected Vehicle Manufacturers who are persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign

adversary, of completed connected vehicles that incorporate VCS Hardware or covered software (Section 791.304, "Related prohibited transactions"), regardless of whether such VCS Hardware or covered software is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary

Prohibited Covered Software transactions will take effect with Model Year (MY) 2027. Prohibited VCS Hardware transactions will begin with MY 2030 or by January 1, 2029, for units without a designated model year. Restrictions on the sale of connected vehicles by manufacturers linked to China, Russia, or other foreign adversary nations will also take effect with MY 2027. As addressed below, there are recordkeeping requirements with respect to Declarations of Conformity (discussed below) as well as compliance pathways for general and specific authorizations where technology may meet the prohibition standards but does not raise the national security concerns that underlie the Final Rule's issuance.

KEY DEFINITIONS FOR REGULATED ENTITIES, TECHNOLOGIES, AND TRANSACTIONS

BIS retained most of the NPRM's definitions in the Final Rule, including those for "Automated Driving System," "Completed Connected Vehicles," and what constitutes "knowingly." Responding to certain of the automotive industry's comments, however, BIS made some key definitional modifications and/or provided further clarification on the requirements of other terms.

Person Owned By, Controlled By, or Subject to the Jurisdiction or Direction of a Foreign Adversary

This definition covers "(1) Any individual acting under the direction or control of a foreign adversary or its affiliates; (2) Any non-U.S. citizen or non-permanent resident from a foreign adversary or its controlled country; (3) Any organization headquartered, incorporated, or primarily operating in a foreign adversary's jurisdiction; and (4) Any entity, regardless of location, that is owned or controlled by a foreign adversary through voting power, board influence, contractual arrangements, or other means."

Key Amendments from NPRM to Final Rule:

- BIS added more examples to the definition to better illustrate scenarios where entities are determined to be "owned by," "controlled by," or "subject to the jurisdiction or direction of a foreign adversary."
- These hypotheticals include direct ownership by state-owned enterprises, joint ventures with dominant voting power held Chinese or Russian entities, and indirect control through board members with ties to foreign governments. The examples also highlight how certain corporate structures, such as voting shares or veto powers, enable influence over critical decisions, thereby subjecting entities to foreign jurisdiction and control or direction.
- Importantly, these examples clarify that the involvement of China or Russian citizens alone does not automatically classify an entity as foreign-controlled if those individuals operate outside of China or Russia. BIS emphasizes that its approach accounts for nuanced relationships beyond simple ownership thresholds, focusing instead on continuous and substantive control or influence that poses national security risks.

Requirements for Regulated Entities:

- This definition and its examples are paramount to determine whether a manufacturer or supplier of connected vehicle technologies falls within the purview of the Final Rule and requires a detailed factual analysis of the entity's organizational structure and ownership team by experienced counsel.

Vehicle Connectivity System

VCS is defined to mean a "hardware or software item installed in or on a completed connected vehicle that directly enables the function of transmission, receipt, conversion, or processing of radio frequency communications at a frequency over 450 megahertz."

Key Amendments from NPRM to Final Rule:

- BIS amended the definition of VCS to explicitly exclude certain low-risk use cases, including automotive sensing functionalities such as LiDAR, radar, cameras, ultrawideband; GNSS; and satellite, AM, and FM radio.
- BIS declined to exclude all convenience functions (e.g., garage door opening or rear seat entertainment) given the difficulty in adequately defining this exemption to address only convenience functions rather than communications functions that present undue risk.
- BIS also added several functional exclusions, most notably unidirectional communication systems.

Requirements for Regulated Entities:

- Manufacturers or importers of VCS technologies, which have sufficient connections to foreign adversary nations, must ensure compliance with the Final Rule by following one of the three designated compliance pathways (discussed below), if their products include hardware and software that enable the localization of a device intended to control vehicle functions, as the vehicle-side hardware and software of that function presents a possible threat vector that could enable the national security risks addressed out in the rule.
- BIS concedes that "the requirements of this regulation may create new compliance burdens," but states that "those requirements seek to ensure automotive supply chain security, which will help secure the future of V2X technology implementation."

VCS Hardware

VCS Hardware is defined to mean "software-enabled or programmable components if they directly enable the function of and are directly connected to VCS, or are part of an item that directly enables the function of VCS, including but not limited to: 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 communication systems, other wireless communication microcontrollers or modules, external antennas, digital signal processors, and field-programmable gate arrays."

Key Amendments from NPRM to Final Rule:

- BIS clarified that VCS Hardware no longer includes component parts that do not contribute to the communication function of VCS Hardware (e.g., brackets, fasteners, plastics, and passive electronics, diodes, field-effect transistors, and bipolar junction transistors).

Requirements for Regulated Entities:

- Manufacturers or importers of VCS technologies, which have sufficient connections to foreign adversary nations, must comply with the Final Rule if their products include software-enabled or programmable components that directly enable the function of VCS, or are part of a component that directly enables the function of VCS.
- VCS Hardware includes, but is not limited to, microcontrollers, microcomputers or modules, systems on a chip, networking or telematics units, cellular modems, Wi-Fi, Bluetooth, satellite communication systems, other wireless communication modules, external antennas, digital signal processors, and field-programmable gate arrays.

Covered Software

Covered Software is defined to mean "software-based components, including application, middleware, and system software, in which there is a foreign interest, executed by the primary processing unit or units of an item that directly enables the function of Vehicle Connectivity Systems or Automated Driving Systems at the vehicle level. Covered software does not include firmware, which is characterized as software specifically programmed for a hardware device with a primary purpose of directly controlling, configuring, and communicating with that hardware device."

Key Amendments from NPRM to Final Rule:

- BIS clarified that if a single software subcomponent of an ADS software suite involves an interest by China, Russia, or other foreign adversary nations, the entire software suite is considered to involve an interest by the foreign adversary nation.
- BIS excluded legal code—software designed, developed, manufactured, or supplied more than one year before the Final Rule's effective date—from the Covered Software definition. However, BIS declined to adopt a de minimis threshold approach to assess software containing code form prohibited foreign entities.
- The term "item" has been added to this definition to align with industry standards-setting organizations, which use "item" as a scoping boundary for analyzing automotive systems in cybersecurity and functional safety assessments (e.g., ISO 21434, ISO 26262).

Requirements for Regulated Entities:

- To determine whether particular embedded software is excluded from the definition, market participants must consider whether the embedded software leverages specific code executed by the primary processing unit or units of the system. This requirement may exclude embedded software systems that are executed on ancillary surface modules or processors, depending on the specific architecture of the VCS.
- If a manufacturer fully owns software purchased from a prohibited supplier, BIS can issue an advisory opinion to determine whether such a software purchase may adequately mitigate the identified risk (assuming the transaction is not otherwise excluded by the modified definition of Covered Software).

Connected Vehicle

A Connected Vehicle is defined to mean "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."

Key Amendments to the Final Rule:

- Importantly, the Final Rule excludes vehicles with a gross vehicle weight (GVWR) over 10,000 pounds from the definition. Recreational vehicles (RVs) exceeding this weight threshold are also excluded and will instead be addressed in a future rule for commercial vehicles.
- Agricultural, construction, and mining equipment are generally exempt if they are not primarily designed for use on public roads and weigh under 10,001 pounds.
- Personal Delivery Devices, bicycles, e-scooters, and e-bikes are also excluded, while motorcycles are classified as Connected Vehicles.

Requirements for Regulated Entities:

- Manufacturers or importers of Connected Vehicles must ensure compliance with the Final Rule, by following one of the three designated compliance pathways (discussed below), if their vehicles fall within the definition of Connected Vehicle.
- Vehicles operated only on a rail are not included in this definition.

Connected Vehicle Manufacturer

A Connected Vehicle Manufacturer is defined to include a US person that "(1) Manufactures or assembles a Completed Connected Vehicle in the United States and for sale in the United States; (2) Imports Connected Vehicles for sale in the United States; and/or (3) Integrates ADS Software on a Completed Connected Vehicle for sale in the United States."

Key Amendments from NORM to Final Rule:

- BIS clarified that ADS integration installed in a completed Connected Vehicle is subject to the prohibitions in the Final Rule.

Requirements for Regulated Entities:

- Connected Vehicle Manufacturers can also qualify as VCS Hardware importers if the VCS Hardware is already installed in the Connected Vehicle when the Connected Vehicle Manufacturer imports their products into the United States.
- Entities that purchase otherwise completed (and compliant) Connected Vehicles from a third party and then integrate their proprietary ADS into them and enable various levels of autonomous driving are also explicitly captured under the definition.

Hardware Bill of Materials (HBOM)

HBOM means "a formal record the supply chain relationships of parts, assemblies, and components required to create a physical product, including information identifying the manufacturer, and related firmware."

Key Amendments from NPRM to Final Rule:

- BIS modified this definition to exclude documents, drawings, technical information, and descriptive information from the definition of HBOM because they do not strictly fall under the scope of a bill of materials. BIS also replaced the term "comprehensive list" with "formal record," because "record" is a more general term.
- BIS further clarified that:
  - BIS will not require the submission of HBOMs as part of Declarations of Conformity.
  - BIS will require entities to keep primary business records related to their certification that due diligence was conducted in analyzing their VCS Hardware supply chains, which could include HBOMs.
  - BIS also included a section in the Final Rule dedicated to the submission of Confidential Business Information (CBI), which would cover the submission of HBOMs.

Requirements for Regulated Entities:

- HBOMs are no longer required as part of Declarations of Conformity. However, BIS still requires entities to maintain primary business records related to their certification that due diligence was conducted in analyzing their VCS hardware supply chains, which could include HBOMs. These primary business records must be maintained for a period of 10 years and be made available to BIS upon request.

Software Bill of Materials (SBOM)

SBOM is defined to mean "a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components."

Key Amendments from NPRM to Final Rule:

- BIS aligned its SBOM definition to the National Telecommunication and Information Administration's (NTIA) "Minimum Elements for a Software Bill of Materials," a report written in collaboration with the Department of Commerce and authorized by Executive Order 14028, "Improving the Nation's Cybersecurity," 86 Fed. Reg. 26633 (May 12, 2021).
- BIS removed several SBOM elements (e.g., version string, component hash, package URL, and unique identifier) from the minimum documentation requirements for the Declarations of Conformity and Specific Authorizations.

Requirements for Regulated Entities:

- BIS requires applicants to retain, for a period of 10 years, minimal documentation of each Declaration of Conformity submitted to BIS, which includes documentation or third-party assessments sufficient to identify, at minimum, the author's name, timestamp, component name, and the supplier's name of all proprietary additions to the development of the covered software.

COMPLIANCE PATHWAYS

The Final Rule provides regulated entities with three compliance pathways.

1. **Declarations of Conformity:** BIS streamlined the process for Declarations of Conformity by clarifying the submission obligations and reducing this pathway's reporting requirements.
    - Entities involved in VCS Hardware or Covered Software transactions must submit a Declaration of Conformity once per model year for vehicle-associated units or once per calendar year for non-vehicle-associated units. Material changes must be reported to BIS within 60 days, and the obligation ends 10 years after the original Declaration submission for that model or calendar year.
    - For VCS Hardware, the Declaration must include details such as Federal Communications Commission identification numbers, hardware descriptions, and, if known, the make and model of connected vehicles with which it integrates. Declarants must certify that the hardware was not designed, developed, manufactured, or supplied by entities connected to China or Russia, perform due diligence (optionally using third-party assessments), and maintain supporting documentation. Additionally, they must confirm that suppliers are prepared to provide further documentation to BIS upon request.
    - For Covered Software, the Declaration of Conformity must provide vehicle-specific details, including make, model, trim, and vehicle identification number (VIN) series. Declarants must certify that the software is designed, developed, manufactured, or supplied by an entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, conduct due diligence (third-party assessments are optional), and maintain related documentation. Suppliers must also be prepared to provide additional documentation to BIS if required.
    - Declarations of Conformity *are not* required if the foreign interest is a passive equity ownership in a public company that does not impact the entity's management or control.
2. **General Authorizations:** BIS will issue general authorizations through its website and through the *Federal Register* as opposed to predetermined general authorizations as conceived by the NPRM.
    - BIS explained that issuing general authorizations on an as-needed basis provides market participants with quicker guidance and more flexible implementation without the delays associated with a formal rulemaking process.
    - BIS will issue general authorizations for small businesses; connected vehicles that are infrequently used on public roads; vehicles that are intended for display, testing, or research purposes; and for repair, alteration, or competitions.
3. **Specific Authorizations:** VCS Hardware importers and Connected Vehicle Manufacturers wishing to engage in an otherwise prohibited transaction which are ineligible for an exemption or general authorization would have to apply for and receive a specific authorization to engage in the otherwise prohibited transaction.
    - When reviewing applications for a specific authorization, BIS will consider the factors that may pose undue or unacceptable risks, particularly as they relate to transactions that could result in the exfiltration of connected vehicle or US persons' data, or the remote manipulation or operation of a connected vehicle.

- The Final Rule gives BIS more latitude to grant exceptions to the minimum one-year specific authorization and for durations of less than one year.

EXEMPTIONS

BIS adopted the exemptions detailed in the NPRM and added certain provisions related to component replacement and/or repair under manufacturer warranties. VCS Hardware importers are exempt from certain requirements for transactions involving VCS Hardware if the following are true:

- The hardware, not tied to a model year, was imported before January 1, 2029.
- The hardware was associated with a vehicle before MY 2030 or integrated into a connected vehicle (completed or incomplete) prior to MY 2030.

Connected Vehicle Manufacturers are similarly exempt from transactions involving Covered Software if the vehicle was completed before MY 2027. In MY 2027 and beyond, manufacturers with Chinese or Russian connections cannot sell connected vehicles or related systems equipped with VCS Hardware or Covered Software absent a general or specific exemption from BIS. Finally, BIS amended its exemptions to clarify that VCS Hardware components imported for repair or warranty purposes are excluded, so long as the vehicle was sold before for MY 2030. For MY 2030 and beyond, the VCS Hardware components will no longer be excluded.

ADVISORY OPINIONS, IS-INFORMED NOTICES, AND APPEALS

1. **Advisory Opinions:** The Final Rule adds a 60-day deadline for BIS to respond to advisory opinion requests, except for limited situations that warrant additional review time. BIS stressed the importance of receiving opinions containing real, specified parties to the transaction and real, specified VCS hardware or covered software in order for BIS to issue the opinion.
2. **"Is-Informed" Notices:** BIS retains the "is-informed" notice provision in the Final Rule.
    - BIS could notify Connected Vehicle Manufacturers or VCS hardware importers, either through direct letters or through a *Federal Register* notice meant to inform a broader set of persons, that a transaction involving certain covered software, VCS hardware, or entities requires a specific authorization because it would constitute a Prohibited Transaction according to the terms of this proposed rule.
    - Any person who engages in a transaction covered by an "is-informed" notice without first receiving a Specific Authorization from BIS would have knowledge that such transaction is prohibited and would therefore be in violation of the Final Rule.
3. **Appeals:** Appeals must be submitted in writing (email or regular mail) to the Office of the Under Secretary of Commerce within 45 days of the adverse action (e.g., denials, suspensions, or revocations of specific authorizations, or notifications of ineligibility for general authorizations).
    - The appeal must detail how the appellant was directly and adversely affected and provide reasons for reversing or modifying the BIS decision.
    - The Under Secretary of Commerce may delegate the review to another BIS official, who may arrange informal hearings at their discretion. Supplementary information may be

submitted within 30 days of the original appeal, though it is generally not accepted afterward.

- Appellants may request an informal hearing in writing at the time of appeal submission, but granting such a request is at the sole discretion of the reviewing official. Third parties may submit amicus filings in support of appellants during granted informal hearings.

ENFORCEMENT AND PENALTIES

BIS reorganized the enforcement sections to provide entities with better clarity without altering its substance. BIS explains how civil and criminal penalties are assessed based on the nature of violations, such as engaging in prohibited transactions or providing false information.

- The maximum civil penalty is $368,136 per violation, while criminal penalties could reach $1,000,000. Entities have opportunities to rectify errors through pre-penalty notices, voluntary self-disclosures, and settlement discussions.
- Final penalty notices cannot be appealed through BIS but may be challenged in any US federal district court. Unpaid penalties may be referred to the US Department of the Treasury and/or US Department of Justice for collection.
- BIS may issue a finding of violation for cases where monetary penalties are deemed unnecessary. These findings may include administrative responses such as cease-and-desist orders. Recipients may respond within 30 days to contest the findings, and BIS will consider new information before issuing a final determination. Unchallenged findings are considered final agency actions.
- BIS also explains that the Final Rule's provisions are designed to operate independently. If a federal court invalidates any provision, the remaining provisions will continue to apply to the fullest extent possible. For instance, prohibitions related to VCS Hardware transactions can remain effective even if those related to China- or Russia-linked entities are invalidated. This ensures the Final Rule remains functional despite partial legal challenges.

RECORDKEEPING AND REPORTING

Regulated entities must maintain accurate records for 10 years after each transaction requiring Declarations of Conformity, General Authorizations, or Specific Authorizations, regardless of whether the transaction proceeded under these pathways. The Final Rule dropped the proposed requirement that required submission of SBOMs and HBOMs, in response to industry concerns about retaining CBI and the burden of reporting such information.

The Final Rule also added provisions to detail measures to protect CBI. Entities submitting information that they want to protect must clearly mark CBI on relevant pages and provide a statement justifying non-disclosure, citing specific legal authorities such as Freedom of Information Act (FOIA) Exemption 4 (5 USC § 552(b)(4)) or other applicable laws. BIS will handle and maintain confidential information in compliance with 15 CFR § 791.102.

WHAT'S NEXT FOR CONNECTED VEHICLES IN THE UNITED STATES?

The BIS Final Rule reflects strong bipartisan support for safeguarding US corporate supply chains and protecting sensitive data of US persons and companies that can potentially be leveraged by a foreign adversary for national security gain.

Assuming that the US administration adopts the Final Rule—which we anticipate it will—market participants should be diligent about assessing their reliance on suppliers from foreign adversary nations and putting mechanisms in place to ensure compliance with the new regulations. Below we offer some initial steps that regulated entities should consider the following:

- Overhaul corporate compliance systems, which includes conducting detailed supplier audits with a specific focus on VCS and ADS technologies implicated by the Final Rule.
- Reexamine sourcing strategies, especially for key components such as connectivity and ADS systems that fall within the purview of the Final Rule. Suppliers of microcontrollers, software, sensors, and telecommunications equipment that incorporate such technologies into their products may need to consider diversifying their sourcing or invest in developing alternative technologies, which could significantly reshape their supply chain.
- Companies with Chinese or Russian interest that are involved in the manufacture of connected vehicles or related technologies may wish to consider restructuring or otherwise modifying their operations to navigate these new barriers. Restructuring could involve, for example, establishing subsidiaries or joint ventures in other countries with modified ownership and operational structures that are not subject to the ownership, control, or direction of China and Russia.
- If these initial steps reveal that certain connected technologies may be subject to the Final Rule, companies may wish to seek counsel to assist them with obtaining general or specific authorizations, advisory opinions, or other exemptions from BIS. While the Final Rule implicates connected vehicles and related systems sold in MY 2027, companies should engage BIS as soon as possible to increase the likelihood of their products obtaining favorable regulatory treatment and thereby being positioned to retain their competitive advantage, as well as to potentially make modifications as needed to keep the products on the market.

CONTACTS

If you have any questions or would like more information on the issues discussed in this report, please contact any of the following:

Authors

David Plotinsky	+1.202.739.5742	david.plotinsky@morganlewis.com
Daniel S. Savrin	+1.617.951.8674	daniel.savrin@morganlewis.com
Mark J. Fanelli	+1.215.963.5069	mark.fanelli@morganlewis.com
Jiazhen (Ivon) Guo	+1.202.739.5163	ivon.guo@morganlewis.com
Brent A. Hawkins	+1.415.442.1449	brent.hawkins@morganlewis.com
Noah J. Kaufman	+1.617.341.7590	noah.kaufman@morganlewis.com
R. Latane Montague	+1.202.739.5582	latane.montague@morganlewis.com

ABOUT US

Morgan Lewis is recognized for exceptional client service, legal innovation, and commitment to its communities. Our global depth reaches across North America, Asia, Europe, and the Middle East with the collaboration of more than 2,200 lawyers and specialists who provide elite legal services across industry sectors for multinational corporations to startups around the world. For more information about us, please visit www.morganlewis.com.

Morgan Lewis

At Morgan Lewis, we're always ready to respond to the needs of our clients and craft powerful solutions for them.

Connect with us

www.morganlewis.com

022025_250355