

ALERT

# BIS Restricts Import and Sales of Automotive Tech Produced by Entities in China and Russia

January 17, 2025

On January 14, 2025, the Department of Commerce Bureau of Industry and Security (BIS) published its Final Rule (Final Rule or the Rule) on “Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles,” adopted in accordance with Executive Order (EO) 13873. This Final Rule follows an advanced notice of proposed rulemaking (ANPRM) published on March 1, 2024, and notice of proposed rulemaking (NPRM) published on September 26, 2024. The Rule adopts regulations addressing national security risks posed by transactions involving vehicle-related information and communications technology and services (ICTS) that are designed, developed, manufactured, or supplied by entities controlled by or subject to the jurisdiction of one of two foreign adversaries – the People’s Republic of China (PCR) and Russia.

The Rule prohibits the import of vehicle connectivity system (VCS) hardware produced by covered entities, and the sale or import of connected vehicles under 10,000 pounds incorporating VCS hardware or certain vehicle-related software produced by such entities. It requires that all covered VCS hardware importers and connected vehicle manufacturers submit annual Declarations of Conformity. The Rule also creates a framework permitting certain transactions otherwise prohibited by the Rule, pursuant to general or specific authorization from BIS.

The Final Rule is effective on March 17, 2025 – 60 days after publication in the Federal Register. The prohibitions on covered transactions and associated compliance obligations are not effective until model year 2027 for prohibited software, model year 2030 for prohibited hardware, and January 1, 2029 for hardware not associated with a vehicle model year. While the Final Rule impacts

## Authors

Sara M. Baxenberg  
Partner  
202.719.3755  
sbaxenberg@wiley.law

Matt Lapin  
Of Counsel  
202.719.3435  
mlapin@wiley.law

Melissa Alba  
Associate  
202.719.4729  
malba@wiley.law

Stephanie Rigizadeh  
Associate  
202.719.4736  
srigizadeh@wiley.law

## Practice Areas

Connected & Autonomous Vehicles  
International Trade  
National Security  
Strategic Competition & Supply Chain  
Telecom, Media & Technology

only passenger vehicles, BIS intends to propose another rule tailored to the commercial vehicle sector in the future. Below, we summarize key provisions of the Rule.

### **Covered Entities, Technologies, and Vehicles**

**Entities.** The Final Rule focuses on vehicle technologies that are “designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of two foreign adversaries – the PRC and Russia.” (p.14). (For ease of analysis, we refer to such persons throughout this alert as “covered entities.”) Covered entities are defined very broadly, including entities “with a principal place of business in, headquartered in, incorporated in, or otherwise organized under the laws of” the PRC or Russia as well as entities “controlled” by parties in the PRC or Russia via a range of relationships, who have the ability to determine, direct, or decide important matters affecting an entity (p. 115).

**Technologies.** The Final Rule prohibits certain transactions related to two types of automotive technologies: vehicle connectivity systems (VCS) and automated driving systems (ADS). “VCS” describes “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” (p. 102), subject to certain exclusions for: automotive sensing, ultrawideband communications (for applications such as key fobs), use of unidirectional radio frequency bands like global navigation satellite systems and radio, and supply or management of power for the VCS. (p. 102). “ADS,” meanwhile, describes “hardware and software that, collectively, are capable of performing the entire dynamic driving task for a completed connected vehicle on a sustained basis, regardless of whether it is limited to a specific [operational design domain].” (p. 43).

The Final Rule encompasses software used for ADS and both software and hardware used for VCS. For purposes of the prohibitions and new requirements, “covered software” is defined broadly to include “the 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 VCS or ADS at the vehicle level.” (p. 62). It excludes firmware, open-source software, and “software subcomponents that were designed, developed, manufactured, or supplied prior to March 17, 2026,” provided those subcomponents have not been “maintained, augmented, or otherwise altered” by a covered entity after that date.

**Vehicles.** As noted above, the Final Rule focuses on passenger vehicles rather than the commercial sector, excluding from the definition of “connected vehicle” any “vehicle[] with a gross vehicle weight rating (GVWR) of over 10,000 pounds.” Vehicles operated only on a rail line are also excluded from the definition of connected vehicle. (p. 50).

### **Prohibited Transactions**

The Rule prohibits three categories of transactions, absent a general or specific authorization from BIS:

1. ***Importation of VCS Hardware Produced by a Covered Entity:*** “VCS hardware importers are prohibited from knowingly importing into the United States any VCS hardware that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.” (p. 113) (emphasis added).
2. ***Sale or Importation of Completed Connected Vehicles Incorporating Covered Software Produced by a Covered Entity:*** “[C]onnected vehicle manufacturers are prohibited from knowingly selling within the United States, or importing into the United States, completed connected vehicles that incorporate covered software that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.” (p. 113-114) (emphasis added).
3. ***Sale by Covered Entities of Completed Connected Vehicles Incorporating Covered Software or VCS Hardware:*** “[C]onnected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia are also prohibited from knowingly selling in the United States completed connected vehicles that incorporate covered software or VCS hardware, 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 control of the PRC or Russia.” (p. 114) (emphasis added). The prohibition applies even where VCS hardware and covered software were not designed or developed by manufacturers owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. Covered connected vehicle manufacturers are also prohibited from “offering commercial services in the United States that utilize completed connected vehicles that incorporate ADS,” which BIS believes could include robotaxi and rideshare services (p. 114-115).

#### **New Declaration of Conformity Requirements for All Covered Imports and Sales**

Connected vehicle manufacturers and VCS hardware importers will be required to submit Declarations of Conformity to BIS at least 60 days prior to importing VCS hardware, or importing or selling connected vehicles that incorporate covered software. (p. 39). In the Declaration, the manufacturer or importer must certify that the VCS hardware or covered software was not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. (p. 39). The importer or manufacturer must also certify that it has “conducted due diligence (with or without the use of third-party assessments)” to inform their certification and has “taken all possible measures, either contractually or otherwise, to ensure any necessary documentation and assessments from suppliers will be furnished to BIS upon request[.]” (p. 135).

Declarations must be submitted “once per model year for units associated with a vehicle model year, or once per calendar year for units not associated with a vehicle model year, and only for the categories of transactions [the persons submitting] seek to execute during that period.” (p. 121).

### **General and Specific Authorizations**

The Final Rule establishes a framework for both general and specific authorizations for BIS to permit otherwise-prohibited transactions. General authorizations permit certain VCS hardware importers and connected vehicle manufacturers to engage in otherwise prohibited transactions without prior notification to BIS. (p. 140). The Rule does not provide for any particular general authorizations, but notes that BIS anticipates it will issue authorizations consistent with those outlined in the NPRM, including:

- Small businesses;
- Connected vehicles used infrequently on public roads;
- Vehicles or hardware used solely for display, testing, or research purposes; and
- Vehicles imported solely for repair, alteration, or competition.

In addition, VCS hardware importers and connected vehicle manufacturers will be able to apply to BIS for specific authorizations to engage in otherwise-prohibited transactions. (p. 145). Such applications will be required to include detailed information regarding the proposed transaction, the covered software and/or the VCS hardware, and/or the associated connected vehicles. BIS will consider compliance with cybersecurity standards like SAE 21434, R155, and NHTSA Cybersecurity Best Practices when evaluating such applications, as well as information regarding the applicant's ability to limit PRC/Russian access to or influence over the technology or mitigate associated risks. Interested parties may also seek advisory opinions from BIS prior to engaging in a transaction to confirm compliance.

### **Recordkeeping and Enforcement**

In contrast to the NPRM, the Final Rule does not require the submission of software bill of materials (SBOMs) and hardware bill of materials (HBOMs). Additionally, connected vehicle manufacturers and VCS hardware importers must "maintain complete records related to any transaction for which a Declaration of Conformity, general authorization, or specific authorization would be required by this rule, for a period of 10 years." These records must be furnished to BIS upon request.

Penalties for violations of the regulations can range up to \$368,136 per violation for civil penalties and \$1 million for criminal penalties. Although the regulations provide that certain steps in the enforcement process constitute "final agency action" that can be appealed to a federal district court, the process does not appear to allow for judicial review *before* a penalty is imposed – nor does BIS address the potential impact of the U.S. Supreme Court's decision in *SEC v. Jarkesy* on this enforcement structure.

### **Next Steps**

While the Final Rule will take effect on March 17, 2025, the prohibitions and compliance obligations are staggered. The Final Rule's software restrictions will take effect starting with model year 2027 vehicles. Hardware restrictions will take effect in model year 2030 vehicles, or Jan. 1, 2029, for units without a model year. (p. 106). Accordingly, BIS will consider as "exempt" any otherwise-covered transactions that occur prior

to these timeframes.

The Final Rule announces that BIS is expected to propose a new rule tailored to the commercial vehicle sector within the upcoming months, although it remains to be seen whether or how the Presidential transition may impact these plans. (p. 20, 48).

In addition, the Federal Communications Commission (FCC) will likely initiate a proceeding to assess whether and how to update its Covered List of equipment and services that “pose[] an unacceptable risk to the national security of the United States or the security and safety of United States persons.” 47 U.S.C. § 1601. Under the statute, “[a] specific determination made by the Department of Commerce pursuant to Executive Order No. 13873” – which BIS has invoked in the Final Rule – is a triggering event that requires the FCC to update the Covered List. Inclusion of VCS and ADS technologies on the Covered List could have additional implications for use of those technologies in the United States, as Covered List equipment and services cannot be funded with federal subsidies through the FCC’s Universal Service Fund programs, Covered List equipment is ineligible to receive FCC equipment authorization (which is required for all technology that emits radiofrequencies) or to participate in the FCC’s Cyber Trust Mark labeling program for Internet of Things (IoT) technologies, and the FCC has several open proceedings that would adopt new restrictions or requirements related to the Covered List. Interested parties should continue to monitor these continuing developments at both the FCC and BIS.

Wiley’s Connected & Autonomous Vehicles, National Security, Telecom, Media & Technology, International Trade, and Strategic Competition & Supply Chain practices have broad experience in navigating rulemakings and compliance surrounding cutting-edge technology and the evolving legal landscape. For questions about this summary, please contact the authors.