



May 02, 2025

Categories:

[Presidential
Administration Impacts
Publications
Tariffs & Economic
Impacts](#)

Authors:

[Zachary D. Mills](#)
[Jan de Beer](#)

New Restrictions on Vehicle Connectivity Systems and Automated Driving Systems with Links to China and Russia

On January 16, 2025, the Bureau of Industry and Security (BIS) introduced [significant changes](#) to 15 CFR Part 791 focused on mitigating national security risks associated with information and communications technology and services (ICTS) in connected vehicles. These changes specifically target transactions involving vehicle connectivity systems (VCS) and automated driving systems (ADS) linked to entities owned or controlled by the People's Republic of China and Russia.

This article provides a high-level overview of the new policies and compliance procedures introduced in the "Connected Vehicles" final rule that are crucial for manufacturers and VCS hardware importers operating within the United States.

Key Definitions

The rule defines a "connected vehicle" as any vehicle manufactured primarily for use on public streets, roads, and highways, integrating onboard networked hardware with automotive software systems to communicate via various wireless connectivity methods. Trains and vehicles weighing more than 10,000 pounds are not considered connected vehicles. A "connected vehicle manufacturer" is defined as a U.S. person who manufactures, assembles, or imports completed connected vehicles for sale in the United States, or integrates ADS software into such vehicles.

"Vehicle connectivity systems" encompass hardware or software items installed in a connected vehicle that enable radio frequency communications over 450 megahertz (for example, telematics control units). Sensing systems, such as radar, audio, video, or LiDAR systems are not considered vehicle connectivity systems. However, hardware and software that enable the transmission or receipt of

data collected by sensing systems would almost certainly be considered components of vehicle connectivity systems.

“Automated driving systems,” include hardware and software that are capable of driving a completed connected vehicle on a sustained basis. Thus, hardware and software related to simpler driver assistance features (such as radar cruise control or automated braking) are not considered ADS.

“VCS hardware” includes programmable components directly enabling VCS functions, such as microcontrollers, networking units, and communication modules. “Covered software” refers to software-based components (including applications, middleware, and system software), in which there is a foreign interest, that enable the function of VCS or ADS at the vehicle level. Firmware and open-source software do not fall under the definition of covered software.

Complying with the rule’s prohibitions requires identifying whether an individual or entity is “owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.” Such individuals or entities include:

- Any individual, regardless of location, who acts on behalf of or under the direction of a foreign adversary (namely, China or Russia) — whether as an agent, employee, or in any other capacity — or who works for someone backed or controlled by either country;
- Any person who is a citizen or resident of China or Russia (or a country under the control of China or Russia), and who is not a U.S. citizen or lawful permanent resident;
- Any company, partnership, or organization that is based in, incorporated in, or governed by the laws of China, Russia, or a Chinese- or Russian-controlled country; and
- Any entity, regardless of where it operates or is organized, that is owned or controlled — directly or indirectly — by China, Russia, or individuals/entities described above. This includes situations where influence is exercised through voting shares, board seats, contracts, or other formal or informal means of control.

Prohibited Transactions

The final rule prohibits the following transactions involving VCS hardware and covered software linked to China and Russia:

- VCS hardware importers are barred from knowingly importing VCS hardware designed, developed, manufactured, or supplied by entities that are owned, controlled by, or subject to the jurisdiction or direction of China or Russia.
- Connected vehicle manufacturers are prohibited from importing or selling completed Connected vehicles incorporating covered software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of China or Russia.
- Connected vehicle manufacturers owned, controlled by, or subject to the jurisdiction of China or Russia are prohibited from selling vehicles with VCS hardware or covered software in the U.S., regardless of the origin of these components.
- Connected vehicle manufacturers owned, controlled by, or subject to the jurisdiction of China or Russia are also prohibited from offering commercial services (e.g., ridesharing services) in the U.S. that utilize completed connected vehicles incorporating ADS.

Compliance

VCS hardware importers and connected vehicle manufacturers are required to certify their compliance with the final rule by submitting Declarations of Conformity at least 60 days prior to the first import or sale of each model year of affected connected vehicles or VCS hardware. These declarations must be renewed annually. An updated Declaration of Conformity must be submitted within 60 days of the declarant's discovery of any material changes to the information contained in the original declaration. In order to prepare accurate Declarations of Conformity, manufacturers and importers of connected vehicles and VCS hardware will need to comprehensively review their supply chains and verify the source of all affected hardware and software.

The final rule also provides for general and specific authorizations to engage in otherwise prohibited transactions. However, no general authorizations have been issued yet. Specific authorizations may be granted on a case-by-case basis if the applicant takes certain steps focused on securing VCS or ADS, such as limiting foreign government access to such systems and implementing other mitigation measures.

Recordkeeping and Penalties

The rule imposes strict recordkeeping requirements, mandating that VCS hardware importers, connected vehicle manufacturers, and third-party assessors maintain primary business records related to transactions for at least 10 years. BIS retains the authority to request complete information regarding any transaction under oath. Violations of these requirements can result in severe penalties, including civil fines of up to \$250,000 and criminal penalties of up to \$1,000,000 and/or 20 years in prison.

Implementation Timeline

Because of the time required for connected vehicle manufacturers to review (and potentially adjust) their supply chains, the final rule's requirements will be phased in over the coming years. The final rule's obligations related to VCS and ADS covered software go into effect beginning with model year 2027, as does the prohibition on the sale of connected vehicles by Chinese- and Russian-linked manufacturers. Beginning with model year 2030, the final rule's hardware-related requirements become effective.

Impacts on Manufacturers, Importers, and Suppliers

Drivers in the United States increasingly expect ADS and VCS to be standard features in new vehicles. As a result, the final rule will impact nearly every vehicle manufacturer and importer. The requirement to submit annual Declarations of Conformity means that connected vehicle manufacturers and importers must have deep visibility into their ADS and VCS hardware and software supply

chains. It also places additional pressure on suppliers throughout the supply chain to accurately disclose any ties to Russia or China.

At the same time, the final rule creates a competitive opportunity for suppliers without such connections, who will be well-positioned to capture greater market share in the U.S. Please reach out to the authors of this article or your contacts on Frost Brown Todd's [Mobility](#) team for support at every step of the connected vehicles supply chain.

Presidential Administration Impacts

Frost Brown Todd has a dedicated team closely monitoring the significant policy changes and their impact on businesses. We are committed to keeping our clients informed as these changes take effect and new information emerges. Visit our resource page for insight into the latest developments and their implications for business and industry.

[View Collection](#)

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.