Updates
February 28, 2025
New US Commerce Prohibitions on Chinese and Russian Connected Vehicle Technology

New security rules designed to protect the connected vehicle supply chain will take effect in March unless they are withdrawn.

The U.S. Department of Commerce Bureau of Industry and Security (BIS) published the final rule implementing Executive Order 13873 (Final Rule), which President Donald Trump issued during his first term, shortly before the end of the Biden administration. The rule is intended to protect vehicle connectivity systems (VCS) and automated driving systems (ADS) against supply-chain compromise by Russia or the People's Republic of China (PRC).

The Final Rule follows a period of public comment and feedback from stakeholders after a notice of proposed rulemaking was announced in September 2024. Because the Final Rule was published, it is not subject to the automatic "freeze" the Trump administration announced in presidential memorandum "Regulatory Freeze Pending Review" issued on January 20, 2025, and though the agency has discretion to delay the effective date, as of the date of this publication, it has not done so.

The Final Rule effectively bans the import or sale of connected vehicles and certain technologies from Russia and the PRC. Consequently, importers and manufacturers of connected vehicles or connected vehicle technology from these countries will be required to obtain covered software and hardware from alternate sources or seek specific authorization. Manufacturers with a sufficient nexus to Russia or the PRC will be banned from selling connected vehicles entirely, even if they were not involved in the design, development, or manufacture of the hardware or software. The Final Rule also adds compliance requirements for importers and manufacturers of connected vehicles. Increased compliance costs, along with the disruption in the supply chain, could ultimately raise the prices of connected vehicles for consumers.

Effective Dates

The Final Rule takes effect on March 17, 2025. Restrictions on software will take effect for Model Year 2027, and prohibitions related to hardware will take effect for Model Year 2030 or January 1, 2029, for components that do not have a model year.

What Is Covered?

- **"ADS"** means hardware and software that, collectively, enable a connected vehicle to perform the entire dynamic driving task on a sustained basis.
- **"VCS"** means a hardware or software component for a completed connected vehicle that enables the function of radio frequency communications over 450 megahertz. Exclusions from this definition include hardware or software for automotive sensing (*e.g.*, radar, video, etc.), physical vehicle access (*e.g.*, key fobs), and unidirectional radio frequency (*e.g.*, AM/FM radio). **"VCS hardware"** means software/programmable parts that enable VCS, including wireless communication microcontrollers or modules.
- **"Covered software"** means software with a foreign interest that directly enables the function of VCS or ADS in a vehicle. The definition in the Final Rule is more detailed and contains numerous exceptions and examples.
- A **"connected vehicle"** essentially means a passenger vehicle (under 10,001 pounds) which wirelessly communicates with any other network or device. A connected vehicle which requires no further manufacturing constitutes a **"completed connected vehicle."** Though the Final Rule narrows its application to passenger vehicles, BIS has stated it intends to develop rules for commercial vehicles in the future.

Who Is Covered?

- **"VCS hardware importer"** means a U.S. person who imports VCS hardware for further manufacture, incorporation, or integration into a completed connected vehicle or VCS hardware that is already a part of a completed connected vehicle that is meant to be sold in the United States.
- **"Connected vehicle manufacturer"** means a U.S. person who manufactures, assembles, imports, or integrates ADS software into completed connected vehicles for sale in the United States.

Prohibitions

1. VCS hardware importers must not knowingly import into the United States any VCS hardware that is designed, developed, manufactured, or supplied by persons or entities with a sufficient nexus to (owned by, controlled by, or subject to the jurisdiction or direction of) the PRC or Russia.
2. Connected vehicle manufacturers must not knowingly sell or import into the United States completed connected vehicles with covered software that is designed, developed, manufactured, or supplied by persons or entities with sufficient nexus to the PRC or Russia.
3. PRC- or Russia-affiliated connected vehicle manufacturers are further prohibited from knowingly selling in the United States completed connected vehicles that incorporate covered software or VCS hardware and from offering commercial services with completed connected vehicles with ADS in the United States. This prohibition applies even if the persons or entities with a sufficient nexus to the PRC or Russia were not involved in the design, development, or manufacture of the VCS hardware or covered software—merely the sale of these vehicles in the United States is covered by the rule.

Compliance

Declarations of Conformity. VCS hardware importers and connected vehicle manufacturers will be required to submit annual "Declarations of Conformity," which certify that they are compliant with the rule. Declarations must also be submitted by entities engaged in VCS hardware transactions and covered software transactions. Declarations indicate that entities have completed due diligence requirements and that they maintain records for BIS verification. The declarations must be submitted 60 days before the first import or sale of each model year of vehicles covered by the rule.

Authorizations—general and specific. BIS and the *Federal Register* may publish general authorizations, which grant various exceptions to the rule. Persons or entities relying on general authorizations must comply with reporting and recordkeeping requirements. If a general authorization does not apply, a person or entity may apply for a *specific authorization* of a prohibited transaction to be reviewed by BIS on a case-by-case basis. BIS also maintains the authority to provide an "is-informed notice," either directly or through the *Federal Register*, which announces that a particular transaction requires specific authorization. If an application for specific authorization is denied, the person or entity may appeal the decision.

Recordkeeping and use of third parties. VCS hardware importers and connected vehicle manufacturers must keep complete records related to any transaction that requires a Declaration of Conformity or authorization for 10 years. Entities may use third parties to maintain compliance and assist with recordkeeping and submission of the Declarations of Conformity.

Advisory opinions. Entities may submit inquiries to BIS on an as-needed basis, and BIS must respond with an advisory opinion within 60 days or notify the need for an extension. BIS may publish some of these opinions, with identifying information redacted.

Enforcement

Failure to comply with the rule may result in civil or criminal penalties under the International Emergency Economic Powers Act. Civil penalties are adjusted annually; as of 2025, the maximum civil fine is $377,700 per violation. Criminal penalties can amount to $1,000,000 and/or imprisonment. BIS can also "find a violation" without administering a penalty and may engage in administrative recourse, such as a cease-and-desist order. Entities have the opportunity to settle and/or contest BIS's finding.

Looking Forward—Trump Administration Policies

The rule was issued by the Biden administration to implement an executive order from the first Trump administration. It is not clear whether, how, or to what degree President Trump will modify the Biden administration's cybersecurity policies, and President Trump's policies toward electric vehicles, Information and Communication Technology and Services, and trade with Russia and the PRC are still emerging. The rule appears to align with some of President Trump's stated policies that affect the automotive industry. For example, President Trump's America First Trade Policy aims to build a trade policy which "enhances our nation's industrial and technological advantages, defends our national security, and—above all—benefits American workers, manufacturers, farmers, ranchers, entrepreneurs, and businesses."

President Trump's second term also aims to champion innovation and technology, deregulation, and reducing governmental inefficiencies. These efforts are led by private industry leaders, including technology and automotive stakeholder Elon Musk. Musk's company, Tesla, owns factories in China that could be subject to the new rule if they develop covered hardware or software. Based on these goals and interests, the new administration could find the new rule burdensome or stifling of innovation.

The rule also lies at the intersection of national security and industrial policy. It is uncertain what Trump's approach to U.S.-China relations will be in the second term. His campaign threatened steep tariffs against Chinese imports, and his administration has already imposed a punitive 10% tariff. This suggests continued antagonism, though perhaps not the same escalation as seen in his previous term. However, he reportedly is open to PRC-based automotive companies building vehicles in the United States, which, if the entities manufacture and sell connected vehicles in the United States, could violate the rule.

Trump's revocation of electric vehicle tax credits and new tariffs demonstrate that significant changes to the current automotive industry's regulatory framework are likely to continue. It remains to be seen, however, which of the administration's priorities—security, American economy, innovation and technology, or deregulation—will inform the decision to maintain, revoke, or alter the new rule.

Authors

Explore more in

International Trade Litigation Privacy & Security Technology Transactions & Privacy Law

Related insights

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law

Update

February Tip of the Month: Federal Court Issues Nationwide Injunction Against Trump Executive Orders on DEI Initiatives