Articles + Publications | October 7, 2024

Locke Lord QuickStudy: BIS Proposes New Rule to Restrict ?Connected Vehicles Linked to ?Chinese or Russian Technology

Locke Lord LLP

WRITTEN BY

Ryan Last

On September 23, 2024, the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") announced a proposed rule that could reshape the automotive industry by restricting the import and sale of connected vehicles. The Notice of Proposed Rulemaking ("NPRM") is intended to block importation of vehicles into the U.S. market if the vehicles are manufactured by companies controlled by or under the influence of the People's Republic of China ("PRC") or Russia. It also targets vehicles that include "vehicle connectivity systems" ("VCS") or related software with ties to these foreign nations. At bottom, these vehicles could export U.S. person's data which could compromise national security.

This NPRM follows a March 1, 2024, Advanced Notice of Proposed Rulemaking and signals the next phase of regulatory action intended to safeguard critical U.S. infrastructure. Stakeholders have the opportunity to provide feedback during the public comment period, which closes on October 28, 2024. Comments on specific areas, such as whether additional automated driving systems ("ADS") hardware or other technologies should be restricted, are particularly encouraged by BIS.

In a public statement, BIS stressed the national security risks that certain foreign technologies pose. "Modern vehicles are equipped with features like cameras, microphones, and global positioning systems (GPS) that are constantly connected to the internet," noted Commerce Secretary Gina Raimondo. "It's not hard to imagine how these systems could be exploited by foreign adversaries, potentially endangering U.S. national security and citizens' privacy. This rule represents a proactive step in removing PRC- and Russian-manufactured technologies from U.S. roadways."

We note that if the NRPM is enacted substantially in its current form, it may moot the proposed "No Limits Act" (H.R.8043 – 118th Congress (2023-2024)) discussed in our June 5, 2024 QuickStudy "Important Update: Changes to Section 232 Exclusion Process and Biden ?Administration's Tariff Policy" since this rule making would apply to all PRC and Russian auto makers and not just those enumerated on the No Limits Act.

Covered Vehicles

The NPRM targets "connected vehicles" and their associated components. "Connected vehicle" is defined as any on-road vehicle that integrates onboard networked hardware with automotive software systems to communicate through dedicated short-range communication, cellular networks, satellite communication, or other wireless

technologies. Examples of such vehicles include cars, motorcycles, buses, small and medium-sized trucks, large commercial trucks, and recreational vehicles. BIS anticipates that this definition will cover nearly all new vehicles sold in the United States, while only connected vehicles containing specific hardware or software components will fall under the rule's scope.

Covered Hardware and Software

The NPRM focuses on hardware and software related to VCS that allow vehicles to communicate via radio and software for ADS. In response to public comments, BIS excluded certain systems that were previously identified as potential supply chain risks. The focus remains on VCS and ADS systems that enable communication with and control of connected vehicles, making them susceptible to data breaches or remote manipulation.

Hardware

BIS proposes to define "VCS hardware" as 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 VCS: 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. "VCS hardware does not include component parts that do not contribute to the communication function of VCS hardware (e.g., brackets, fasteners, plastics, and passive electronics)."

Software

BIS proposes to define "covered software" to mean the 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. "Covered software does not include firmware, which is characterized as software specifically programmed for a hardware device with a primary purpose of controlling, configuring, and communicating with that hardware device." At a minimum, this definition of covered software would include operating systems such as a real-time operating system, and general-purpose operating systems. Covered software does not include open-source software.

Linkage to the PRC or Russia

The prohibitions focus on VCS hardware and connected vehicles that include covered software, which are designed, developed, manufactured, or supplied by entities that are owned, controlled by, or under the jurisdiction of current and future potential foreign adversaries, specifically Russia and the PRC (including Hong Kong). BIS proposes a wide-reaching definition of entities connected to the PRC or Russia, which includes:

- Individual acting on behalf of, or whose activities are supervised, directed, financed, or subsidized by the PRC or Russia.
- Citizens or residents of the PRC or Russia who are not U.S. citizens or permanent residents (however, involvement of Chinese or Russian employees in development outside of the PRC or Russia does not automatically trigger the rule).
- Organizations headquartered, incorporated, or organized under Chinese or Russian laws (including subsidiaries

or joint ventures with U.S. companies).
- Entities where individuals from the above categories have direct or indirect influence over key organizational decisions, whether through ownership stakes, board representation, proxy voting, special shares, contracts, or other means. This broad definition can also apply to entities within the U.S.

Prohibitions

The NPRM proposes prohibition of the following activities related to both VCS hardware and software and ADS software:

- Knowingly importing in the U.S. VCS hardware that is developed by parties linked to the PRC or Russia;
- Knowingly selling connected vehicles with covered software from PRC or Russian sources; and
- Selling connected vehicles in the U.S. that contain VCS hardware or software from the PRC or Russia, regardless of where the vehicles are assembled.

BIS says companies should consider the risks associated with VCS and ADS when designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC and Russia. BIS signaled that it may interpret "designed, developed, manufactured, or supplied by" Chinese or Russian entities broadly, which could include minimal involvement of parties from these countries in the development process. This could have major consequences for companies with development teams for hardware or software based in the PRC or Russia. Even minimal involvement by these teams, such as contributing portions base code, could violate the proposed rule.

Phased Implementation

BIS proposes to implement the prohibitions through a phased approach:

- Model Year 2027: The ban would begin with vehicles equipped with the relevant VCS hardware or ADS software tied to the PRC or Russia.
- Model Year 2030: Importers of standalone VCS hardware would face restrictions starting in 2029, with full implementation by 2030.

If, following consideration of comments received on the NPRM, BIS issues a final rule to adopt the proposal, that final rule would take effect 60 days after publication in the Federal Register.

Compliance and Declarations

The NPRM requires connected vehicle manufacturers and VCS hardware importers to submit annual declarations confirming that they are not engaging in prohibited transactions before they import or sell covered items in the U.S. This declaration must include detailed information and evidence of due diligence, including a hardware or software bill of materials and documentation of due diligence efforts to ensure no foreign adversary-linked components are present. Manufacturers and importers will also be required to maintain records for 10 years and conduct robust supply chain reviews to ensure compliance. Declarations must be filed at least 60 days before the import or sale of items linked to a vehicle mode, or within 30 days of material changes.

Failure to comply with these requirements or submitting false declarations could result in substantial civil or

criminal penalties. Companies will need to track their supply chains meticulously, including gathering certifications from suppliers to mitigate the risk of liability.

General Authorizations

The NPRM proposes the following exemptions and authorizations.

- Manufacturers producing fewer than 1,000 connected vehicles annually.
- Connected vehicles used for research, testing, or display purposes for less than 30 days per year.
- Vehicles imported for repairs or competition that will be reexported within a year.

Companies using general authorizations would be allowed to self-certify their compliance with the applicable general authorization without notifying BIS. However, such companies would still be required to retain all relevant records for a period of 10 years documenting compliance and to continuously monitor for any changes that render a transaction ineligible for continued reliance on the general authorization. Companies connected to the PRC or Russia re not eligible for general authorization.

Companies wishing to engage in an otherwise prohibited transaction who 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. Specific authorizations are determined on a case-by-case basis to ensure the proposed transaction does not pose a significant national security threat.

Implications for the Automotive Industry

The NPRM's broad prohibitions, if enacted, could significantly impact U.S. automotive supply chains, particularly for manufacturers or suppliers with ties to the PRC or Russia. Companies relying on Chinese or Russian components for VCS or ADS will need to assess their supply chains and take proactive steps to find alternative suppliers.

Rather than imposing a strict liability standard, BIS seeks to impose civil and/or criminal penalties against any person who violates, attempts to violate, conspires to violate, or *knowingly* causes a violation of this rule, if finalized, under International Emergency Economic Powers Act, 50 U.S.C. 1705 ("IEEPA"), depending on the circumstances of the violation. At the time of publishing of the NPRM, the maximum civil penalty for violations of IEEPA is $368,136 per violation and the maximum criminal penalty is $1,000,000.

Conclusion

The BIS's proposed rule marks a significant regulatory step to address growing concerns over foreign adversary influence in the U.S. connected vehicle market. Affected businesses, particularly those with supply chains tied to Chinese or Russian technologies, should review the NPRM closely and consider submitting comments.

This paper is intended as a guide only and is not a substitute for specific legal or ?tax advice. ????Please ???reach out to the authors for any specific questions. We expect ?to continue to monitor the ????topics ???addressed in this paper and provide future ?client updates when useful.?

RELATED INDUSTRIES + PRACTICES

- Corporate
- International
- Sanctions + Trade Controls