SQUIRE PATTON BOGGS

Signs of Things to Come

BIS Issues Notice of Proposed Rulemaking Aimed at Connected Vehicle Technologies from China and Russia

Global – October 2024

On September 26, 2024, the US Department of Commerce's Bureau of Industry and Security (BIS) issued a Notice of Proposed Rulemaking (NPRM) that, when final, would prohibit the sale or import of connected vehicles (and certain related component hardware and software) with a sufficient nexus to either the People's Republic of China (PRC) or Russia. This action follows an Advanced Notice of Proposed Rulemaking (ANPRM) that the agency issued on March 1, 2024. Comments on the NPRM must be submitted to BIS on or before October 28, 2024.

If finalized, this BIS action would create new and significant compliance obligations and risks for automakers and their suppliers, aimed primarily at countering risks posed by data collection, transmission and other nefarious purposes by recognized foreign adversaries. Stakeholders must understand their risk, evaluate their supply chains and consider engaging with agency officials to ensure the final regulations balance mitigating risk against the need to promote innovation, and continue US leadership in the production of automobiles and related technological capabilities. And while this current action focuses on connected vehicles, we expect this is the first of a serious of regulations targeting connected technologies and their links to national and economic security.

Who is Responsible for Administering This New Framework?

BIS's Office of Information and Communications Technology and Services (OICTS) is leading broader federal government efforts to address data privacy and other risks in information and communications technologies. This effort began under President Trump with E.O. 13873 (Securing the Information and Communications Technology and Services Supply Chain), and was later modified and expanded under President Biden's E.O. 14034 (Protecting Americans' Sensitive Data From Foreign Adversaries).

While BIS generally administers export controls, OICTS has proposed a see-through rule on the importation of these connected vehicles and related technologies capturing VCS capabilities, pursuant to the President's emergency powers granted in the International Emergency Economic Powers Act (IEEPA) (50 U.S.C. 1701, *et seq.*). BIS has determined that certain technologies related to connected vehicles present a risk to national security and critical infrastructure when those technologies originate in the PRC or Russia.

What Products Are Covered?

The NPRM focuses on the hardware and software of a vehicle connectivity system (VCS), which are critical components that allow a connected vehicle to integrate various radio frequency communication technologies, access external data sources, facilitate vehicle-to-vehicle communication and provide enhanced services to drivers. BIS has broadly defined the relevant terms in the proposed rule to include as much of the significant ICTS for connected cars that are developed or manufactured with links to PRC or Russia, including the following terms.[1]

"Connected Vehicle"

BIS defined a connected vehicle as any on-road vehicle (including passenger vehicles, motorcycles, buses, small and medium trucks, class 8 commercial trucks[2] and recreational vehicles) that integrates onboard networked hardware with automative software systems to communicate via a range of wireless mediums with "any other network or device." The proposed definition excludes vehicles operated only on a rail line (e.g., "rolling stock") and unmanned aerial vehicles, although BIS leaves open the possibility for future regulation to address potential threats in these areas. Additionally, the proposed rule excludes vehicles that are not used on public roads such as agricultural or mining vehicles.[3]

"Vehicle Connectivity System (VCS)"

The proposed rule defines a VCS as "a hardware or software item for a completed connected vehicle that has the function of enabling the transmission, receipt, conversion or processing of radio frequency communications at a frequency over 450-megahertz." The 450-megahertz threshold was set to exclude ICTS that BIS considers lower risk and higher utility for consumers, such as electronic key fobs and tire pressure monitoring systems.

1 89 Fed. Reg. 79088 (proposed Sept. 26, 2024) (hereinafter "NPRM") at 79116—17.

2 A "Class 8" truck is a heavy-duty vehicle with a Gross Vehicle Weight Rating (GVWR) of over 33,000 pounds. These trucks are used for transporting large loads, typically seen in industries like freight, construction and logistics. Examples include semi-trucks, dump trucks and cement trucks.

3 *Commerce Announces Proposed Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats*, Sept. 23, 2024, Bureau of Industry and Security, Office of Congressional and Public Affairs, www.bis.gov.

"VCS Hardware"

BIS proposes defining VCS hardware as the physical components and subcomponents that are software-enabled or programmable to support Vehicle Connectivity Systems. The list of hardware includes: "[the] 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." Component parts (brackets, fasteners, plastics and passive electronics) that do not contribute to the communication function of these systems are excluded.

"Covered Software"

The software that the proposed rule cover would, at a minimum, include operating systems for connected vehicles such as a real-time operating system (RTOS) and general-purpose operating system. Both VCS software and automated driving systems (ADS) software would be included in covered software if the source can be traced to a "foreign interest." Foreign interest is defined broadly and includes "any interest in property, of any nature whatsoever, whether direct or indirect, by a non-US person" (emphasis added). If the rule is finalized, US persons will need to adhere to the compliance mechanisms discussed below if any VCS hardware or covered software was sourced from a foreign interest. Any source code that is developed outside of the US would require compliance with the proposed rule, but the rule would exclude firmware[4] or open-source software.[5]

What Activities Are Prohibited?

Under the proposed rule, a US person will be prohibited from the following activities if they have knowledge[6] the subject item was " designed, developed, manufactured or supplied by persons owned by, controlled by or subject to the jurisdiction or direction of the PRC or Russia."

- US persons are prohibited from knowingly importing VCS hardware with any of the above links to PRC or Russia
- US persons are prohibited from knowingly importing into the US, or selling in the US completed connected vehicles that incorporate covered software with any of the above links to the PRC or Russia

Additionally, non-US connected vehicle manufacturers with links to the PRC or Russia would be prohibited from knowingly selling completed connected vehicles that incorporate VCS hardware or covered software in the US.

What Links to the PRC and Russia are Captured Under the Proposed Prohibition?

BIS has explained that the proposed rule is aimed at the risks posed by VCS hardware and connected vehicles with covered software. These risks arise from supply chains where the PRC or Russia could exploit data or insert harmful hardware or software into ICTS products. To capture as many significant components of the ICTS supply chain involved with VCS hardware and covered software as possible, BIS has broadly defined "person owned by, controlled by or subject to the jurisdiction or direction of a foreign adversary" to mean:

1. Any person, wherever located, who acts as an agent, representative or employee, or any person who acts in any other capacity at the order, request or under the direction or control, of a foreign adversary or of a person whose activities are directly or indirectly supervised, directed, controlled, financed or subsidized in whole or in majority part by a foreign adversary
2. Any person, wherever located, who is a citizen or resident of a foreign adversary or a country controlled by a foreign adversary, and is not a US citizen or permanent resident of the US
3. Any corporation, partnership, association or other organization with a principal place of business in, headquartered in, incorporated in or otherwise organized under the laws of a foreign adversary or a country controlled by a foreign adversary
4. Any corporation, partnership, association or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary, to include circumstances in which any person identified in paragraphs [1—3] possesses the power, direct or indirect, whether or not exercised, through the ownership of a majority or a dominant minority of the total outstanding voting interest in an entity, board representation, proxy voting, a special share, contractual arrangements, formal or informal arrangements to act in concert or other means, to determine, direct or decide important matters affecting an entity

The NPRM provides twenty-one example scenarios that would or would not involve "persons owned by, controlled by or subject to the jurisdiction or direction of the PRC and Russia." Although some of the example transactions are obvious on their face, other examples highlight the broad reach of BIS's proposed definition. Included in the prohibitions would be a person or company with ties to the PRC or Russia with a minority interest in the VCS manufacturer (or other covered item) with "certain veto rights," including the right to veto the dismissal of senior executives or the right to block a "significant business decision" of a board of directors. The minority power to stop a company decision is enough to satisfy the "controlled by" or "subject to the direction of" the PRC or Russia requirement.

4 BIS characterizes "firmware" as "software specifically programmed for a hardware device with a primary purpose of controlling, configuring, and communicating with that hardware device." NPRM at 79116.

5 BIS characterizes "open-source software" as "software that can be freely used, modified, and distributed by anyone, with both access to the source code and the ability to contribute to the software's development and improvement." NPRM at 79116.

6 Knowledge includes "not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence. Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person's willful avoidance of facts." NPRM at 79116.

Has BIS Suggested Any Measures to Assist With Compliance Efforts?

BIS proposed three general compliance mechanisms to support impacted market participants.

- **Declarations of Conformity** – BIS proposes requiring VCS hardware importers and connected vehicle manufacturers to provide once yearly (or upon material changes, such as a model year change) Declarations of Conformity to BIS that they have not engaged in a prohibited transaction, including with such declaration certain required information. The proposed rule details further the proposed types of Declarations of Conformity and submission procedures (including that such Declarations may be submitted via a new BIS web portal).
- **General Authorizations** – BIS proposes certain general authorizations, to allow VCS hardware importers and/or connected vehicle manufacturers from engaging in otherwise prohibited transactions, without notifying or seeking approval from BIS. Such general authorizations will only be granted for narrow circumstances, such as small businesses that only produce a total model year production of completed connected vehicles containing covered software or total model year production of VCS hardware less than 1,000 units, or completed connected vehicles and VCS hardware that is used for research purposed.
- **Specific Authorizations** – Otherwise, BIS would permit VCS hardware importers and connected vehicle manufactures to seek specific authorizations, but they "would only be available in circumstances where BIS determines, based on the information submitted by the applicant and other collected information, that the otherwise prohibited transactions does not present an undue or unacceptable risk to US national security." BIS may impose certain requirements and mitigation measures on the party seeking to engage in the prohibited transaction. The agency would be required to reply to requests for specific authorizations with a status update and any request for additional information/documents within 90 days.

If the proposed rule is finalized, covered parties would be required to maintain complete records related to a Declaration of Conformity, general authorization or specific authorization for ten years, regardless of whether such authorization applies or whether the party has yet sought an authorization (including information pertinent to the authorization, and business records related to execution of the transaction).

BIS would authorize appeals to the BIS Undersecretary after decisions to deny, or suspend/revoke a previously granted, specific authorization or upon written notification that a party is ineligible for a general authorization. BIS would also issue advisory opinions on prospective transactions as requested and may notify parties that certain activities could constitute a prohibited transaction through "is-informed" letters or, for notice to a wider audience, through the Federal Register.

When Will These Prohibitions Enter Into Effect?

Once BIS has considered comments on the NPRM, it will issue a final rule that will take effect 60 days after publication in the Federal Register. After going into effect, the following grace periods would allow certain exemptions for VCS hardware and connected vehicle importers and manufacturers before stricter compliance measures take effect:

- VCS hardware importers may continue to import otherwise prohibited VCS Hardware (without complying with the mechanisms above) until January 1, 2029 (if the VCS Hardware is not associated with a vehicle Model Year) or until model year 2030 (if the VCS hardware is associated with a vehicle model year)
- Connected vehicle importers and manufacturers in the US may continue to import and sell connected vehicles that incorporate covered software that would otherwise be prohibited (without complying with the mechanisms above) until vehicle model year 2027
- Connected vehicle manufacturers linked to the PRC or Russia may continue to sell connected vehicles in the US that incorporate covered software or VCS hardware that would otherwise be prohibited (without complying with the mechanisms above) until vehicle model year 2027

Failure to comply with the proposed rule may result in both civil and criminal penalties under IEEPA. The current civil penalty is the greater of US$368,136 per violation, or an amount twice the amount of the transaction with respect to which the penalty is imposed. A criminal conviction for willful violations of the proposed regulation can result in fines up to US$1,000,000 and up to 20 years imprisonment, or both.

Who Should Consider Commenting?

Several times in the NPRM, BIS cites the complexity and opacity of connected vehicle supply chains as justifying the proposed rule, emphasizing the risks US importers and manufacturers face from unknown suppliers in those supply chain. BIS sees the new rules as a potential benefit for importers and manufacturers to bolster their due diligence and compliance programs. But for importers, manufacturers and parts suppliers to extract this intended benefit, they will have to understand the scope of the rule relative to their business and more broadly understand the supply chains that support their business. And if they find the regulations to be overly broad – particularly, as balanced against the draft rule's objectives for data privacy and technology security – affected parties should participate in the comment process to help guide the final regulations. Ultimately, all imports with VCS capabilities must do the required conformity reporting, not just those importing from the PRC or Russia, creating new and burdens on compliance requirements across connected vehicle supply chains.

As another example, industry stakeholders may be concerned that the proposed definitions capture technologies falling outside of the goals of addressing data privacy and security concerns, or capture business relationships that should not pose a risk to US data and national security. To what extent would the definition of a "person owned by, controlled by or subject to the jurisdiction or direction of a foreign adversary" (e.g., the PRC and Russia) require companies to assess current and future structures of subsidiary and joint venture arrangements? And how might any required reorganization stifle US innovation in the manufacturing of next-generation automobiles?

BIS has not recommended a specific method of due diligence for complying with the proposed rule. However, it mentions in the NPRM that VCS hardware importers and connected vehicle manufacturers need to do more thorough investigations, looking beyond just their first and second-tier suppliers for connections to the PRC and Russia. While original equipment manufacturers may not currently have knowledge to which suppliers have access to connected vehicle software, if the proposed rule is finalized further investigation will be necessary to satisfy the Declaration of Conformity mechanism discussed above.

To date, US policymakers have viewed Chinese EVs differently than their EU counterparts, with the US firmer in the view that economic security is now national security. The NPRM in the US follows a Section 301 tariff hike that will raise the total tariff on Chinese EVs to about 127%, compared to 35% in the EU. Notably, EU officials, concerned about Chinese and Russian technology in the automotive sector, have suggested they may examine limits on connected vehicles in the future.

We strongly recommend companies operating in this domain to examine their supply chains, understand their risk and consider engaging in the comment process and stand ready to support that effort, as needed.

Contacts

Kate Kim Tuma
Partner, Los Angeles
T +1 213 689 5147
E kate.tuma@squirepb.com

George N. Grammas
Partner, Washington DC
T +1 202 626 6234
E george.grammas@squirepb.com

Everett Eissenstat
Partner, Washington DC
T +1 202 457 6535
E everett.eissenstat@squirepb.com

David Stewart
Principal, Washington DC
T +1 202 457 6054
E david.stewart@squirepb.com

Bridget McGovern
Partner, Washington DC
T +1 202 457 6104
E bridget.mcgovern@squirepb.com

Ludmilla L. Kasulke
Partner, Washington DC
T +1 202 457 5125
E ludmilla.kasulke@squirepb.com

Pablo E. Carrillo
Of Counsel, Washington DC
T +1 202 457 6415
E pablo.carrillo@squirepb.com

Robert B. Kelly
Partner, Washington DC
T +1 202 626 6216
E robert.kelly@squirepb.com

Scott A. Warren
Partner, Tokyo
T +81 3 5774 1800
E scott.warren@squirepb.com

Daniel F. Roules
Partner, Shanghai
T +86 21 6103 6309
E daniel.roules@squirepb.com