When Connected Cars Meet National Security Concerns: Proposed Rule Prohibits Certain Russian and Chinese Software and Hardware in Connected and Automated Vehicles

Client Alert
10.3.2024

With vehicle connectivity becoming ubiquitous, massive amounts of data, through cameras, microphones, GPS tracking and other devices connected to the internet, are being captured and transmitted by connectivity hardware and software. Any threat to the connectivity supply chain could potentially upend the automotive supply chain. At the same time, the national security community has expressed serious concerns that technologies that enable vehicle connectivity systems (VCS) could endanger national security if that technology is controlled by U.S. adversaries, specifically, China and Russia. In response, last week, the U.S. Department of Commerce issued a Proposed Rule related to the sale of Chinese or Russian connected vehicle hardware and software. The Department's stated goal according to Under Secretary Alan F. Estevez is "to address this national security risk before Chinese and Russian suppliers proliferate within the U.S. automotive ecosystem." The Proposed Rule, if adopted, could both threaten supply chain continuity and create extremely complex compliance challenges for seeking to assess whether a transaction is covered by the Proposed Rule.

What is the Proposed Rule?

On September 26, 2024, the *Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles* notice of proposed rulemaking (the "Proposed Rule") was issued by the Commerce Department's Bureau of Industry and Security. The Proposed Rule seeks to prohibit importation or use of VCS hardware and software that are designed, developed, manufactured or supplied by entities that are owned by, controlled by, or subject to the jurisdiction or direction of the People's Republic of China (PRC) or the Russian Federation. Under the Proposed Rule, a VCS that was designed,

Related People

Jennifer A. Dukarski
Shareholder

Related Services

Automotive Industry Team

Connected Car and Autonomous Vehicles

White Collar Criminal Defense

developed, manufactured or supplied by a company that is owned or controlled by China or Russia may not be knowingly imported or sold by connected vehicle manufacturers and hardware importers, regardless of whether separately or in a complete vehicle.

The software prohibition would take effect for Model Year 2027 and the hardware prohibition would take effect for Model Year 2030, or January 1, 2029, for units without a model year. These proposed regulations would apply regardless of whether the vehicle was made in the United States.

Who Would Fall Under the New Regulation?

These prohibitions apply directly to two main groups: VCS hardware importers and connected vehicle manufacturers. A VCS hardware importer is a U.S. person or company that imports VCS hardware for further manufacturing, integration, resale or distribution. VCS hardware importers could be OEMs, suppliers, or aftermarket companies. A connected vehicle manufacturer is a company that either (1) manufactures or assembles a complete connected vehicle or (2) imports completed vehicles for sale in the U.S.

Indirectly, the Proposed Rule implicates anyone in the connected and automated driving supply chain who may source hardware or software from Russia or China.

What Does it Mean to be "Owned By" or "Controlled By"?

The Proposed Rules apply to anyone who sources or sells certain connected and automated technology coming from a "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary." The proposed regulation defines this level of control as:

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 United States citizen or permanent resident of the United States;
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 (a) through (c) 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. Sale means, in the context of

this subpart, distributing for purchase, lease, or other commercial operations a new completed connected vehicle for a price, to include the transfer of completed connected vehicles from a connected vehicle manufacturer to a dealer or distributor.

What Technology Falls Under This Proposed Regulation?

The Proposed Rule targets connected and automated hardware and software.

Under the Rule, connected vehicle hardware and software systems are defined that those who fall within telematics, cellular modems, antennas, and other components that use communications technologies that connect vehicles to external data sources. The Rule further includes automated driving systems (ADS) that operate at SAE Standard J3016 Levels 3, 4, and 5. The following are subject to the potential restrictions:

VCS Hardware: Software-enabled or programmable components and subcomponents that support the function of vehicle connectivity. These products include: 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).

Connected and Automated Vehicle Software: The software-based components that are part of an item that supports either vehicle connectivity or Level 3, 4, and 5 automated driving systems. It does not include firmware programmed for a hardware device that controls, configures or communicates with that device or open-source software unless that open-source software has been modified for proprietary purposes.

What Due Diligence and Documentation Does the Regulation Require?

The Proposed Rule includes several requirements for due diligence and documentation, including the preparation of Declarations of Conformity by VCS hardware importers and connected vehicle manufacturers. These importers and manufacturers must certify that the company has not knowingly imported prohibited transactions and provide a list of all third-party external endpoints where the hardware connects including the country where that endpoint is located or the location and identity of the service provider. For hardware, a hardware bill of materials (HBOM) must be provided along with due diligence, including third party or independent research to assure that the hardware isn't designed, developed, manufactured or supplied by Russian or Chinese entities. A software bill of materials (SBOM) must be provided for software. The company must also provide documentation of the due diligence efforts, which would include independent or hired third-party research, to ensure that the covered hardware and software listed in the bill of materials 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. It is highly likely that this will be cascaded through the supply chain by vehicle manufacturers and importers where appropriate.

This cascading of requirements and need to understand the depths of the supply chain may create significant compliance challenges. Full supply chain diligence is often plagued with the reality of data limitations. A supplier may request downstream information, but there may be a company in the chain that fails to request information further downstream or fails to fully vet that information. Terms and conditions themselves may not be sufficient to allow for an audit to assure compliance with the law. Additional risks may arise for companies seeking to identify the breadth of Chinese design and development based on the implementation of the Chinese state secrets law revisions. The revised law expands what information is deemed "sensitive" and therefore, full diligence may not be shared with international companies.

What are the Penalties for Failing to Comply?

Under the proposed regulation, failure to comply may subject a person to civil and criminal penalties under Section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705). The resulting civil penalty would be the greater of $250,000 or twice the amount of the transaction of the sale or importation. Criminal penalties include the potential of a fine of not more than $1,000,000, or imprisonment for not more than 20 years, or both. Any party trying to conceal a failure to comply would be further subject to 18 U.S.C. 1001, resulting in a fine and/or potential imprisonment.

Can I Comment on the Proposed Rule?

Yes. The Bureau of Industry and Security is accepting public comments for 30 days after publication (which was September 26, 2024). Comments for the Rule (docket number BIS-2024-0005 or RIN 0694-AJ56) must be submitted through the Federal eRulemaking Portal or emailed directly to connectedvehicles@bis.doc.gov with "RIN 0694-AJ56" included in the subject line. Your Butzel Automotive Team is available to assist in drafting or review of comments.

The Butzel Advantage

When new regulations and compliance is at stake, comprehensive experience is a must. Butzel's Automotive Team brings significant experience in the automotive industry, including design engineers, program managers, testing engineers and quality and manufacturing leaders. Butzel is uniquely positioned to assist in an audit and review of compliance with both regulations and industry standards across a tiered manufacturer's supply chain. Butzel's Automotive Team's unparalleled experience at automotive terms and conditions is critical in assuring that compliance is managed throughout an organization's supply chain.

Further, for any investigation, Butzel's White Collar Team has significant industry experience supporting some of the most well-known automotive compliance issues in the last two decades. Contact the author of this Alert or your Butzel attorney for further assistance.

Jennifer Dukarski
734.213.3427
dukarski@butzel.com