GIBSON DUNN

BIS Connected Vehicles Rule Effective as of March 17, 2025

Client Alert | March 19, 2025

A new Connected Vehicles Rule has arrived and with it, new requirements for supply chain due diligence for auto manufacturers and importers. As of March 17, 2025, a final rule[1] prohibiting the import and sale of certain connected vehicles and key components, including Vehicle Connectivity Systems (**VCS**) and Automated Driving Systems (**ADS**), has officially taken effect (the "**Connected Vehicles Final Rule**" or "**Final Rule**"). Issued by the U.S. Department of Commerce's Office of Information and Communications Technology and Services (**OICTS**) within the Bureau of Industry and Security (**BIS**), the Connected Vehicles Final Rule applies to hardware and software products made in, or incorporating parts or technology sourced from, Russia or China. The Final Rule will significantly impact companies importing or manufacturing connected vehicles and related systems, particularly those with supply chains linked to China and Russia. The Final Rule addresses concerns about risks posed by certain autonomous and connectivity technologies from China and Russia, notably regarding the potential for unauthorized access to sensitive data and internal vehicle systems. Compliance with this Final Rule, which introduces new declaratory and due diligence obligations, will require careful evaluation of hardware and software sourcing, potentially altering existing automotive supply chains. **I. Key Takeaways** Below we outline key takeaways and the near-term implications of the Connected Vehicles Final Rule.

- Under the Final Rule, "**VCS Hardware Importers**" and "**Connected Vehicle Manufacturers**" (as defined below in Section III) will be prohibited from engaging in certain sale or import transactions involving VCS hardware and software and ADS software connected to Chinese-affiliated or Russian-affiliated companies for future model year vehicles.[2]
- In addition, Connected Vehicle Manufacturers with a sufficient nexus to China or Russia will be prohibited from knowingly selling new connected vehicles that incorporate covered VCS hardware or software or ADS software in the United States, even if the vehicle was made in the United States.
- Software-related prohibitions will take effect for model year 2027. Hardware-related prohibitions will take effect for model year 2030, or January 1, 2029, for units without a model year. Prohibitions on the sale of connected vehicles by manufacturers with a sufficient nexus to China or Russia, even if manufactured in the United States, take effect for model year 2027.
- In coming years, affected companies will need to submit a Declaration of Conformity for any imports of VCS or ADS software, or systems containing such software, involving foreign interests[3]—even a non-Chinese or non-Russian interest—at least once a year for each affected part or model year vehicle; conduct supply chain due diligence to ensure compliance with the Connected Vehicles Final Rule; and keep records of relevant transactions for up to 10 years.
- The Final Rule applies only to passenger vehicles under 10,001 pounds, though BIS announced in its press release that a rule for commercial vehicles is forthcoming.[4]

The Final Rule was announced on January 14, 2025, and follows a Notice of Proposed Rulemaking (**NPRM**)[5] published by BIS on September 26, 2024, as well as an Advance

Related People

Chris R. Mullen

Hugh N. Danilack

Christopher T. Timura

Adam M. Smith

Stephenie Gosnell Handler

Vivek Mohan

Roxana Akbari

Soumya B. Kandukuri

Notice of Proposed Rulemaking (**ANPRM**)[6] published by BIS on March 1, 2024. Authorized under Executive Order 13873, the Final Rule grants the Secretary of Commerce and his delegates the authority to mitigate "undue" or "unacceptable" risks to national security from information and communications technology and services transactions involving "**foreign adversaries.**"[7] However, the specific prohibitions in the Connected Vehicles Final Rule are currently limited to China and Russia.[8] BIS's Compliance and Application Reporting System (**CARS**) webpage is currently live and accepting submissions from industry users for (1) Specific Authorization Applications, (2) Declarations of Conformity, and (3) Advisory Opinion Requests, which are discussed in greater detail below. BIS has also issued several "Frequently Asked Questions" related to these topics.[9] At a high level, the Final Rule broadly applies to connected vehicles that are "manufactured primarily for use on public streets, roads, and highways" with onboard technology that allows the vehicle to communicate with external networks.[10] This includes on-road vehicles with onboard systems capable of communicating with external networks or devices via Bluetooth, cellular, satellite, or Wi-Fi. Considering the ubiquity of this technology in modern cars, BIS initially anticipated in September's NPRM that the Final Rule would cover essentially "all new vehicles sold in the United States"[11] after the Final Rule takes effect for model year 2030 vehicles. However, in the Final Rule, BIS specified that vehicles not meeting the weight or passenger requirements for a "connected vehicle," including recreational vehicles and agricultural equipment, would not be affected.[12] BIS acknowledged that it will take time for manufacturers to evaluate and adjust their supply chains to comply with the Final Rule and accounted for this transition period through a staggered implementation model. **II. Policy Considerations Underlying the Final Rule**

A. National Security Concerns

The U.S. government has long been concerned with physical and information security risk posed by interference with autonomous vehicles (**AV**s) by foreign adversaries. Increasingly, lawmakers have become concerned with advanced technology, including technology allowing for the remote control of a vehicle, because such technology could allow bad actors to take over steering or operation of a car. AVs collect relatively advanced GPS and location data. AV technology also relies on camera and visuospatial data collection, some of which may be processed outside the vehicle. The NPRM specifically intended to address lawmakers' concerns that if a foreign adversary were permitted to gain access to those data sources, it could collect and exfiltrate extensive video or photo data of sensitive locations like military bases and secure facilities (e.g., server farms or data warehouse locations), as well as personal data regarding driving habits and locations.[13] The Final Rule is similarly aimed at preventing technology with such vulnerabilities to be used in cars sold on the U.S. market.

a. China

In the Final Rule, BIS expressed national security concerns with the use of Chinese hardware and software in U.S. connected vehicles, premised largely on China's "military-civil fusion strategy."[14] In addition, BIS explained that Chinese laws require Chinese-registered companies to provide business information and other data to the Chinese government on request, regardless of their location.[15]

b. Russia

Though Russia has historically been less active in the global automotive industry, the Russian government has recently sought to revitalize its domestic auto manufacturing sector, experiencing a projected 15% increase in passenger vehicle sales in 2024 alone.[16] The Russian government also employs a suite of laws that enable it to compel domestic companies with overseas operations to surrender data and similar operational assets gleaned through foreign ventures.[17] For these reasons, BIS remains concerned

that concerted efforts by the Russian government to develop the domestic Russian automotive industry, the growing U.S. electric vehicle (**EV**) market, and Russian resilience to Western sanctions and export control regimes increase the likelihood that Russia-linked connected vehicle technology will enter the U.S. connected vehicle supply chain and pose an undue or unacceptable risk to U.S. national security.[18]

B. Economic Competition

The Final Rule also appears motivated by efforts to promote the development of domestic EV and AV production, including technologies associated with those vehicles. By prohibiting the importation of cars equipped with covered technology from China, the U.S. government has sought to promote the onshore development of that technology or, at least, sourcing that technology from markets other than China. Because Chinese manufacturers dominate the EV battery market, this effort appears aimed at driving car companies out of China and stunting the growth of Chinese EV and AV industries. Though domestic industry was not a focus of the Final Rule, the Final Rule dovetails with other Biden-era U.S. government measures, including the 2022 Inflation Reduction Act (**IRA**), which limited tax credits for consumer EVs that use batteries made in China,[19] and the Biden administration's tariff increase on Chinese EVs from 25% to 100% under Section 301 of the Trade Act of 1974, which came into effect in September 2024.[20] However, the transition to the Trump administration has somewhat altered the federal government's approach to EVs. While the Final Rule remains in place, President Trump has shown little interest in expanding the EV market or maintaining strong incentives for domestic EV production. His administration has already begun rolling back Biden-era policies aimed at increasing EV uptake, including reviewing tax credits, freezing funding for charging infrastructure, and reconsidering the 2024 vehicle emissions rules, which sought to reduce tailpipe emissions by nearly 50% by 2032.[21] These reversals represent a shift away from government-driven EV expansion. That said, President Trump has maintained a hardline stance on limiting China's role in the auto industry. His administration has continued efforts to curb Chinese EV imports and reduce reliance on Chinese battery technology, primarily through expanded trade restrictions. In February 2025, he imposed additional tariffs on Chinese imports, which also apply to EVs, reinforcing earlier tariff increases under the Biden administration.[22] His administration has also considered implementing Section 232 tariffs on Chinese EV supply chain components, such as batteries and critical minerals, for national security reasons.[23] On balance, despite his broader skepticism of government-backed EV policies, President Trump has highlighted American EV manufacturing as a demonstration of domestic industrial strength, emphasizing the importance of domestic production over reliance on foreign competitors. This reflects a nuanced approach to EV policy, one that rejects federal incentives and emissions regulations but still prioritizes restricting China's influence in the global auto industry.

C. Convergence of Regulatory Focus on Supply Chains

China is currently the dominant player in the battery market, with Chinese companies producing 80% of global EV batteries as of March 2025.[24] Access to high-voltage batteries and battery technology are necessary components of EV manufacturing and therefore critical to the expansion of the domestic EV market. Major battery manufacturers in China have been identified as having continued ties to forced labor in the Xinjiang region of China.[25] The Uyghur Forced Labor Prevention Act (**UFLPA**), which took effect in June 2022, prohibits import of "any goods, wares, articles, and merchandise mined, produced, or manufactured wholly or in part in the Xinjiang Uyghur Autonomous Region of the People's Republic of China."[26] Although ICTS is not explicitly tasked with combatting forced labor, we assess that—just as with efforts to strengthen domestic manufacturing—the Final Rule nevertheless strengthens a constellation of efforts to deter the use of forced labor abroad, combat the corollary economic benefits to China and Chinese companies, and keep products made using forced labor from reaching our shores. **III. Key Provisions of the Final Rule** The Final Rule defines "**Connected Vehicle**" as any on-road vehicle that "integrates onboard networked hardware with

automotive software systems to communicate via dedicated short-range communication, cellular telecommunications connectivity, satellite communication, or other wireless spectrum connectivity with any other network or device."[27] ***Scope of Covered Parties.*** The Final Rule applies to all "**Connected Vehicle Manufacturers**," defined as a "U.S. person who (1) [m]anufactures or assembles completed connected vehicles in the United States for sale; (2) [i]mports completed connected vehicles for sale in the United States; and/or (3) [i]ntegrates ADS software on a completed connected vehicle for sale in the United States,"[28] as well as to "**VCS Hardware Importers**," who are "U.S. person[s] who import (1) VCS hardware for further manufacturing, incorporation, or integration into a completed connected vehicle that is intended to be sold or operated in the United States or (2) VCS hardware that has already been installed, incorporated, or integrated into a connected vehicle, or a subassembly thereof, that is intended to be sold as part of a completed connected vehicle in the United States."[29] The Final Rule prohibits these Connected Vehicle Manufacturer and VCS Hardware Importers from importing into the United States vehicles with "**Covered Software**," defined as "software-based components, including application, middleware, and system software in which there is a *foreign interest*, executed by the primary processing unit or units of an item that directly enables the function of the Vehicle Connectivity Systems or Automated Driving Systems at the vehicle level"—with limited exclusions.[30] ***Changes in "Covered Software" Definition.*** Based on public comments on the Proposed Rule, BIS changed its definition of "Covered Software," narrowing its scope from software that "supports" the function of Vehicle Connectivity Systems and Automated Driving Systems to software that "directly enables" these systems.[31] Software subcomponents, including "legacy codes" designed, developed, or supplied before March 17, 2026, are excluded from the definition of "Covered Software," provided they are not modified or maintained by entities controlled by foreign adversaries after that date. This exclusionary period—introduced in response to industry concerns—aims to prevent sudden market disruptions and provide the affected parties with additional time to adapt to the new requirements. ***Changes in the Definition of VCS.*** **VCS** includes any "hardware or software item installed in or on a completed connected vehicle that directly enables the function of transmission, receipt, conversion, or processing of radio frequency communications at a frequency over 450 megahertz," such as Bluetooth, cellular, satellite, or Wi-Fi connections as well as microcontrollers and/or modules enabling such functions.[32] BIS excluded certain common hardware and software components[33] with limited connectivity capabilities from the definition based on the reasoning that they do not pose as significant a risk as initially anticipated. ***Changes in the Definition of ADS.*** **ADS** includes "hardware and software that, collectively, are capable of performing the entire dynamic driving task for a completed connected vehicle on a sustained basis, regardless of whether it is limited to a specific operational design domain."[34] Notably, the Final Rule only applies to systems that allow a vehicle to operate autonomously at Levels 3 and above of automation (per SAE International standards).[35] Systems classified as Levels 0 to 2 (e.g., cruise control, lane keeping assistance program) do not qualify as ADS because they rely on the driver making decisions while operating the vehicle and require the driver's engagement and attention to do so.[36] ***Changes in the Definition of a "Person Owned by, Controlled by, or Subject to the Jurisdiction or Direction of a Foreign Adversary."*** The Final Rule establishes specific standards for determining whether a party has a covered connection to a foreign adversary and is, therefore, subject to the prohibitions of the Final Rule. If any of the following criteria are met, the person is considered "**owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary**":

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; or
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 [above] 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.[37]

Most notably, U.S. and EU-based companies with joint ventures, subsidiaries, or affiliates incorporated in a foreign adversary may also fall within the above definition, though as noted previously, the prohibitions in the Final Rule are limited to "persons owned by, controlled by, or subject to the jurisdiction or direction of" China and Russia. Vehicle manufacturers, importers, and exporters operating subsidiaries in these jurisdictions should conduct a thorough risk assessment to ensure compliance with the Final Rule. Additionally, BIS clarified that in determining whether VCS hardware or connected vehicles that incorporate Covered Software are "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of [China] or Russia," BIS will not make its determination "based solely on the country of citizenship of one or more natural persons who are employed by, contracted by, or otherwise similarly engaged in such actions through the entity designing, developing, manufacturing, or supplying the hardware."[38] Therefore, companies will need to undertake a careful analysis of their supply chains to determine when a supplier does or does not qualify as "owned by, controlled by, or subject to the jurisdiction or direction of" China or Russia. The first model year to be impacted by the regulations will be model year 2027, which provides auto manufacturers and their suppliers only a brief time to map their supply chains and, when necessary, locate and qualify alternate non-China and Russia-linked suppliers for VCS and ADS software systems (as related hardware prohibitions came into effect for subsequent model years).[39] ***Advisory Opinions.*** The Final Rule also establishes an advisory opinion process to allow VCS Hardware Importers and Connected Vehicle Manufacturers to obtain guidance from BIS on whether a prospective transaction may be prohibited.[40] Such requests may be submitted via the CARS webpage and must involve actual (not hypothetical) transactions and disclose the proposed parties to the transaction. **IV. Timing and Implementation** Based on the understanding that it will take time for Connected Vehicle Manufacturers and VCS Hardware Importers to evaluate and adjust their supply chains to comply with the new regulations, BIS has established the following timeline for when the prohibitions will take effect:

- **Model Years 2027–2029 vehicles**: Connected Vehicle Manufacturers are prohibited from knowingly importing into and selling within the United States connected vehicles containing Covered Software designed, developed, manufactured, or supplied by persons linked China or Russia. This includes completed connected vehicles that incorporate covered VCS or ADS software designed, developed, manufactured, or supplied by "persons owned by, controlled by, or subject to the jurisdiction or direction of [China] or Russia," regardless of whether the vehicles are manufactured or assembled in the United States.[41]
- **Model Year 2030 vehicles or, for hardware not associated with a vehicle model year, as of January 1, 2029**: Connected Vehicle Manufacturers are prohibited from knowingly importing VCS hardware *or* connected vehicles containing VCS hardware designed, developed, manufactured, or supplied by "persons owned by, controlled by, or subject to the jurisdiction or direction of [China] or Russia," or knowingly selling the same within the United States.[42]

While BIS may have intended staggering effective dates of the new prohibitions for

different model years and focusing on software first to be less disruptive for industry, we note that the software affected by the rule's earliest implementation date can be highly specific to the hardware on which VCS and ADS systems rely to gather and process relevant sensor data. Connected Vehicle Manufacturers will likely need to review and modify their software and hardware in tandem in order to be in a position to continue importing their cars and ADS and VCS systems, parts, and components by mid-2026.

V. Compliance Obligations The Final Rule imposes three additional compliance measures: (1) Declarations of Conformity, (2) recordkeeping, and (3) supply chain due diligence requirements.

1. **Declarations of Conformity**: The Final Rule requires VCS Hardware Importers and Connected Vehicle Manufacturers to submit Declarations of Conformity to BIS at least 60 days prior to the importation of the first import or sale of items associated with a particular vehicle model or calendar year beginning for model year 2027.[43] Declarations of Conformity will be required annually thereafter and whenever a VCS Hardware Importer or Connected Vehicle Manufacturer discovers a "material change" to the information conveyed that makes a prior Declaration of Conformity "no longer to the information conveyed in a previously submitted Declaration of Conformity.[44] Such material change updates must be submitted within 60 days of the discovery of the change, and the obligation remains ongoing until 10 years after submission of the original Declaration of Conformity.[45]
    a. **Submission Procedures**: The Declaration of Conformity form is accessed and submitted through BIS's CARS webpage.[46] OICTS recommends the prioritization of Declarations of Conformity for covered software transactions "due to the separate implementation timelines for the covered software and VCS hardware prohibitions."[47] A Declaration of Conformity may incorporate assessments produced by third parties as long as the assessment is disclosed.[48] If a previously submitted Declaration of Conformity remains accurate the following year, Connected Vehicle Manufacturers and VCS Hardware Importers may submit a confirmation that associates the relevant new model year vehicles to an existing Declaration of Conformity.[49] After the submission of a Declaration of Conformity, OICTS will only follow up directly if additional information is required.[50]
    b. **VCS Hardware Importers**: Prior to import of items for the covered model year vehicles described above, VCS Hardware Importers are required to submit a Declaration of Conformity for all VCS hardware not otherwise prohibited outlining, *inter alia*, detailed item information, due diligence efforts undertaken to ensure compliance with this rule, and third-party external endpoints to which the VCS hardware connects.[51] After considering public comments, BIS will no longer require the submission of Hardware Bills of Materials (**HBOMs**)[52] to support Declarations of Conformity.[53] However, BIS will require entities to maintain primary business records supporting their certification that they conducted adequate supply chain due diligence, which could include HBOMs.[54]
    c. **Connected Vehicle Manufacturers**: Connected Vehicle Manufacturers will be required to submit a Declaration of Conformity for the covered model year vehicles described above prior to import that includes, *inter alia*, information on the make, model, and trim of the group of completed vehicles and any "Covered Software" contained within the completed vehicles.[55] BIS requires **Connected Vehicle Manufacturers** to keep documentation supporting these Declarations as well, which may be in the form of Software Bills of Materials (**SBOM**).[56] Notably, BIS makes clear that Declarations of Conformity are not required if "the only foreign interest in a transaction [with respect to the "Covered Software" contained within the vehicle] arises from a foreign person's equity ownership of a U.S. person, whether through public shares or otherwise.[57]

2. **Recordkeeping**: Under the Final Rule, VCS Hardware Importers and Connected Vehicle Manufacturers will be obliged to maintain all primary business records related to the execution of each transaction for which Declarations of Conformity and authorizations have been sought for a minimum of 10 years after the date of submission. These records must be furnished on demand to BIS.[58] As described above, while HBOMs and SBOMs are not required to support a Declaration of Conformity, they can nevertheless be useful for this purpose where they are available.

3. **Due Diligence**: The Final Rule requires companies to undertake due diligence of their entire supply chain, including third-party suppliers and contractors. To support this endeavor, the Final Rule provides that companies may optionally use a qualified third-party assessor to ensure compliance, though in certain cases, the use of a third-party assessor will be mandated in the terms of an approved specific authorization (as described below).[59] BIS provides the following minimum guidelines for third-party assessors, which may also be illustrative in understanding how BIS would audit the due diligence efforts of covered VCS Hardware Importers and Connected Vehicle Manufacturers:

    a. Identify the suppliers of each relevant component and describe the nature of any foreign interest;

    b. Describe the methodology undertaken, including the policies and other documents reviewed, personnel interviewed, and any facilities, equipment, or systems examined;

    c. Describe the effectiveness of the VCS hardware importer or connected vehicle manufacturer's corporate policies related to compliance with this rule;

    d. For VCS Hardware Importers or Connected Vehicle Manufacturers conducting transactions under the auspices of a general authorization or specific authorization, describe any vulnerabilities, or deficiencies in the implementation of the authorization; and

    e. Recommend any improvements or changes to policies, practices, or other aspects to maintain compliance with this subpart, as applicable to each transaction.[60]

VI. General and Specific Authorizations ***General Authorizations*** BIS may issue General Authorizations for certain types of transactions otherwise prohibited, considering any information it deems relevant and appropriate.[61] OICTS will publish General Authorizations on its website and in the *Federal Register* as they are issued and will maintain a repository of previously issued General Authorization Letters for public reference.[62] If it is unclear whether a particular transaction is authorized under a General Authorization, industry users may request an Advisory Opinion from OICTS through a submission on the CARS webpage.[63] OICTS will issue an Advisory Opinion to the requestor within 60 days of receipt unless otherwise specified.[64] For transactions authorized by a General Authorization, the submission of a Declaration of Conformity for that transaction is not required.[65] ***Specific Authorizations*** BIS also may, at its discretion, issue Specific Authorizations on a case-by-case basis in response to applications submitted through the CARS webpage by affected parties and will consider both the import's risk factors and proposals that the applicant offers to implement to mitigate such risks.[66] OICTS encourages requestors to include in their Specific Authorization applications as many details and materials as possible to demonstrate any nexus with China and/or Russia as it relates to covered software and VCS hardware, as well as mitigation measures the company has or intends to implement.[67] Similar to their recommendation for Declarations of Conformity, OICTS advises that applicants prioritize Specific Authorizations for covered software transactions "due to the separate implementation timelines for the covered software and VCS hardware prohibitions."[68] The Final Rule establishes that BIS will respond to applicants, in most cases, with an

update within 90 days of the initial application.[69] While reviewing a Specific Authorization application, OICTS may request additional information, including an oral briefing.[70] As a condition to granting a Specific Authorization, OICTS may "require unique terms" regarding compliance, auditing, or verification requirements to "mitigate any risk arising from the otherwise prohibited transaction."[71] Generally, Specific Authorizations will be approved for no less than one model year.[72] **VII. Penalties** Violations under the Final Rule are punishable by civil and criminal penalties under the International Emergency Economic Powers Act (**IEEPA**).[73] Civil penalties under IEEPA consist of monetary fines up to $377,700 per violation (an amount adjusted annually for inflation) or twice the value of the transaction, whichever is greater.[74] In case of willful violation, criminal penalties can reach up to a fine of $1,000,000, and if the violator is a natural person, the criminal penalty is either imprisonment for no more than 20 years, or both a fine and imprisonment.[75] **VIII. Impact of the Final Rule** The Final Rule requires auto manufacturers and importers to carefully and thoroughly review their supply chains and due diligence processes. As explained above, the Final Rule takes a staggered approach—it would impose a narrower set of obligations beginning with model years 2027–2029 (applying only to VCS and ADS connected software) and expand to include hardware for model year 2030 and beyond (at which point the Final Rule will apply to both software and hardware). This staggered approach is intended to allow manufacturers and importers time to comply with the more onerous and comprehensive obligations for model years 2030 and beyond. Even still, the initial model year 2027 obligations are substantial and will implicate hardware design by default. Auto manufacturers have little more than 18 months to undertake the following:

1. **Identify which parts will be affected by the Final Rule.**

As described above, for model years 2027–2029, the Final Rule prohibits the importation or sale of connected vehicles equipped with covered VCS or ADS connected software designed, developed, manufactured, or supplied by certain persons linked to China or Russia. For model year 2030 and forward, the Final Rule expands to include both VCS or ADS software *and* hardware designed, developed, manufactured, or supplied by certain persons linked to China or Russia. Sophisticated hardware used in VCS and ADS technologies often takes years, potentially decades, to develop, and software is often built around specific hardware. This means that even though the Final Rule regulates only *software* for model years 2027–29, in reality, modifications to software may also affect hardware compatibility and require manufacturers to source new hardware long before the model year 2030 deadline. Accordingly, it is imperative that manufacturers start to understand how their supply chain may be affected by the Final Rule now.

2. **Evaluate and document sourcing for all affected parts.**

Manufacturers should endeavor to identify from where all components for affected parts are sourced and collect documentation detailing the same. If not in place already, manufacturers should ask sourcing entities to guarantee in writing that no relevant products in their supply chain come from "persons owned by, controlled by, or subject to the jurisdiction or direction of" China or Russia.[76] Collecting relevant documentation will be critical to comply with the Final Rule's requirement that manufacturers submit Declarations of Conformity to BIS, starting with model year 2027 vehicles.

3. **Source and replace affected software and hardware or related components.**

At present, a significant portion of technology supporting internet or Bluetooth connectivity in the United States is imported from China, including many hardware and software components. This means that (a) manufacturers will likely be required to replace at least some components in their supply chain for VCS and ADS hardware and software if they wish to continue importing vehicles containing these items into the United States, (b) manufacturers may have trouble sourcing these items from entities outside of China given China's current dominance, and (c) suppliers outside of China may be inundated with

similar requests and may not be able to keep up with the increased demand, resulting in supply chain delays. Ultimately, given these constraints, some vehicles that were in the supply chain pipeline for the U.S. market may no longer be releasable, causing delays for U.S. consumers hoping for access to cutting edge vehicles. Acting early is essential to ensuring that these changes will not cause disruptions to customers, damage brand loyalty, or harm manufacturers' and importers' fiscal interests.

4. Implement or bolster compliance protocols.

The Final Rule will require that manufacturers maintain records related to Declarations of Conformity and authorizations for a minimum of 10 years after the date of submission. Similarly, manufacturers will be expected to continually evaluate from where VCS and ADS hardware and software are sourced. Manufacturers should be prepared to bolster or implement sourcing controls and recordkeeping protocols to ensure compliance with the Final Rule. Gibson Dunn remains ready to assist parties in preparing for these changes, including supply chain diligence, sourcing documentation, preparing required declarations, and evaluating and fortifying your compliance programs and controls. [1] Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 90 Fed. Reg. 5,360 (Jan. 16, 2025) [hereinafter Connected Vehicles Final Rule] (codified at 15 C.F.R. § 791.300 *et seq.*). [2] This includes all Chinese and Russian companies involved in the connected vehicle supply chain (not merely automobile manufacturers), as well as their foreign affiliates. *See* 15 C.F.R. 791.301. [3] 90 Fed. Reg. at 5,382 ("[A] foreign interest can include, but is not limited to, an interest through ownership of the item itself, intellectual property present in the item, a contractual right to use, update, or otherwise impact the property, (e.g., ongoing maintenance commitments, any license agreement related to the use of intellectual property), profit-sharing or fee arrangement linked to the property, as well as any other cognizable interest."). However, as discussed herein, Declarations of Conformity will not be required "if the only foreign interest in a transaction arises from a foreign person's equity ownership of a U.S. person, whether through ownership of public shares or otherwise." 15 C.F.R. § 791.305(*l*). [4] Press Release, BIS, Commerce Finalizes Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats, BIS Press Release (Jan. 14, 2025), https://www.bis.gov/press-release/commerce-finalizes-rule-secure-connected-vehicle-supply-chains-foreign-adversary ("BIS recognizes the acute national security threat presented by foreign adversary involvement in the commercial vehicle supply chain and intends to issue a separate rulemaking addressing the technologies present in connected commercial vehicles – including in trucks and buses – in the near future."). [5] Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 89 Fed. Reg. 79,088, 79,116 (Sept. 26, 2024) [hereinafter **NPRM**]. [6] Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 89 Fed. Reg. 15,066 (Mar. 1, 2024) [hereinafter **ANPRM**]. [7] "Foreign adversaries" are currently defined as the People's Republic of China, including Hong Kong and Macau ("China"), Cuba, Iran, North Korea, Russia, and the regime of "Venezuelan politician Nicolás Maduro"—though, as discussed above, the prohibitions in the Final Rule apply directly to China and Russia. 15 C.F.R. § 791.4. [8] *See* 15 C.F.R. §§ 791.302–305. [9] *See Connected Vehicles*, BIS, https://www.bis.gov/node/22645 (last accessed Mar. 18, 2025). [10] Connected Vehicles Final Rule, 90 Fed Reg. at 5,374. [11] NPRM, 89 Fed. Reg. at 79,091. [12] Connected Vehicles Final Rule, 90 Fed Reg. at 5,374–75. [13] NPRM, 89 Fed. Reg. at 79,089. [14] Connected Vehicles Final Rule, 90 Fed. Reg. 5,360, at 5,367. [15] *See id.* [16] *See id.* at 5,368. [17] *See id.* at 5,369. [18] *See id.* [19] *See* Matthew Broersma, *US House Passes Bill Targeting Chinese EV Battery Tech*, Silicon (Sept. 16, 2024), https://www.silicon.co.uk/e-innovation/green-it/us-bill-china-battery-579757. [20] *See, e.g.*, David Shepardson, *Trump Administration Takes Aim at Biden Electric Vehicle Rules,* Reuters (Mar. 12, 2025), https://www.reuters.com/sustainability/climate-energy/trump-administration-begins-effort-reverse-epa-vehicle-rules-2025-03-12/. [21] *See, id.* [22] Fact Sheet: President Donald J. Trump Imposes Tariffs on Imports from Canada, Mexico, and China, White House (Feb. 1, 2025), https://www.whitehouse.gov/fact-sheets/2025/02/fact-sheet-president-donald-j-trump-imposes-tariffs-on-imports-from-canada-mexico-and-china/. [23] *See*, e.g., Jarret Renshaw & Chris

Kirkham, *Exclusive: Trump Transition Team Plans Sweeping Rollback of Biden EV, Emissions Policies*, Reuters (Dec. 17, 2024), https://www.reuters.com/business/autos-transportation/trump-transition-team-plans-sweeping-rollback-biden-ev-emissions-policies-2024-12-16/. [24] *See, e.g.*, Christian Shepherd, *How China Pulled Ahead to Become the World Leader in Electric Vehicles,* Wash. Post (Mar. 3, 2025), https://www.washingtonpost.com/world/2025/03/03/china-electric-vehicles-jinhua-leapmotor/. [25] *EV Batteries and Forced Labor: Investigating Possible Links Between CATL and Xinjiang-Based Companies*, Sayari (May 16, 2024), https://sayari.com/wp-content/uploads/2024/05/Sayari_EV_Batteries_Report.pdf. [26] *Uyghur Forced Labor Prevention Act*, U.S. Customs & Border Protection (Oct. 16, 2024), https://www.cbp.gov/trade/forced-labor/UFLPA; *see* Uyghur Forced Labor Prevention Act, Pub. L. No. 117-78, 135 Stat. 1525. [27] 15 C.F.R. § 791.301. [28] *Id.* [29] *Id.* [30] *Id.* (emphasis added). The following categories are notably excluded from the definition of "Covered Software": (1) firmware (i.e., "software specifically programmed for a hardware device with a primary purpose of directly controlling, configuring, and communicating with that hardware device"; (2) open-source software (i.e., "software for which the human-readable source code is available in its entirety for use, study, re-use, modification, enhancement, and redistribution by the users of such software"), provided such software has not been modified for proprietary purposes and not redistributed or shared; and (3) software subcomponents that were "designed, developed, manufactured, or supplied prior to March 17, 2026, as long as those software subcomponents are not maintained, augmented, or otherwise altered by an entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary after March 17, 2026." *Id.* [31] *See* NPRM, 89 Fed. Reg. at 79,116; *see also* 15 C.F.R. § 791.300. [32] 15 C.F.R. § 791.300. [33] BIS excluded hardware or software that exclusively: "(1) enables the transmission, receipt, conversion, or processing of automotive sensing (e.g. LiDAR, radar, video, ultrawideband); (2) enables the transmission, receipt, conversion, or processing of ultrawideband communications to directly enable physical vehicle access (e.g., key fobs); (3) enables the receipt, conversion or processing of unidirectional radio frequency bands (e.g., global navigation satellite systems (GNSS), satellite radio, AM/FM radio); or (4) supplies or manages power for the VCS." *Id*. [34] *Id.* [35] Connected Vehicles Final Rule, 90 Fed. Reg. at 5,373. [36] *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_202104*, SAE International (Apr. 30, 2021), https://www.sae.org/standards/content/j3016_202104; *see* Connected Vehicles Final Rule, 90 Fed. Reg. at 5,364. [37] *See* 15 C.F.R. § 791.301. [38] *Id.* §§ 791.302(b), 791.303(c). [39] *See id*. § 791.308. [40] *See id*. § 791.310. [41] *Id*. § 791.302; *see id*. § 791.308. [42] *Id*. §§ 791.303–791.304; *see id*. § 791.308. [43] *Id*. §§ 791.305, 791.308. [44] *See id*. § 791.305. [45] *Id*. § 791.305(g). The 60-day timeline for submitting updates to a Declaration of Conformity reflects a key change from the original 30-day timeline in the Proposed Rule. *See* Connected Vehicles Final Rule, 90 Fed. Reg. at 5,396. [46] Compliance Application and Reporting System, BIS, https://cars.bis.gov (last accessed Mar. 18, 2025). [47] Declarations of Conformity Frequently Asked Questions, BIS, https://www.bis.gov/oicts/connected-vehicles/declarations-of-conformity (last accessed Mar. 18, 2025); . [48] *Id.* [49] *Id.* [50] *Id.* [51] 15 C.F.R. § 791.305(a)(1). [52] Hardware Bill of Materials **(HBOM)** means "a formal record [of] the supply chain relationships of parts, assemblies, and components required to create a physical product, including information identifying the manufacturer and related firmware." *See id*. § 791.301. [53] *See* Connected Vehicles Final Rule, 90 Fed. Reg. at 5,383. [54] *See id.* [55] *See* 15 C.F.R. § 791.305(a)(2). [56] Software Bill of Materials **(SBOM)** means "a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product." *Id*. § 791.301. [57] *Id.* § 791.305(*l*). [58] *See id.* §§ 791.312–791.313(a). [59] *See id.* § 791.315(a). [60] *See id.* § 791.315(d). [61] *See id.* § 791.306. [62] General Authorizations Frequently Asked Questions, BIS, https://www.bis.gov/oicts/connected-vehicles/general-authorizations (last accessed Mar. 18, 2025). [63] *Id.* [64] Advisory Opinion Frequently Asked Questions, BIS, https://www.bis.gov/oicts/connected-vehicles/advisory-opinions (last accessed Mar. 18, 2025). [65] General Authorizations Frequently Asked Questions, BIS,

https://www.bis.gov/oicts/connected-vehicles/general-authorizations (last accessed Mar. 18, 2025). [66] *See* 15 C.F.R. § 791.307; Specific Authorizations Frequently Asked Questions, BIS, https://www.bis.gov/oicts/connected-vehicles/specific-authorizations (last accessed Mar. 18, 2025). [67] Specific Authorizations Frequently Asked Questions, BIS, https://www.bis.gov/oicts/connected-vehicles/specific-authorizations (last accessed Mar. 18, 2025). [68] *Id.* [69] *See* 15 C.F.R. § 791.315(h). [70] Specific Authorizations Frequently Asked Questions, BIS, https://www.bis.gov/oicts/connected-vehicles/specific-authorizations (last accessed Mar. 18, 2025). [71] *Id.* [72] *Id.* [73] *See* 15 C.F.R. § 791.318. [74] *See* 50 U.S.C. § 1705; *see also* Inflation Adjustment of Civil Monetary Penalties, 89 Fed. Reg. 106,308, 106,310 (Dec. 30, 2024). [75] *See* 15 C.F.R. § 791.318. [76] *See id*. § 791.301; *supra* Section III.

The following Gibson Dunn lawyers prepared this update: Roxana Akbari, Soumya Bhat Kandukuri*, Soo-Min Chae*, Hayley Lawrence, Lindsay Bernsen Wardlaw, Chris Mullen, Hugh Danilack, Christopher T. Timura, Adam M. Smith, Stephenie Gosnell Handler, and Vivek Mohan.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these issues. For additional information about how we may assist you, please contact the Gibson Dunn lawyer with whom you usually work, the authors, or the following leaders and members of the firm's International Trade Advisory & Enforcement practice group: **United States**: Ronald Kirk – Co-Chair, Dallas (+1 214.698.3295, rkirk@gibsondunn.com) Adam M. Smith – Co-Chair, Washington, D.C. (+1 202.887.3547, asmith@gibsondunn.com) Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com) Donald Harrison – Washington, D.C. (+1 202.955.8560, dharrison@gibsondunn.com) Christopher T. Timura – Washington, D.C. (+1 202.887.3690, ctimura@gibsondunn.com) Matthew S. Axelrod – Washington, D.C. (+1 202.955.8517, maxelrod@gibsondunn.com) David P. Burns – Washington, D.C. (+1 202.887.3786, dburns@gibsondunn.com) Nicola T. Hanna – Los Angeles (+1 213.229.7269, nhanna@gibsondunn.com) Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com) Courtney M. Brown – Washington, D.C. (+1 202.955.8685, cmbrown@gibsondunn.com) Amanda H. Neely – Washington, D.C. (+1 202.777.9566, aneely@gibsondunn.com) Samantha Sewall – Washington, D.C. (+1 202.887.3509, ssewall@gibsondunn.com) Michelle A. Weinbaum – Washington, D.C. (+1 202.955.8274, mweinbaum@gibsondunn.com) Hugh N. Danilack – Washington, D.C. (+1 202.777.9536, hdanilack@gibsondunn.com) Mason Gauch – Houston (+1 346.718.6723, mgauch@gibsondunn.com) Chris R. Mullen – Washington, D.C. (+1 202.955.8250, cmullen@gibsondunn.com) Sarah L. Pongrace – New York (+1 212.351.3972, spongrace@gibsondunn.com) Anna Searcey – Washington, D.C. (+1 202.887.3655, asearcey@gibsondunn.com) Audi K. Syarief – Washington, D.C. (+1 202.955.8266, asyarief@gibsondunn.com) Scott R. Toussaint – Washington, D.C. (+1 202.887.3588, stoussaint@gibsondunn.com) Lindsay Bernsen Wardlaw – Washington, D.C. (+1 202.777.9475, lwardlaw@gibsondunn.com) Shuo (Josh) Zhang – Washington, D.C. (+1 202.955.8270, szhang@gibsondunn.com) **Asia**: Kelly Austin – Denver/Hong Kong (+1 303.298.5980, kaustin@gibsondunn.com) David A. Wolber – Hong Kong (+852 2214 3764, dwolber@gibsondunn.com) Fang Xue – Beijing (+86 10 6502 8687, fxue@gibsondunn.com) Qi Yue – Beijing (+86 10 6502 8534, qyue@gibsondunn.com) Dharak Bhavsar – Hong Kong (+852 2214 3755, dbhavsar@gibsondunn.com) Arnold Pun – Hong Kong (+852 2214 3838, apun@gibsondunn.com) **Europe**: Attila Borsos – Brussels (+32 2 554 72 10, aborsos@gibsondunn.com) Patrick Doris – London (+44 207 071 4276, pdoris@gibsondunn.com) Michelle M. Kirschner – London (+44 20 7071 4212, mkirschner@gibsondunn.com) Penny Madden KC – London (+44 20 7071 4226, pmadden@gibsondunn.com) Irene Polieri – London (+44 20 7071 4199, ipolieri@gibsondunn.com) Benno Schwarz – Munich (+49 89 189 33 110, bschwarz@gibsondunn.com) Nikita Malevanny – Munich (+49 89 189 33 224, nmalevanny@gibsondunn.com) Melina Kronester – Munich (+49 89 189 33 225, mkronester@gibsondunn.com) Vanessa Ludwig – Frankfurt (+49 69 247 411 531, vludwig@gibsondunn.com) **Soumya Kandukuri, an associate in Palo Alto, and Soo-*

Min Chae, a visiting attorney in Washington, D.C., are not admitted to practice law.

Related Capabilities

International Trade Advisory and Enforcement

Artificial Intelligence