

Client Alert

International Trade

OCTOBER 21, 2024

For more information,
contact:

Christine E. Savage
+1 202 626 5541
csavage@kslaw.com

Jamieson L. Greer
+1 202 626 5509
jgreer@kslaw.com

J. Philip Ludvigson
+1 202 626 9267
pludvigson@kslaw.com

Danielle Pressler
+1 202 626 9122
dpressler@kslaw.com

Adam Harper
+1 202 393 3799
arharper@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue,
NW
Suite 900
Washington, D.C. 20006
Tel. +1 202 737 0500

Biden Administration Issues Proposed Rule Targeting “Connected Vehicles” Tied to China or Russia

The Proposed Rule imposes substantial new reporting, diligence, and compliance obligations for companies in the automotive supply chain

On September 26, 2024, the U.S. Department of Commerce’s Bureau of Industry and Security (“BIS”) issued a proposed rule related to the information and communications technology and services (“ICTS”) supply chain that will prohibit certain transactions involving “connected vehicles” and Vehicle Connectivity System (“VCS”) hardware and software or Automated Driving System (“ADS”) software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of China (including Hong Kong) or Russia (the “Proposed Rule”).ⁱ The Proposed Rule builds on and incorporates public feedback from a March 1, 2024, Advance Notice of Proposed Rulemaking (the “ANPRM”) and aims to protect certain automotive critical technologies that are most vulnerable to exploitation or sabotage by foreign adversaries.

If adopted, the Proposed Rule will have sweeping compliance implications on the automotive industry, as well as component manufacturers and suppliers and software developers in the automotive supply chain. Pursuant to the Proposed Rule, VCS hardware importersⁱⁱ and connected vehicle manufacturersⁱⁱⁱ will be subject to substantial new requirements that are likely to require implementation of extensive compliance measures, including with respect to due diligence, policies and procedures, supplier agreement and contract provisions, recordkeeping, and reports to the U.S. government. Under the Proposed Rule,



automotive suppliers will need to assess their compliance programs to ensure they incorporate requirements of the Proposed Rule and any related authorizations, seek any desired guidance, and timely submit required information and updates to the U.S. government, as necessary.

BACKGROUND

BIS's Office of Information and Communications Technology and Security ("OICTS") will administer any Final Rule. OICTS is responsible for implementing the ICTS framework originally established by the May 2019 Executive Order [13873](#), "Securing the Information and Communications Technology and Services Supply Chain," which is based on the International Emergency Economic Powers Act ("IEEPA"), [50 U.S.C. § 1701 et seq.](#) (IEEPA).^{iv}

In its ANPRM, described in our previous [client alert](#), BIS identified six systems—vehicle operating systems, telematics systems, Advanced Driver-Assistance Systems, ADS, satellite or cellular telecommunications systems, and battery management systems—as ICTS potentially presenting undue or unacceptable risks. BIS is proposing to regulate "transactions involving two systems of ICTS integral to connected vehicles, VCS and ADS" under the Proposed Rule.^v Importantly, however, "BIS does not foreclose the possibility of further addressing other systems, including additional aspects of VCS and ADS, in future regulation."^{vi} The Proposed Rule will take effect 60 days after the final rule is published. BIS requested comments from the public on the Proposed Rule by October 28, 2024.

RULE PROHIBITIONS

If adopted, the Proposed Rule would—absent a General or Specific Authorization—prohibit the following:

- VCS hardware importers from **knowingly importing** into the United States **VCS hardware** that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of China or Russia;
- Connected vehicle manufacturers from **knowingly importing** into or **selling** in the United States **completed connected vehicles** that incorporate certain software that supports the function of VCS or ADS (collectively, "**covered software**") designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of Russia or China; and
- Connected vehicle manufacturers who are persons owned by, controlled by, or subject to the jurisdiction or direction of China or Russia from **knowingly selling** in the United States **completed connected vehicles that incorporate VCS hardware or covered software**.^{vii}

As noted above, if adopted, any Final Rule will take effect 60 days after it is published. However, implementation of the compliance obligations under the Proposed Rule will be phased in over time as follows:

- Beginning with model year ("MY") 2027, connected vehicle manufacturers are prohibited from importing into and selling in the United States connected vehicles containing covered software.
- Beginning with MY 2027, connected vehicle manufacturers that are owned by, controlled by, or subject to the jurisdiction or direction of China or Russia are prohibited from selling in the United States completed connected vehicles that incorporate VCS hardware or covered software.
- Beginning with MY 2030, VCS hardware importers are prohibited from importing VCS hardware (1) associated with a 2030 or later vehicle MY or (2) imported as part of a connected vehicles with a MY of 2030 or later. For VCS hardware not associated with a vehicle MY, the effective date is January 1, 2029.^{viii}



KEY DEFINITIONS AND CONCEPTS

The Proposed Rule defines certain key terms and concepts that affect the scope and application of the rule.

HARDWARE, SOFTWARE, AND VEHICLES SUBJECT TO THE PROPOSED RULE

- **ADS:** “Automated Driving System” is “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 (ODD).”^{ix}
 - ADS software includes software enabling the control of automated systems classified as Levels 3 – 5 by SAE International Standard J3016, which has been adopted by the National Highway Traffic Safety Administration, and does not include automated systems classified as Levels 0 – 2 that offer driver assistance through systems that control steering or acceleration and braking but still rely on the driver to make driving decisions.^x
- **VCS:** “Vehicle Connectivity System” is “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.”^{xi}
- **VCS Hardware:** The Proposed Rule defines “VCS hardware” as the following “software-enabled or programmable components and subcomponents that support the function of [VCS] or 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.”^{xii}
 - VCS hardware does not include component parts that do not contribute to the communication function of VCS hardware, such as brackets, fasteners, plastics, and passive electronics.
- **Covered Software:** “Covered software” is “software-based components, **in which there is a foreign interest**,^{xiii} 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 or open-source software unless the software has been modified for proprietary purposes and not redistributed or shared.^{xiv}
- **Connected Vehicles:** The Proposed Rule will cover “connected vehicles” that incorporate VCS hardware and/or covered software. BIS proposes to define “connected vehicle” as “a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways, 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.”^{xv} Vehicles operated only on a rail line will not be included in the definition. In the Proposed Rule, BIS states that it believes “with very few exceptions, all new vehicles sold in the United States will be captured by this definition.”^{xvi}



PERSONS OWNED BY, CONTROLLED BY, OR SUBJECT TO THE JURISDICTION OR DIRECTION OF A FOREIGN ADVERSARY

- The Proposed Rule prohibitions apply with respect to “persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary” and target China and Russia. The definition, as follows, is expansive and will have particularly broad reach.
 - **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;
 - 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 U.S. citizen or permanent resident of the United States;
 - 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
 - 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.**^{xvii}

PROHIBITION STANDARD

The prohibitions in the Proposed Rule are based on a knowledge standard, which includes positive knowledge and conscious disregard of facts or willful avoidance of facts. Specifically, the Proposed Rule defines “knowingly” as “having knowledge of a circumstance (the term may be a variant, such as ‘know,’ ‘reason to know,’ or ‘reason to believe’), to include 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.”^{xviii}

COMPLIANCE OBLIGATIONS AND AUTHORIZATIONS

The Proposed Rule will impose far-reaching compliance obligations on affected companies, primarily through an affirmative obligation to submit “Declarations of Conformity,” which require, among other things, compliance certifications and documents supporting such certifications. This obligation will, in turn, require a level of due diligence that allows companies to submit truthful and complete declarations. In certain limited circumstances, companies may be able to use General Authorizations or seek Specific Authorizations from BIS.



COMPLIANCE OBLIGATIONS

- **Declaration of Conformity:** Under the Proposed Rule, VCS hardware importers and connected vehicle manufacturers that import VCS hardware or import or sell completed connected vehicles that contain covered software would be required to submit declarations (*i.e.*, Declarations of Conformity) providing detailed information and certifying compliance with the Proposed Rule, even though connected vehicles containing VCS hardware and covered software are not prohibited from importation into or sale in the United States. VCS hardware importers and connected vehicle manufacturers would need to submit a Declaration of Conformity “once per model year for units associated with a vehicle model year, or calendar year for units not associated with a vehicle model year, and only for the categories of transactions they seek to execute during that period.”^{xix} If preferred, VCS hardware importers and connected vehicle manufacturers could consolidate multiple required Declarations of Conformity.^{xx}
- **Recordkeeping:** The Proposed Rule, based on IEEPA, requires that VCS hardware importers and connected vehicle manufacturers maintain records related to any transaction for which a Declaration of Conformity, General Authorization, or Specific Authorization would be required for ten years.^{xxi} BIS states that such required records will include “all information pertinent to a general authorization or submitted when applying for a Specific Authorization, as well as business records related to the execution of the transaction, such as contracts, import records, bills of sale, [and] relevant correspondence[.]”^{xxii}

AUTHORIZATIONS

- **General Authorizations:** The Proposed Rule will include General Authorizations, which will authorize certain transactions in the following limited circumstances:
 - The connected vehicle manufacturer or VCS hardware importer and entities under common control, including parents, engaging in an otherwise prohibited transaction produce less than 1,000 units of a total MY production of either: (1) completed connected vehicles containing covered software; or (2) VCS hardware; or
 - The completed connected vehicle that incorporates covered software or VCS hardware meets one of the following conditions:
 - It is used on public roadways on fewer than 30 calendar days in any calendar year;
 - It is used solely for the purpose of display, testing, or research, and will not be used on public roadways; or
 - It is imported solely for purposes of repair, alteration, or competition off public roads and will be reexported within one year from the time of import.^{xxiii}
- **Specific Authorizations:** When a transaction is prohibited and would not qualify for a General Authorization, companies may consider seeking Specific Authorization from BIS. The agency will review applications for Specific Authorizations on a case-by-case basis and, if granted, “determine conditions to be applied to each specific authorization as may be needed to mitigate any risk that arises as a result of the otherwise prohibited transaction.”^{xxiv} BIS endeavors to provide, at minimum, a status update of a Specific Authorization application after 90 days.^{xxv} When considering an application for Specific Authorization, BIS will evaluate risks and potential mitigation measures proposed by the applicant for the particular transaction, including, but not limited to:



- Risks of data exfiltration from, and remote manipulation or operation of, the connected vehicle;
- The extent and nature of a foreign adversary involvement in the design, development, manufacture, or supply of the VCS hardware or covered software;
- The applicant's ability to limit Chinese or Russian government access to, or influence over the design, development, manufacture or supply of the VCS hardware or covered software;
- Security standards used by the applicant and if such standards can be validated by BIS or a third-party; and
- Other actions and proposals the applicant intends to take to mitigate undue or unacceptable risk.^{xxvi}

PENALTIES FOR NONCOMPLIANCE

- BIS signals throughout the Proposed Rule that it intends to enforce vigorously the ICTS prohibitions once implemented. The Proposed Rule discusses a requirement to furnish reports on demand under oath, which indicates that BIS can and will issue subpoenas or requests for information should it have concerns about noncompliance. The Proposed Rule also outlines pre-penalty notice, settlement, and penalty processes, which are similar to processes implemented by BIS Office of Export Enforcement ("OEE") and the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"). Pursuant to IEEPA, for violations of ICTS regulations, BIS may impose a maximum civil penalty of \$368,136 per violation, and the maximum criminal penalty is \$1,000,000 per violation or 20 years imprisonment for willful violations.^{xxvii} BIS will annually adjust the specific maximum civil penalty by notice in the Federal Register under the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015.
- We expect BIS to issue guidance about the general factors that will be considered when evaluating potential ICTS violations and appropriate enforcement responses. We also expect the general factors to be similar to the those that BIS OEE and OFAC consider under their regulations, including willful or reckless violation of law, awareness of conduct at issue, harm to regulatory objectives, individual characteristics of the company, compliance programs, and remedial responses.

KEY COMPLIANCE ISSUES AND CONSIDERATIONS

- **Due Diligence:** Although BIS does not provide specific due diligence requirements in the Proposed Rule, the proposed Declaration of Conformity requirement is likely to impose an obligation to conduct a significant degree of supply chain due diligence and tracing to certify that VCS hardware importers and connected vehicle manufacturers have not knowingly engaged in prohibited transactions. In response to comments requesting that BIS establish a trusted trader program to assist companies with diligence, BIS stated that it did not plan to do so "because of the complexity, scale, and opacity of existing connected vehicle supply chains, but may consider establishing such a program to facilitate compliance as supply chains evolve and welcomes comment on such a program as well as any other alternate compliance mechanisms."^{xxviii} BIS states that "VCS hardware importers and connected vehicle manufacturers are given flexibility to provide evidence of compliance efforts tailored to their unique operations," and suggests that due diligence efforts could include using third-party researchers or independently conducting supply chain diligence.^{xxix}

As discussed, the Proposed Rule's knowledge standard includes positive knowledge and willful blindness or avoidance of facts. Consequently, companies required to comply with the Proposed Rule likely need to conduct



a level of due diligence that goes well beyond merely screening parties and also includes issuing questionnaires, obtaining certifications, gathering and reviewing bills of material and related documentation, examining the ownership and controlling features of parties in the supply chain, and conducting open-source research and examination of parties in the different supply chain tiers. In addition, companies should reconsider representations, warranties, and requirements in agreements with direct suppliers. Companies should consider establishing information-sharing requirements and obligations for suppliers to cooperate with OICTS and other U.S. government agencies to allow the preparation and submission of declarations of conformity.

Notably, BIS indicates in the Proposed Rule that it understands such diligence may be difficult, but that it expects companies to undertake the required diligence. Specifically, in response to comments from original equipment manufacturers that “they do not always know the source of all inputs from hardware and software suppliers, making conducting due diligence beyond tier one and tier two suppliers particularly difficult,” BIS emphasized that this lack of transparency “demonstrates the need for regulation to protect U.S. national security,” and that “[s]uch regulation will also incentivize greater supply chain transparency for not only existing supply chains but also for developing supply chains.”^{xxx}

- **Preparing and Updating Declarations of Conformity:** The required Declarations of Conformity will impose substantial obligations and require significant attention. In addition to certifying that the declarant has not knowingly engaged in a prohibited transaction, declarants must include the following information, as well as other information that is specific to VCS hardware and covered software.
 - Declarations of Conformity must be submitted annually and: (1) 60 days prior to the first sale or first import of a Vehicle Identification Number (“VIN”) series of completed connected vehicles comprised of a single MY; or (2) 60 days prior to the import of VCS hardware covered by the declaration. As a result, companies required to submit Declarations of Conformity will need to include sufficient time for the preparation of the declaration early in their processes before importing or selling VCS hardware or connected vehicles incorporating covered software.
 - BIS states that Declarations of Conformity will require Hardware Bills of Materials^{xxxi} (“HBOMs”) for VCS hardware and Software Bills of Materials^{xxxi} (“SBOMs”) for covered software. Therefore, companies required to submit declarations will need to obtain these documents from their suppliers and potentially work with their suppliers to: (1) ensure their accuracy; and (2) create form/template HBOMs and SBOMs that are satisfactory to BIS.
 - VCS hardware importers and connected vehicle manufacturers will need to provide documentation of the steps they took to verify that transactions comply with the provisions of the Proposed Rule.^{xxxi}
 - In the event of any material changes to Declarations of Conformity, or HBOMs or SBOMs submitted as part of declarations, the Proposed Rule requires declarants to update declarations within 30 days of the change. BIS states changes in the suppliers of key subcomponents or functional aspects of the VCS hardware or covered software incorporated in the completed connected vehicle would constitute material changes.^{xxxi} Therefore, companies required to submit Declarations of Conformity will need to conduct ongoing reviews of their declarations and the information contained therein to: (1) confirm the information remains accurate or identify where there have been changes; and (2) determine whether a given change rises to the level of a material change that requires updating a declaration.



Significantly, the Proposed Rule states that updates to the Declaration of Conformity must be made within 30 days of the change, not within 30 days of the declarants becoming aware of the change.^{xxxv} As a result, this raises the risk that changes made by suppliers without immediate notification could result in a failure to update the Declaration of Conformity within the required timeframe. To address this risk, companies may want to include contractual requirements to provide immediate notifications of any changes to information included in declarations and require indemnification for any liability resulting from a failure to provide such notifications.

- As noted above, all VCS hardware importers and connected vehicle manufacturers that import VCS hardware or import or sell completed connected vehicles that contain covered software would be required to submit a Declaration of Conformity. However, BIS is seeking comments on the “necessity and efficacy” of such a broad requirement, including whether to require Declarations of Conformity with respect to VCS hardware and covered software only in which there is a foreign adversary interest (*i.e.*, China or Russia) or to require an otherwise narrower set of VCS hardware importers and completed connected vehicle manufacturers to submit declarations.^{xxxvi}
- **BIS Use of Declarations of Conformity:** As noted above, the submission of the Declarations of Conformity will require VCS hardware importers and connected vehicle manufacturers to conduct substantial diligence and submit that diligence with the declarations. Importantly, in the Proposed Rule, BIS states the purpose of the Declarations of Conformity is to “ensur[e] that parties subject to this proposed rule implement the due diligence and other procedures necessary to fully understand the supply chains for their VCS hardware and covered software and thus comply” with the Proposed Rule.^{xxxvii} In addition, BIS will use the declarations to “facilitate enforcement of the proposed rule, including by allowing BIS to proactively identify red flags and potential violations of the proposed prohibitions” and “maintain an understanding of technological advancements and changes in the U.S. connected vehicle industry.”^{xxxviii} Therefore, to avoid raising scrutiny from BIS, companies required to submit Declarations of Conformity will need to ensure that their declarations are detailed, well prepared, and include the appropriate levels of diligence.

Furthermore, companies should consider the information about them that could be included in other parties’ declarations and the potential for declarations to bring attention to them. Notably, the Proposed Rule does not include discussion of a voluntary self-disclosure (“VSD”) process. Although unclear from the Proposed Rule, BIS may intend, at least initially, to exclusively rely on declarations to probe for potential violations and therefore may not view a VSD process to be necessary or of value because declarations will be required. BIS may use its subpoena powers to obtain additional information about suspected violations based on declarations.

- **Definition of Persons Owned by, Controlled by, or Subject to the Jurisdiction or Direction of a Foreign Adversary:** The expansive definition of persons owned by, controlled by, or subject to the jurisdiction or direction of China or Russia will result in the need to reexamine due diligence processes relating to information and details collected and reviewed for parties in the various tiers of the supply chain. The Proposed Rule includes several examples (including the following) of “ownership, control, and subject to the jurisdiction or direction of” China or Russia, demonstrating the breadth of the Proposed Rule. Coupled with the Declaration of Conformity requirement, diligence could require companies to undertake significant reform of their due diligence programs because diligence will require not only understanding supplier ownership, but also understanding how suppliers are controlled and the rights of specific owners.



Company A, a company that is organized under the laws of [China] or Russia, owns a minority interest in Company B, a U.S. business. Based on special voting powers vested in that minority interest, Company A maintains certain veto rights that determine important matters affecting Company B, including the right to veto the dismissal of senior executives of Company B. Company B would be considered “controlled by” and “subject to the direction of” Company A, and therefore owned by, controlled by, or subject to the jurisdiction or direction of [China] or Russia.^{xxxix}

Company A has eight members on its board of directors. Company A is characterized by a shareholder and corporate governance structure that requires a 75 percent supermajority for any significant business decision. Three of the members of the board are citizens of, and therefore subject to the jurisdiction of, [China] or Russia. Because these three members make up 37.5 percent of the voting power of the board, they can block any supermajority and therefore determine, direct, or decide important matters affecting Company A. Company A would be “controlled by” or “subject to the direction of” [China] or Russia.^{xi}

Company A is privately held and incorporated in the United States. One member of Company A’s board of directors, Person X, a former chairman of the board of a large [Chinese] corporation, has known ties to the government of [China], owns a large minority share of Company A, and has previously made significant investments in other companies founded by Company A’s chief executive officer. Person X also facilitated a large minority investment in Company A by the large [Chinese] corporation where they were previously chairman of the board. Person X’s professional background indicates that they are directly or indirectly supervised, directed, controlled, financed, or subsidized by the [Chinese] government. The combination of Person X’s close ties to Company A’s CEO, Person’s X’s ownership interest and ability to direct investment from large, highly regulated [Chinese] corporate entities, and Person X’s close ties to [Chinese] government indicate that Company A would be “subject to the direction” of [China].^{xli}

As demonstrated in relevant definitions and examples included in the Proposed Rule, “VCS hardware and covered software would not be considered designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of [China] or Russia, solely based on the country of citizenship of natural persons who are employed, contracted, or otherwise similarly engaged to participate in the design, development, manufacture, or supply of that VCS hardware or covered software.”^{xlii}

- **Recordkeeping:** As described above, companies are required to maintain detailed records for transactions subject to the Proposed Rule for at least ten years. Importantly, “[a]ll connected vehicle manufacturers and VCS hardware importers would be required to submit records when requested by BIS related to any transaction for which a Declaration of Conformity, general authorization, or specific authorization would be required by this rule, whether or not that transaction was carried out under a general authorization, specific authorization, or without an authorization from BIS.”^{xliii} Therefore, affected companies will need to ensure that such records are maintained and readily available to provide to BIS if requested and may need to reconsider current recordkeeping and destruction policies and practices.



- **Advisory Opinions:** Under the Proposed Rule, BIS will issue Advisory Opinions (“AOs”) about how to comply with the Proposed Rule. BIS, however, emphasizes that it “will only consider [AO] requests for actual, not hypothetical, prospective transactions in which all parties, as opposed to anonymous parties, are identified.”^{xliv} In addition, there is no timeline on which BIS must complete its review of a request for an AO. Therefore, companies planning to submit AOs will need to build time into their planning to gather the information required for an AO, prepare and submit the AO, and engage with BIS on the request.
- **Monitoring General Authorization Use:** In the Proposed Rule, BIS states that companies using a General Authorization “would be required to continuously monitor for any changes that render a transaction ineligible for continued reliance on the general authorization.”^{xlv} Accordingly, companies relying on a General Authorization will need to incorporate into their compliance program reviews and alerts to note when the General Authorization is no longer applicable or if new transactions are not consistent with the General Authorization.
- **Complying with Specific Authorization Conditions:** As described above, following receipt of an application for a Specific Authorization, BIS “will respond to applicants with a processing update within 90 days of the initial application for a specific authorization, and typically endeavor to provide either a request for more information or a decision within that time period.”^{xlvi} BIS is not required to provide a Specific Authorization or a decision on the application within a given time period. As such, companies will want to determine whether a Specific Authorization is needed and prepare any necessary application early in its processes, build in sufficient time to obtain a Specific Authorization, and plan for contingencies if BIS does not grant the Specific Authorization request.

In addition, companies that receive a Specific Authorization will be required to comply with any conditions or requirements that are included in the Specific Authorization. BIS includes technical controls (e.g., software validation), operational controls (e.g., physical and logical access monitoring procedures), and a requirement that all VCS hardware and covered software be assembled and integrated into the connected vehicle in the United States as examples of conditions that could be imposed. Moreover, as a condition for the issuance of a Specific Authorization, BIS may require an applicant to file certain reports. Therefore, companies that obtain Specific Authorizations will need to implement processes to oversee and monitor transactions subject to Specific Authorizations to ensure the transactions comply with all required conditions and that required reports are timely submitted.

CONCLUSION

The ICTS Proposed Rule will impose substantial new compliance obligations and likely require significant updates and changes to affected companies’ compliance programs, including extensive due diligence processes. U.S. companies that meet the definition of “VCS hardware importer” and “connected vehicle manufacturer” will be affected by the rule. Other U.S. companies directly or indirectly involved in the automotive supply chain, such as components manufacturers or suppliers and software developers, also will be affected, particularly with respect to participating in supply chain tracing exercises. Moreover, non-U.S. companies should carefully consider the Proposed Rule and the potential impacts on them given that the ICTS framework is based on IEEPA, which prohibits “causing” violations.^{xlvii} We expect to see additional activity from BIS as OICTS continues to develop the ICTS framework and its enforcement mechanisms, using this Proposed Rule as a potential template for future regulations and looking to sister agencies, such as OFAC—which also implements regulations based on IEEPA—for ideas about enforcement approaches.



King & Spalding has a global footprint, substantial automotive industry experience, and a deep bench of former trade and national security government officials that are uniquely positioned to advocate on behalf of clients before BIS, help guide companies in complying with the Proposed Rule, and designing and implementing compliance policies and procedures, including due diligence processes, consistent with the Proposed Rule.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,300 lawyers in 24 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered “Attorney Advertising.” View our [Privacy Notice](#).

ABU DHABI	CHARLOTTE	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY
ATLANTA	CHICAGO	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE
AUSTIN	DALLAS	GENEVA	MIAMI	RIYADH	TOKYO
BRUSSELS	DENVER	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.

ⁱ See *Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles*, 89 Fed. Reg. 79088 (Sept. 26, 2024).

ⁱⁱ The Proposed Rule defines “VCS hardware importer” as “a U.S. person importing VCS hardware for further manufacturing, integration, resale, or distribution. A connected vehicle manufacturer may be a VCS hardware importer if VCS hardware has already been installed in a connected vehicle when imported by the connected vehicle manufacturer.” *Id.* at 79117.

ⁱⁱⁱ The Proposed Rule defines “connected vehicle manufacturer” as “a U.S. person (1) Manufacturing or assembling completed connected vehicles in the United States; and/or (2) Importing completed connected vehicles for sale in the United States.” *Id.* at 79116.

^{iv} *Executive Order 13873* of May 15, 2019, *Securing the Information and Communications Technology and Services Supply Chain*.

^v See 89 Fed. Reg. 79088 at 79092.

^{vi} See *id.* at 79093.

^{vii} See *id.* at 79117.

^{viii} See *id.* at 79120.

^{ix} See *id.*

^x See *id.* at 79095.

^{xi} See *id.* at 79117.

^{xii} See *id.*

^{xiii} The Proposed Rule defines “foreign interest” as “any interest in property of any nature whatsoever, whether direct or indirect, by a non-U.S. person.” *Id.* at 79116. This definition is similar to the definition of “interest” in sanctions regulations administered by the U.S. Treasury Department’s Office of Foreign Assets Control.

^{xiv} See 89 Fed. Reg. 79088 at 79116.

^{xv} See *id.* at 79116.

^{xvi} See *id.* at 79091.

^{xvii} See *id.* at 79116-79117.

^{xviii} See *id.* at 79116.

^{xix} See *id.* at 79108.

^{xx} “For example, an OEM that manufactures or assembles completed connected vehicles in the United States, imports connected vehicles into the United States, and imports VCS hardware into the United States would be able to submit a single Declaration of Conformity based on vehicle make, model, and trim and VCS hardware that will be imported or manufactured that Model Year.” *Id.* at 79108.

^{xxi} See *id.* at 79121.

^{xxii} See *id.* at 79111.



^{xxxiii} See *id.* at 79119.

^{xxxiv} See *id.*

^{xxxv} See *id.* at 79110.

^{xxxvi} See *id.* at 79119.

^{xxxvii} See *id.* at 79112.

^{xxxviii} See *id.* at 79093.

^{xxxix} See *id.* at 79091.

^{xxx} See *id.* at 79093.

^{xxxii} The Proposed Rule defines “hardware bill of materials” as “a comprehensive list of parts, assemblies, documents, drawings, and components required to create a physical product, including information identifying the manufacturer, related firmware, technical information, and descriptive information.” *Id.* at 79116.

^{xxxiii} The Proposed Rule defines “software bill of materials” as “a formal and dynamic, machine- readable inventory detailing the software supply chain relationships between software components and subcomponents, including software dependencies, hierarchical relationships, and baseline software attributes, including author’s name, timestamp, supplier name, component name, version string, component hash package URL, unique identifier, and dependency relationships to other software components.” *Id.* at 79117.

^{xxxiiii} See *id.* at 79107.

^{xxxv} See *id.* at 79109.

^{xxxvi} See *id.*

^{xxxvii} See *id.* at 79103.

^{xxxviii} See *id.* at 79108.

^{xxxix} See *id.*

^{xl} See *id.* at 79106.

^{xli} See *id.*

^{xlii} See *id.*

^{xliii} See *id.*

^{xliiii} See *id.* at 79112.

^{xliv} See *id.* at 79111.

^{xlv} See *id.* at 79109.

^{xlvi} See *id.* at 79110.

^{xlvii} Section 1705(a) of IEEPA states, “It shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under this chapter.” 50 U.S. Code § 1705.