This document is scheduled to be published in the
Federal Register on 09/26/2024 and available online at
https://federalregister.gov/d/2024-21903, and on https://govinfo.gov

BILLING CODE: 3510-33

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

15 CFR Part 791

[Docket No. 240919-0245]

RIN 0694-AJ56

Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles

AGENCY: Bureau of Industry and Security, Department of Commerce.

ACTION: Notice of proposed rulemaking.

SUMMARY: In this notice of proposed rulemaking (NPRM), the Department of Commerce's (Department) Bureau of Industry and Security (BIS) proposes a rule to address undue or unacceptable risks to national security and U.S. persons posed by classes of transactions involving information and communications technology and services (ICTS) that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of certain foreign adversaries, and which are integral to connected vehicles, as defined herein. BIS is soliciting comment on this proposed rule, which builds on the advance notice of proposed rulemaking (ANPRM) issued by BIS on March 1, 2024.

DATES: Comments to this proposed rule must be received on or before [INSERT DATE 30 DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: All comments must be submitted by one of the following methods:

• *By the Federal eRulemaking Portal: http://www.regulations.gov* at docket number BIS-2024-0005.

• *By email directly to: connectedvehicles@bis.doc.gov.* Include "RIN 0694-AJ56" in the subject line.

• *Instructions:* Comments sent by any other method, to any other address or individual, or received after the end of the comment period, may not be considered. For those seeking to submit confidential business information (CBI), please clearly mark such submissions as CBI and submit by email, as instructed above. Each CBI submission must also contain a summary of the CBI, clearly marked as public, in sufficient detail to permit a reasonable understanding of the substance of the information for public consumption. Such summary information will be posted on *regulations.gov.* Comments that contain profanity, vulgarity, threats, or other inappropriate language or content will not be considered.

• The Regulatory Impact Analysis is available at http://www.regulations.gov at docket number BIS-2024-0005.

FOR FURTHER INFORMATION CONTACT: Marc Coldiron, U.S. Department of Commerce, telephone: (202) 482-3678. For media inquiries: Jessica Stallone, Office of Congressional and Public Affairs, Bureau of Industry and Security, U.S. Department of Commerce: OCPA@bis.doc.gov.

SUPPLEMENTARY INFORMATION

I. Background

In this notice, BIS solicits comment on a proposed rule to prohibit transactions involving Vehicle Connectivity System (VCS) hardware and covered software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the People's Republic of China, including the Hong Kong Special Administrative Region (PRC), or the Russian Federation (Russia). It follows an advance notice of proposed rulemaking (ANPRM), 89 FR 15066 (Mar. 1, 2024), in which BIS sought public comment to inform a rulemaking that would address the undue or unacceptable risks, as identified in Executive Order (E.O.) 13873, "Securing the Information and Communications Technology and Services Supply Chain," 84 FR 22689 (May 17, 2019), posed by a class of transactions that involve information and communications technology and services (ICTS) designed, developed,

manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary and integral to Connected Vehicles.

In E.O. 13873, the President delegated to the Secretary of Commerce (Secretary), to the extent necessary to implement the order, the authority granted under the International Emergency Economic Powers Act (IEEPA) (50 U.S.C. 1701, *et seq.*), "to deal with any unusual and extraordinary" foreign threat to the United States' national security, foreign policy, or economy, if the President declares a national emergency with respect to such threat. 50 U.S.C. 1701(a). In E.O. 13873, the President declared a national emergency with respect to the "unusual and extraordinary" foreign threat posed to the ICTS supply chain and has, in accordance with the National Emergencies Act (NEA), extended the declaration of this national emergency in each year since E.O. 13873's publication. *See Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain,* 85 FR 29321 (May 14, 2020); *Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain,* 86 FR 26339 (May 13, 2021); *Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain,* 87 FR 29645 (May 13, 2022); *Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain,* 88 FR 30635 (May 11, 2023); *Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain,* 89 FR 40353 (May 9, 2024).

Specifically, the President identified the "unrestricted acquisition or use in the United States of ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries" as "an unusual and extraordinary" foreign threat to the national security, foreign policy, and economy of the United States that "exists both in the case of individual acquisitions or uses of such technology or services, and

when acquisitions or uses of such technologies are considered as a class." *See* E.O. 13873, *and* 50 U.S.C. 1701(a)-(b).

Once the President declares a national emergency, IEEPA empowers the President to, among other acts, investigate, regulate, prevent, or prohibit, any "acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States." 50 U.S.C. 1702(a)(1)(B).

To address the identified risks to national security from ICTS transactions, the President in E.O. 13873 imposed a prohibition on transactions determined by the Secretary, in consultation with relevant agency heads, to involve foreign adversary ICTS and to pose certain risks to U.S. national security, technology, or critical infrastructure. Specifically, to fall within the scope of the prohibition, the Secretary must determine that a transaction: (1) "involves [ICTS] designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary," defined in E.O. 13873 as "any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons;" and (2):

A. "Poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;"

B. "Poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States;" or

C. "Otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons."

These factors are collectively referred to as "undue or unacceptable risks." Further, E.O. 13873 grants the Secretary the authority to design or negotiate mitigation measures that would allow an otherwise prohibited transaction to proceed. E.O. 13873 section 1(b).

The President also delegated to the Secretary the ability to promulgate regulations that, among other things, establish when transactions involving particular technologies may be categorically prohibited. E.O. 13873 section 2(a)-(b); *see also* 3 U.S.C. 301-02. Specifically, the Secretary may issue rules establishing criteria, consistent with section 1 of E.O. 13873, by which particular technologies or market participants may be categorically included in or categorically excluded from prohibitions established pursuant to E.O. 13873.

II. Introduction

Today's vehicles contain a myriad of connected components that provide greater convenience for consumers and increase road safety for both drivers and pedestrians, such as Wi-Fi, Bluetooth, cellular, and satellite connectivity. However, the incorporation of progressively more complex hardware and software systems that facilitate these features has also increased the attack surfaces through which malign actors may exploit vulnerabilities to gain access to a vehicle. As BIS outlined in its March 1, 2024, ANPRM, certain ICTS integral to Connected Vehicles could present an undue or unacceptable risk to U.S. national security when those systems are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.

In the *Securing the Information and Communications Technology and Services Supply Chain* interim final rule, 86 FR 4909 (January 19, 2021), the Secretary determined that certain foreign governments or foreign non-government persons including the PRC, Republic of Cuba, Islamic Republic of Iran, Democratic People's Republic of Korea, Russia, and Venezuelan politician Nicolás Maduro constitute foreign adversaries for purposes of E.O. 13873 and rules promulgated pursuant to E.O. 13873. *See* 15 CFR 791.4 (to the extent that the list of foreign adversaries identified in 15 CFR 791.4 is updated to add or remove governments or non-government

persons, this proposed rule intends to reflect the most up-to-date designations of foreign adversaries). Additionally, E.O. 13873 provides that the Secretary may issue rules that identify particular technologies or countries with respect to which transactions involving ICTS warrant particular scrutiny. E.O. 13873 2(b). For the purposes of this proposed rule regarding transactions involving ICTS integral to Connected Vehicles, BIS is focusing its regulatory efforts on ICTS that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. BIS has identified that, for the purposes of addressing the national security risks posed by Connected Vehicles, these two foreign adversaries pose particular risks to U.S. national security because of their legal, political, and regulatory regimes, combined with their current and anticipated growth and involvement in the automotive sector, to include Connected Vehicles. However, BIS specifically seeks public comment on whether the other identified foreign adversaries pose similar risks to U.S. national security in the connected vehicle supply chain.

The PRC and Russia are able to leverage domestic legislation and regulatory regimes to compel companies subject to their jurisdiction, including carmakers and their suppliers, to cooperate with security and intelligence services. Such control over companies and their products and services means that equipment is easily exploitable by PRC and Russian authorities. The privileged access that the PRC and Russia may gain to Connected Vehicles through their components, including software, could enable those foreign adversaries to exfiltrate sensitive data collected by connected vehicles and, potentially, allow remote access and manipulation of connected vehicles driven by U.S. persons. Pursuant to E.O. 13873, BIS has determined that certain classes of transactions that facilitate the exfiltration of data and remote manipulation of connected vehicles pose undue or unacceptable risks to U.S. national security and the safety and security of U.S. persons.

a. Overview of Proposed Rule

To address these identified undue or unacceptable risks, BIS is proposing regulations that would, absent a General or Specific Authorization, (1) prohibit VCS Hardware Importers from knowingly importing into the United States certain hardware for VCS ("VCS Hardware," as further defined below); (2) prohibit connected vehicle manufacturers from knowingly importing into the United States completed connected vehicles incorporating certain software that supports the function of VCS or ADS (VCS and ADS software are collectively referred to herein as "covered software," as further defined below); (3) prohibit connected vehicle Manufacturers from knowingly Selling within the United States completed connected vehicles that incorporate covered software; and (4) prohibit connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia from knowingly selling in the United States completed connected vehicles that incorporate VCS hardware or covered software. The prohibitions would apply when such VCS hardware or covered software is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

If, following consideration of comments received on this proposed rule, BIS issues a final rule to adopt the proposal, that final rule would take effect 60 days after publication in the Federal Register. However, VCS Hardware Importers would be permitted to engage in otherwise Prohibited Transactions involving VCS Hardware and exempt from certain requirements so long as: (1) for VCS Hardware not associated with a Model Year, the import of the VCS Hardware takes place prior to January 1, 2029; or (2) the VCS Hardware unit is associated with a vehicle Model Year prior to 2030 or the VCS Hardware is integrated into a connected vehicle (completed or incomplete) with a Model Year prior to 2030. connected vehicle manufacturers would be permitted to engage in otherwise prohibited transactions involving covered software and exempt from certain requirements, so long as the completed connected vehiclethat is imported, or sold within the United States, is of a model year prior to 2027. connected vehicle Manufacturers that are owned by, controlled by, or subject to the jurisdiction or direction of the

PRC or Russia would be permitted to sell completed connected vehicles with a model year prior to 2027 that incorporate VCS hardware or covered software.

BIS is also proposing to implement several mechanisms to facilitate compliance with these prohibitions: (1) Declarations of Conformity submitted to BIS by VCS hardware importers and connected vehicle manufacturers to confirm that they are not engaging in prohibited transactions involving VCS hardware or covered software, as defined herein; (2) Advisory opinions to allow VCS hardware importers and connected vehicle manufacturers to seek guidance from BIS on whether a prospective transaction may be prohibited; (3) General authorizations to allow certain VCS hardware importers and connected vehicle manufacturers to engage in otherwise prohibited transactions without the need to notify BIS prior to the prohibited activity if they qualify under stated conditions; (4) Specific authorizations which, following an application to and approval by BIS, grant VCS hardware importers and connected vehicle manufacturers the ability to engage in otherwise prohibited transactions, including because the associated undue or unacceptable risks have been, or can be, mitigated; and (5) A process to inform VCS hardware importers and connected vehicle manufacturers that a specific authorization may be required because an activity could constitute a Prohibited Transaction.

This proposed rule benefits from the responses received during the public comment period for the ANPRM and incorporates significant portions of that feedback. For example, BIS considered public feedback to define the scope of connected vehicles, identify ICTS integral to Connected Vehicles, and better understand the effects of any potential prohibition. Determining the scope of the prohibitions outlined in this proposed rule required balancing the need to address the undue or unacceptable risk posed by foreign adversary involvement in the connected vehicles supply chain with the impact on the public and industry.

III. Comments on the Advance Notice of Proposed Rulemaking

On March 1, 2024, the Department published in the Federal Register an ANPRM, 89 FR 15066, pursuant to the authority the President delegated to the Secretary in E.O. 13873. The

purpose of the ANPRM was to solicit stakeholder feedback and to gather information to further BIS's consideration of a proposed rule to address any undue or unacceptable risks to U.S. national security posed by ICTS used in connected vehicles, when designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. Specifically, BIS sought public input on certain definitions, capabilities of connected vehicles that may increase the likelihood of vulnerabilities, and consequences to U.S. persons and critical infrastructure if these vulnerabilities are exploited by a foreign adversary. BIS also solicited input on the ICTS most integral to connected vehicles and most vulnerable to compromise, as well as input on mechanisms to address identified risks through potential design, implementation standards and protocols, manufacturing integrity protection systems and procedures, or prohibitions.

BIS received 57 comment submissions in response to the ANPRM, from original equipment manufacturers (OEMs), component suppliers, two foreign governments, nonprofit organizations, and individuals. Five comments contained CBI, and one comment was retracted at the request of the commenter. Each of the comments is available on the public rulemaking docket at https://www.regulations.gov.

In general, commenters expressed agreement with BIS on the overall risks posed by compromised ICTS in Connected Vehicles, as outlined in the ANPRM. Commenters were also generally aligned on the need for further clarity on what would constitute a person "owned by, controlled by, or subject to the jurisdiction or direction" of a foreign adversary, the challenge of implementing due diligence requirements due to the complexity of the global automotive supply chain, the need for substantial lead time to implement a regulation given the difficulty of sourcing alternative suppliers, the breadth and depth of data collected by ICTS integral to Connected Vehicles, and the potential negative impact such a regulation could have on long-term U.S. innovation, competitiveness, and health and safety. On the other hand, commenters disagreed on a number of issues, including the ICTS most integral to connected vehicles, the

level of risk that may be posed by transactions involving the identified connected vehicle systems, the definition of connected vehicle, and approaches for how the proposed rule could be most effective in risk mitigation.

Below, BIS addresses in more detail the key issues raised by the comments received and describes how they were considered and, where applicable, addressed in the proposed rule.

a. Definitions

In the ANPRM, BIS sought comments on the definition of the term "connected vehicle," proposing to define it as "an automotive 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." Commenters offered differing views on BIS's proposed definition with some, but not all, commenters agreeing that it appropriately captured the platform BIS seeks to regulate.

Commenters that disagreed with BIS's proposed definition offered several reasons. For example, many commenters viewed the term as overly broad and noted that it failed to identify the specific types of vehicles that would be captured by a regulation (e.g., commercial, industrial, agricultural, rolling stock). Commenters also noted that the phrase "connected vehicle" is an existing term of art within the automotive industry referring to vehicles with external communication capabilities, particularly in short-range communication. As an alternative, some commenters suggested that BIS adopt the term "networked vehicle" to capture the ability of a vehicle to communicate with networks or devices external to a vehicle while others suggested the term "software-defined vehicles" which would encompass the technologies and capabilities outlined in the ANPRM's proposed connected vehicle definition while also capturing internal software capabilities for functions within a vehicle beyond communication (e.g., starting a vehicle, malfunction checks, navigation).

After full consideration of each of the comments, BIS maintains the use of the term "connected vehicle" in the proposed rule. However, BIS proposes to narrow its definition to mean, "[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. Vehicles operated only on a rail line are not included in this definition." This definition captures the vehicles that would be subject to the rule (e.g., passenger vehicles, motorcycles, buses, small and medium trucks, class 8 commercial trucks, recreational vehicles), while excluding those that pose a less acute risk of data exfiltration, modification, or sabotage by foreign adversaries. BIS further believes that the term connected vehicle, as defined in this proposed rule, will capture future trends in vehicle development, particularly as software comes to play a larger role in vehicle operation. BIS emphasizes its belief that, with very few exceptions, all new vehicles sold in the United States will be captured by this definition. BIS seeks comment on this assessment. In the interest of issuing a rule that is narrow, yet also would address the risks posed by connected vehicles, BIS declines to extend this definition to all "rolling stock" or unmanned aerial vehicles as suggested by some comments, although BIS does not preclude the possibility of addressing these vehicles in future regulation. BIS believes that these sectors, to include vehicles operating on a rail line, are materially different from the connected vehicle sector as defined by this proposed rule, and capturing these vehicles in a regulation primarily targeting wheeled on-road vehicles could lead to unintended consequences and supply chain disruption.

A subset of commenters requested further clarity on what would constitute an entity "subject to the jurisdiction or direction" of a foreign adversary and expressed concerns that foreign subsidiaries of U.S. businesses or foreign nationals working in the United States would potentially be captured by this term. Others suggested that BIS should ensure that the

subsidiaries of companies located in foreign adversary countries are captured by the proposed rule, even when the subsidiaries are located in third countries outside the United States that are not foreign adversaries, but supply entities within the United States.

After full consideration of the comments, BIS has adopted the definition of a "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" to mean, (a) 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; (b) 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; (c) 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 (d) 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. BIS has also provided, below in Section V, numerous non-exhaustive examples to explain how this term will apply in various representative situations.

b. ICTS Supply Chain for Connected Vehicles

In the ANPRM, BIS sought comments on "the ICTS supply chain for Connected Vehicles in the United States," in order to better understand the role played by persons owned by, controlled

by, or subject to the jurisdiction or direction of foreign adversaries within it. Public comments broadly discussed the ICTS incorporated into Connected Vehicles and noted the difficulty that manufacturers and suppliers may face in conducting supply chain due diligence for the purposes of complying with any potential final rule. Submissions explained the complexity of ICTS systems contained within Connected Vehicles and outlined several categories of technologies incorporated into Connected Vehicles, including microcontrollers, applications processors, analog products (e.g., power management integrated circuits and transceiver physical layers), automotive software operating systems (OS), automotive vision, light detection and ranging (LiDAR) systems, radar, and other application software systems. Many commenters who identified as OEMs also noted 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. Moreover, submissions highlighted that suppliers are often capable of updating the firmware on their components independently of an OEM, further complicating efforts to understand which entities have access to software and when such access occurs.

The comments received on this topic highlight the depth and complexity of connected vehicle supply chains, indicating that it is not always clear to OEMs which suppliers have access to connected vehicle software and when they have access to it. As some commenters pointed out, some of these technologies and their associated supply chains are still in development and will grow even more complex as the industry develops. Such existing and growing complexity, coupled with the likelihood of ICTS that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary being incorporated into connected vehicles, demonstrates the need for regulation to protect U.S. national security. Such regulation will also incentivize greater supply chain transparency for not only existing supply chains but also for developing supply chains. To facilitate compliance, the rule would include a delayed implementation timeline so that industry can adjust their existing

supply chains and plans for future supply chains. BIS is not currently proposing specific due diligence requirements. Instead, VCS hardware importers and connected vehicle manufactures are given flexibility to provide evidence of compliance efforts tailored to their unique operations. Such efforts could include using third-party researchers or independently conducting supply chain diligence.

Several commenters raised a variety of potential trade-related concerns relating to this proposed rulemaking and other recent U.S. government actions related to automotive trade involving the PRC. While some commenters explicitly advocated for exclusionary tariffs on the import of all PRC vehicles into the United States, others cautioned BIS to avoid creating unnecessary trade barriers when crafting a proposed rule. One commenter specifically warned that BIS regulation of connected vehicle software could amount to a digital trade barrier and urged BIS to avoid certain policies such as data localization requirements, digital service taxes, or forced code inspection. BIS underscores the U.S. government's commitment to the trusted and secure flow of data across borders. This proposed rule seeks to narrowly address, pursuant to E.O. 13873, the acute national security concerns posed by certain foreign adversary ICTS in connected vehicle supply chains while minimizing any unnecessary disruptions in manufacturing and trade. BIS has drafted this proposed rule irrespective of any other automobile-related trade actions taken by the U.S. government.

c. ICTS Most Integral to Connected Vehicles and Their Capabilities

In its ANPRM, BIS identified six systems (i.e., vehicle operating systems (OS), telematics systems, Advanced Driver-Assistance System (ADAS), Automated Driving Systems (ADS), satellite or cellular telecommunications systems, and battery management systems (BMS)) that it was considering identifying as the ICTS in Connected Vehicles most likely to present undue or unacceptable risks if exploited by foreign adversaries. BIS requested comment on the levels of risk associated with these various ICTS as well as any additional ICTS that commenters might consider integral to Connected Vehicles.

Commenters held differing views on which ICTS are integral to connected vehicles and should be captured by the scope of a rule. For example, whereas some commenters noted that ADAS present a low risk of data exfiltration given that these systems often lack direct external connectivity, others noted that such systems may nevertheless be indirectly connected to external devices and systems (e.g., microcontrollers), thus offering indirect access to the data they collect. As another example, while many commenters identified LiDAR systems as a concern, there was disagreement about the nature of the vulnerability posed by these systems. Some commenters noted that LiDAR systems could be manipulated to cause grave harm (e.g., to ignore pedestrians) given their instrumental role in vehicle guidance. However, BIS's further technical analysis found that LiDAR generally lacks the ability to transmit from the vehicle and does not, as a standalone system, control the vehicle. Importantly, BIS notes that in many cases, ADS exerts control over both LiDAR and the vehicle and thus presents a higher risk. Other commenters pointed to the growing role of mobile applications that allow drivers to access and control core functions of the vehicle remotely (e.g., keyless driving). A number of commenters also highlighted concerns related to aftermarket connected devices. These devices, which often feature some forms of connectivity, are introduced to the vehicle after manufacture and sale and may contain vulnerabilities over which OEMs have little to no oversight.

Several submissions expressed a desire for BIS to tailor any regulation as narrowly as possible, arguing that BIS should focus only on those systems with direct connectivity to the connected vehicle or the ability to transmit from the connected vehicle. Some commenters pointed specifically to devices that connect to a vehicle's controller area network (CAN) bus as posing a specific cybersecurity risk. Others recommended that BIS should critically examine electric vehicle charging infrastructure and associated technologies due to a potential risk of exploitation by foreign adversaries. A few OEM commenters ascribed the highest level of potential risk to "finished" or "vertically integrated" vehicles from suppliers with a foreign adversary nexus that are operating in the United States. One commenter pointed to ICTS

components inside safety-critical systems (e.g., braking systems, steering systems, traction systems, battery-charging and management systems, airbag systems) as posing greater levels of potential risk. On the other hand, some commenters recommended that BIS should aim to address the widest possible aperture of risk by regulating a wide variety of the technologies enumerated in the ANPRM along with additional technology categories (e.g., microcontrollers, analog products).

Following consideration of these comments, BIS is proposing a rule that aims to strike a balance between minimizing supply chain disruptions and the need to address the national security risks posed by Connected Vehicles. BIS proposes to achieve this balance by focusing the rule only on those systems that most directly facilitate the transmission of data both into and from the vehicle, rather than focusing on all systems. Therefore, BIS is proposing to regulate transactions involving two systems of ICTS integral to connected vehicles, VCS and ADS. As further discussed below, in many cases, these systems serve as controllers for subordinate systems within the Connected Vehicle, like those highlighted in the ANPRM, making them a target for exploitation related to data exfiltration or remote vehicle manipulation. After reviewing comments, BIS has determined that aftermarket telematics devices, including fleet tracking devices and systems, that fulfill functions consistent with the definition of VCS hardware are covered by this proposed rule.

Additionally, the proposed rule does not cover ICTS with the function of enabling the transmission, receipt, conversion, or processing of radio frequency communications at a frequency below 450 megahertz. Setting such a threshold enables BIS to capture those ICTS that pose a higher risk due to their connectivity and transmission functions, while lowering compliance burden by excluding from regulation those ICTS with functions that pose a lower risk and offer high utility to consumers (e.g., tire pressure monitoring systems, electronic key fobs).

For similar reasons, BIS ultimately chose to exclude other systems highlighted in the ANPRM – such as OS, ADAS, or BMS – from this proposed rule unless they have VCS components and fall within the proposed rule's definition of VCS hardware. For example, automotive software systems like BMS and automotive OS do not have their own connectivity, and require communication through a VCS, thereby making VCS a more effective focus for rulemaking. BMS traditionally do not have their own external wireless data link and instead rely on VCS for wireless communication through a VCS. Likewise, automotive OS software, which generally resides on an in-vehicle infotainment unit or centralized head unit, are characterized by a wide diversity in architecture, design, and supply chain among OEMs while also generally lacking their own data link, instead relying on communication through a VCS. Given how these systems are typically placed within connected vehicles and the ways in which they achieve connectivity, BIS has chosen to focus on the systems that ultimately facilitate the transmission of data both to and from the vehicle as opposed to these subordinate systems.

Additionally, to reduce unnecessary economic impacts and supply disruption, BIS is proposing to regulate ADS software rather than the hardware components of ADAS and ADS. The hardware that enables ADAS and ADS varies widely between different OEMs. In contrast, the hardware that enables VCS are relatively consistent across different automotive architectures and designs. ADAS and ADS hardware encompasses a wide variety of different sensors, distributed electronic control units (ECUs), centralized computing units, actuators, and signaling units, among others. These sensors and internal vehicle networking hardware rarely have independent connectivity. Most, if not all, scalable cybersecurity vulnerabilities to these systems are achieved by connectivity through VCS systems. A rule that coherently and feasibly addresses these varied supply chains would have disproportionate economic and supply chain impacts relative to the reduction of national security risks. Further, focusing on the ADS software supply chain appropriately mitigates the national security risks that they present while limiting the supply chain and economic impact. While BIS recognizes that the scope of data captured by

connected automotive systems is vast and that multiple systems may pose national security risks, as discussed above, it has decided to focus its current efforts on VCS hardware and covered software. However, BIS does not foreclose the possibility of further addressing other systems, including additional aspects of VCS and ADS, in future regulation. BIS therefore also specifically seeks comment on its determination that VCS and ADS are automotive ICTS integral to Connected Vehicles and pose the greatest and most addressable national security risk, and on its decision to focus this rule on those systems. BIS also specifically seeks comment on whether any risks posed by other connected vehicle ICTS should also be addressed in this rule.

d. Cybersecurity Best Practices

In the ANPRM, the Department requested comments regarding cybersecurity concerns with the connected vehicle supply chain, as well as standards, best practices, and norms that are relied upon and built up by the connected vehicle industry. Commenters largely emphasized that OEMs dedicate significant resources to bolstering the cybersecurity of connected vehicle systems in addition to following or conforming to relevant, established best practices and standards. Some commenters referenced work by vehicle manufacturers to deploy advanced encryption techniques as well as the importance of conducting thorough testing on connected vehicle systems and components, to include penetration testing, fuzz testing, and static code analysis. Others identified specific techniques and best practices, including role-based access controls. Among the best practices and standards most referenced by commenters were the National Highway Traffic Safety Administration's (NHTSA) Cybersecurity Best Practices for the Safety of Modern Vehicles, International Organization for Standardization's (ISO) and SAE International's standard ISO/SAE 21434, Institute of Electrical and Electronics Engineers Standards Association's (IEEE) standard IEEE 1609.2, SAE J3061, and SAE J3161. At the international level, commenters also referenced the United Nations Economic Commission for Europe (UNECE) Regulations 155 (R155) and R156, which address whole-of-vehicle and software update cybersecurity, respectively. One commenter encouraged BIS to pay particular

attention to R155 and R156 given the standards' mandatory coverage in UNECE member states and their ability to provide common best practices to vehicle manufacturers globally.

Many commenters underscored that security is a shared responsibility between OEMs and cloud service providers (CSPs), explaining that while CSPs manage the infrastructure layer, CSP customers are responsible for implementing appropriate configurations and controls in the cloud to protect their data. Commenters also emphasized that practices for automotive cloud security and cloud data access vary between OEMs and according to the specific contractual terms between the OEM and CSP. Some submissions pointed to ISO's and International Electrotechnical Commission's (IEC) standard ISO/IEC 27001 and third-party certifications and attestations, such as the Cloud Security Alliance Cloud Controls Matrix, as models for cloud security best practices and standards. With regard to electric vehicle charging infrastructure, commenters pointed to ISO 15118, National Institute of Standards and Technology's (NIST) Internal Report (IR) 8473, and German technical specification DIN 70121, but they emphasized that specific practices vary according to OEM due to differing battery types and configurations.

BIS acknowledges that cybersecurity standards and best practices, particularly many of those mentioned in submissions, serve a crucial function in promoting the safety and security of vehicles. While BIS generally encourages the use of cyber security standards and best practices, BIS also acknowledges that no standard BIS is aware of or that was identified in comments—either currently in effect or under development—would sufficiently mitigate the undue or unacceptable risks posed by foreign adversary involvement in connected vehicle ICTS supply chains as described in this proposed rule, even if widely adopted by industry. The standards and guidance BIS reviewed are primarily focused on hardening automotive systems from external access. Standards and guidance alone are insufficient to address risks from within the supply chain, as the systems are not, and cannot be hardened against the OEM or tier 1 and 2 suppliers that have or maintain privileged access to them. As a result, BIS is not proposing to adopt cybersecurity standards and best practices as part of the rule but may consider the scope and

nature of their adoption on a case-by-case basis as part of the Specific Authorizations process described in greater detail below.

e. Authorizations and Mitigations

In the ANPRM, BIS sought comment on processes and mechanisms that BIS could implement to authorize an otherwise prohibited transaction with the adoption of mitigation measures. Commenters were generally aligned regarding authorizations and potential mitigation schemes. Several commenters requested that BIS adopt (1) an advisory opinion program for connected vehicles; (2) a trusted trader program to simplify compliance and avoid the complexity and uncertainty associated with a licensing regime; and (3) a program allowing OEMs and suppliers to self-certify compliance with the regulation. BIS has considered each of the comments in full and is proposing an advisory opinion program; procedures for VCS hardware importers and connected vehicle manufacturers to submit Declarations of Conformity, which allow OEMs and suppliers to self-certify their compliance with the regulation; as well as procedures for VCS hardware importers and connected vehicle manufacturers to determine eligibility for a General Authorization or apply for a Specific Authorization. BIS is not proposing a trusted trader program at this time 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.

A significant portion of commenters raised and rejected data localization requirements as a potential solution to the data exfiltration concerns associated with connected vehicles. Instead, many argued that data exfiltration concerns could instead be mitigated by securing a demonstrated commitment to privacy and security from OEMs and suppliers, primarily through the adoption of industry cybersecurity best practices and standards. Some commenters also pointed to company membership in the Automotive Information Sharing and Analysis Center (Auto-ISAC) as another method for entities to demonstrate commitment to cybersecurity best

practices. As discussed above, BIS has opted not to require adherence to any specific standard or best practice as a prerequisite to securing an authorization to engage in an otherwise prohibited transaction, but BIS reserves the right to consider compliance with them on a case-by-case basis in conjunction with other potential mitigations.

f. Economic Impacts

Comments generally agreed that prohibitions affecting a major supplier of a component used in Connected Vehicles could result in negative economic outcomes. Commenters raised several concerns, including increased manufacturing costs for U.S. auto manufacturers that would likely be passed onto consumers; a decline in long-term U.S. competitiveness vis-à-vis foreign auto manufacturers; disincentivizing further investment in connected vehicles and autonomous vehicle research and development (R&D), potentially reducing future employment in the U.S. auto industry; and a decline in the safety and quality of connected vehicles available to U.S. consumers. Several commenters also noted that regulation may have an outsized impact on small businesses, which often lack the due diligence and compliance resources of their larger competitors. To mitigate these outcomes, several commenters requested substantial lead time for manufacturers to identify and source from alternative suppliers. Lastly, multiple submissions emphasized that not all components in connected vehicles produced by entities owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary necessarily pose a cybersecurity or national security risk, especially for components with minimal or no connectivity capability.

Following consideration of these comments, BIS proposes to allow 1) until Model Year 2027, for connected vehicle manufacturers to come into compliance for transactions involving covered software, 2) until model year 2030, or January 1, 2029, for VCS hardware importers to come into compliance for transactions involving VCS hardware; and 3) until model year 2027 for connected vehicle manufacturers that are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia to sell connected vehicles with VCS hardware

and/or covered software. Moreover, to address concerns about the resources small businesses are able to devote to compliance, BIS is proposing a general authorization that would permit certain small businesses to engage in otherwise prohibited transactions. BIS also emphasizes that this rule would narrowly target the specific automotive systems that pose the greatest risk when designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of certain foreign adversaries. As such, the rule would not broadly prohibit the import of connected vehicle technologies from foreign adversary nations, nor would it require market participants to alter supply chains for low-risk or unconnected components.

BIS believes that the implementation timeline strikes an appropriate balance between minimizing significant disruptions to the connected vehicles supply chain and mitigating the national security risk posed by foreign adversary involvement in the connected vehicles supply chain. Given the relatively limited amount of foreign adversary linked hardware and software in U.S. vehicles today, the software prohibitions proposed in this rule would address the most immediate threats to U.S. national security while allowing industry time to come into compliance with the prohibitions on VCS Hardware.

IV. Risks Associated with Vehicle Connectivity Systems and Automated Driving Systems When Designed, Developed, Manufactured, or Supplied by Persons Owned by, Controlled by, or Subject to the Jurisdiction or Direction of the PRC and Russia.

Following consideration of comments received on the ANPRM, and further consideration of the risks and vulnerabilities associated with various ICTS components that are critical to the operation of CVs, BIS proposes to focus its rule on two integral ICTS systems—VCS and ADS—when designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of two foreign adversary entities—the PRC and Russia. Below, BIS further explains its understanding of the undue and unacceptable risks associated with these particular systems, and these particular foreign adversaries, and seeks public comment on the systems and foreign adversaries addressed in the proposed rule.

a. Vulnerabilities Associated with Vehicle Connectivity Systems and Automated Driving Systems

1. Vehicle Connectivity Systems

The term VCS encompasses hardware and software systems—such as the telematics control unit (TCU), cellular modems and antennas, and other automotive components—that integrate various radio frequency communication technologies and enable Connected Vehicles to access external data sources, facilitate vehicle-to-vehicle communication, and provide enhanced services to users through seamless connectivity options. For example, as the primary automotive VCS component, a TCU acts as the primary interface between the internal network and external communication channels. It collects data from onboard sensors such as GPS, accelerometers, gyroscopes, BMS, and other ECUs via wired networks like CAN bus, LIN, FlexRay, Automotive Ethernet, K-Line, as well as wireless protocols such as Bluetooth and Wi-Fi. Some systems use cameras and microphones to facilitate facial recognition of drivers, or to respond to voice commands of drivers. Once gathered, the TCU converts this internal data into radio frequency signals suitable for transmission over the chosen wireless protocol. In other words, as the vast array of sensors on a connected vehicle collect information about a driver's location, speed, voice patterns, battery state of charge, or other vehicle diagnostic and operational information, the TCU converts that data into a format that can be transmitted to systems outside the vehicle and then enables that transmission.

While the increased degree of vehicle connectivity offers benefits to both consumers and manufacturers, it also increases risks to consumers and manufacturers due to the number of access points into the internal vehicle network, each of which may present multiple new software vulnerabilities for adversaries to exploit. *See* National Renewable Energy Laboratory, "Vehicle Cybersecurity Threats and Mitigation Approaches," (Aug. 2019), https://www.nrel.gov/docs/fy19osti/74247.pdf. Such compromise of VCS software could occur at various points of the software development lifecycle, including tool development, source code

repositories, open-source dependencies, software updates, and shipment interdiction. For instance, Upstream's 2024 Global Automotive Cybersecurity Report documented a case where security researchers installed malicious software on the VCS by performing a simulated jailbreak attack of an OEM's VCS using a voltage fault injection on the chip-maker's processor. This malicious software unlocked vehicle manipulating features such as acceleration and heated seats, provided access to private user data such as a user's phonebook and calendar entries, and enabled decryption of encrypted Non-Volatile Memory Express (NVMe) storage, manipulation of the car's identity, and extraction of the vehicle-unique credential used for authenticating and authorizing the OEM's internal service network. *See* Upstream, *2024 Global Automotive Cybersecurity Report* (Feb. 2024), https://upstream.auto/reports/global-automotive-cybersecurity-report/. By compromising software or its dependencies, malign actors may surveil, disrupt, damage, or otherwise exploit the data or systems of those who use the software. *See* National Counterintelligence and Security Center, "Software Supply Chain Attacks," (Mar. 2021), https://www.dni.gov/files/NCSC/documents/supplychain/Software_Supply_Chain_Attacks.pdf.

The threat of such a cyber operation by malicious actors can grow significantly when firmware or hardware components are intentionally designed with vulnerabilities. Access to the hardware supply chain for VCS provides an avenue for threat actors to manipulate or insert, with malicious intent, hardware, or firmware modules into telematics hardware components such as modems, Systems on Chip (SoC), Printed Circuit Boards (PCB), central processing units, and antennae. Manipulating or modifying hardware and associated firmware in the supply chain could also allow foreign adversaries to insert a backdoor, granting them control over the VCS. *See* Cybersecurity and Infrastructure Security Agency, *Defending Against Software Supply Chain Attacks* (April 2021), https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508.pdf, *and* National Counterintelligence and Security Center, "*Software Supply Chain*

Attacks," (Apr. 2023), https://www.dni.gov/files/NCSC/documents/supplychain/Software-Supply-Chain-Attacks.pdf. For instance, cellular and satellite telecommunications transceivers are pivotal connectivity components in the VCS, utilizing radio frequency (RF) energy to facilitate the transmission and reception of data between a vehicle and the external world. If these transceivers are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, such actors would have the means and capability to introduce vulnerabilities that could be exploited to intercept and/or compromise the information exchanged between the connected vehicle and the external world.

2. Automated Driving Systems

The complexity of ADS software, the large foundation of data sources, and the driving responsibilities inherent to ADS render it a valuable target for exploitation. An ADS encompasses the upper end of the spectrum of autonomy levels that dictate the vehicle's independence and the extent of driver intervention required. As defined by the SAE J3016, autonomy levels range from Level 0 (no automation) where the driver controls all aspects of driving, to Level 5 (full automation) where the vehicle can operate independently under all conditions without human intervention. Levels 1 and 2 offer driver assistance through systems that control either steering or acceleration and braking, while Levels 3 through 5 (which generally comprise ADS) progressively increase the system's responsibility for driving tasks, with Level 4 requiring the ability to complete all driving functions within defined operational design domains (ODDs). As the autonomy level increases, the reliability and safety of the ADS become increasingly reliant on the system's operational performance, safety protocols, and cybersecurity measures. *See* Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, SAE International, (Apr. 2021), https://www.sae.org/standards/content/j3016_202104/.

An ADS must be able to execute Dynamic Driving Tasks (DDTs) within specific ODDs. DDTs include critical tasks such as steering, braking, acceleration, and Object and Event Detection, Classification and Response (OEDR). OEDR enables an ADS to perceive and respond to surrounding objects and events, a responsibility that shifts progressively from the driver to the ADS itself as the degree of vehicle autonomy increases. *See* Edward Griffor, David Wollman, and Christopher Greer "Automated Driving System Safety Measures Part 1: Operating Envelope Specification," *NIST Special Publication 1900-301* (2021), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-301.pdf.

An ADS relies on a large foundation of connected information sources for decisions and outputs which in turn could create inherent vulnerabilities. As a result, the complex software systems that drive decisions for an ADS are valuable targets for malicious actors to exploit. Software-based threats to Connected Vehicles equipped with an ADS include manipulation of sensors to create phantom objects; manipulation of ADS software to detect, capture, and retain information about specific geographic areas or other sensitive data; or other manipulation of sensor fusion processing software that could lead to faulty and dangerous vehicle decision making, to include unauthorized control over the Connected Vehicle. *See* National Counterintelligence and Security Center, "Autonomous Automotive Vehicle Supply Chain Risk," (2022), https://www.dni.gov/files/NCSC/documents/supplychain/autonomous-vehicles-placemat-2022-D9A54B50-.pdf.

A compromised ADS creates opportunities for data exfiltration and unauthorized vehicle manipulation due to the direct access it has to the internal vehicle network (IVN). The IVN controls the communication framework within a Connected Vehicle, overseeing the ECUs responsible for engine control, traction control, door locks, climate control, battery management, powertrain, airbags, cameras, and radar functionalities. These ECUs also communicate via overlayed communication networking protocols such as a CAN bus, Local Interconnect Network (LIN), and ethernet. *See* Anastasios Giannaros, et al. "Autonomous Vehicles: Sophisticated

Attacks, Safety Issues, Challenges, Open Topics, Blockchain and Future Directions," *Journal of Cybersecurity and Privacy* 3.3 (2023). Because ADS interacts with ECUs through the IVN, a compromised ADS has the capability to execute functions that affect nearly all of a Connected Vehicle's software and hardware components. For example, an update to an ADS could alter the outputs the ADS makes to a body control unit, enabling the ADS to erroneously and dangerously open a vehicle's door while in motion. Moreover, because many Connected Vehicles maintain their own networks and actively scan their operating environment for other proximate networks, an ADS can also potentially be used to impact the IVN of other vehicles or transportation infrastructure networks through vehicle-to-vehicle communication. *See* National Counterintelligence and Security Center, *Autonomous Automotive Vehicle Supply Chain Risk*, (Apr. 2022), https://www.dni.gov/files/NCSC/documents/supplychain/autonomous-vehicles-placemat-2022-D9A54B50-.pdf, *and* Patrick Wagner, Nikolai Puch, and David Emeis, "Cybersecurity risk analysis of an automated driving system," *Fraunhofer Institute AISEC*, (Oct. 2023), https://publica.fraunhofer.de/entities/publication/4d66e81e-3570-4c49-9f8c-8c9967a34ca6/details.

Given the significant processing power and complex decision-making ability of an ADS, the risks arising from ADS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary extend beyond the IVN itself and can include risks to the fidelity and integrity of data that flows to downstream or adjacent transportation infrastructure. Foreign adversaries can corrupt ADS data by exploiting existing vulnerabilities in ADS connectivity environments (*see* section IV(b) below). As such, direct access to an ADS afforded to a malicious actor through the design, development, manufacture, or supply of ADS software has the potential to cause severe adverse consequences to U.S. national security and U.S. persons.

b. Threats Associated with the PRC and Russia

The design, development, manufacture, or supply of certain VCS and ADS components by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia poses undue or unacceptable risks to national security and U.S. persons. The PRC and Russia have adopted political, legal, and regulatory regimes that enable their governments to exercise direct and indirect ownership, control, or influence over entities in the connected vehicle supply chain. Unlike other foreign adversaries, the PRC and Russia also have certain current and anticipated industrial capabilities and expertise that uniquely position them within the global automotive market to pose an outsized risk, particularly when paired with the vulnerabilities present within certain connected vehicle systems.

1. PRC

The PRC's role in the U.S. connected vehicle supply chain presents undue and unacceptable risks. The PRC has a large and growing automotive sector with strong connections to non-PRC, including U.S., automakers providing it potential increased access to the U.S. automotive market. Further, the PRC's automotive sector has historical and ongoing links to the PRC military and is influenced by pervasive government intervention, including through legal and regulatory structures that increase government oversight of and control over PRC-based companies and their foreign subsidiaries. *See* Du Xiaoying and Wang Siyi, "Dongfeng plays pivotal role in supporting China's military," *China Daily*, (Sept. 25, 2015), https://www.chinadaily.com.cn/cndy/2015-09/25/content_21976945.htm, *and* Matthew Funaiole et al, "China Accelerates Construction of 'Ro-Ro' Vessels, with Potential Military Implications," Center for Strategic and International Studies, (Oct. 2023), https://chinapower.csis.org/analysis/china-construct-ro-ro-vessels-military-implications/. Moreover, the PRC possesses advanced cyber espionage capacities that it exercises through both state and non-state cyber actors exacerbating such risks.

First, the size and scale of state control in the PRC auto sector poses outsized risks, increasing the vectors by which the national security threats associated with Connected Vehicles

can enter the United States. The PRC automotive sector has played an important role in its domestic industrial policy since 1986, when the sector was first named a "pillar industry" in the Seventh Five-Year Plan. The Fourteenth Five-Year Plan, the latest strategic framework for the PRC, continues to prioritize the technology innovation and sustainable development of the automobile market, including new energy vehicles and connected vehicle software and hardware systems. *See* Ben Murphy, "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035," Center for Security and Emerging Technology, (May 2021), https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf. For many years, the state has pursued a number of policies and practices to further its industrial policy objectives in the automotive sector, including mandatory joint venture requirements, foreign equity restrictions, massive subsidies and other financial support measures, and various other preferences and discriminatory policies and practices. The PRC automotive sector's growth was also led in part by several prominent state-owned firms that began as military equipment suppliers (e.g., Chang'an Automobile, Changhe, Hunan Changfeng Motor) or have since risen to become prominent state-owned firms (e.g., GAC Group, Chery Automobile Co.). *See* Mattias Holweg, Jianxi Luo, and Nick Oliver, The past, present and future of China's automotive industry: a value chain perspective, *International Journal of Technological Learning, Innovation and Development* 2 (Feb. 2009), https://www.pure.ed.ac.uk/ws/portalfiles/portal/7765689/Oliver.pdf. In recent years, this growth and development has led to a massive surge in domestic vehicle production, with Chinese vehicle production increasing by 1.5 times over the 15-year span between 2008 and 2023. Indeed, in 2023, the PRC alone was responsible for nearly 33 percent of global passenger vehicle production. *See* VDA, *Global passenger vehicle production in 2023, by country [Graph]*, (Retrieved July 23, 2024), https://www.statista.com/statistics/277055/global-market-share-of-regions-on-auto-production/, *and* OICA & Statista*, China's share in global vehicle production from 2008 to 2021 [Graph],* (Mar. 17, 2022), https://www.statista.com/statistics/233942/chinas-

share-of-global-production-capacity-of-the-automobile-industry/. Amid this significant growth in the PRC's domestic auto industry, Chinese automakers, both state-owned and private firms, have leveraged their significant state-backed support, including subsidies, to fuel a global expansion that has seen Chinese automakers establishing foreign operations in countries like South Africa, the Netherlands, Thailand, Japan, and Brazil, among others, increasing the risks stemming from PRC auto manufacturing in third countries. This expansion, combined with recent investment announcements, has spurred concerns that Chinese automakers may soon seek to further expand into the United States either through exports or the establishment of additional manufacturing facilities. Some PRC-based companies have announced plans to establish manufacturing facilities in Mexico, which could enable them to receive favorable trade terms contained in the U.S.-Mexico-Canada Agreement (USMCA). Such a significant position within the global auto sector greatly expands the number of potential nexus points between PRC connected vehicle suppliers and U.S. automakers and U.S. consumers, including indirectly through auto manufacturers in third countries.

Second, the military linkage between the PRC government and the automotive sector continues to the current day with the PRC's military-civil fusion strategy—which seeks to, among other goals, exploit investment and innovation within the PRC's private sector to achieve military modernization goals—and has prioritized specific information and communication technologies that are integral to connected vehicle supply chains (e.g., telecommunications, artificial intelligence). *See* Ben Murphy, "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035," Center for Security and Emerging Technology (May 2021), https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf. Strategies to achieve these goals include mandating collaboration between PRC-based companies and the military and establishing public and private firms as vectors to facilitate technology transfer, industrial espionage, and intellectual property theft that would be advantageous for the PRC

military. *See* Office of the Dir. of Nat'l Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, (Feb. 6, 2023), https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

Third, even beyond military-civil fusion, the role of the PRC government in the auto sector has only grown as government intervention in the market increases, including through direct ownership of prominent industry participants, the purchasing of so-called "golden shares" to gain significant levels of influence within otherwise private firms, embedding Chinese Communist Party (CCP) representatives within corporate boards and management, and the forceful application, or threat thereof, of the PRC's expanding security laws, including its digital era legal structure. *See* Lingling Wei, "China's New Way to Control Its Biggest Companies: Golden Shares," Wall Street Journal (Mar. 2023), https://www.wsj.com/articles/xi-jinpings-subtle-strategy-to-control-chinas-biggest-companies-ad001a63. Laws promulgated in recent years provide the PRC government increased oversight and control over PRC-based companies and their foreign subsidiaries, providing a lever for influence over corporate operations that further exacerbates the threat that the PRC poses to U.S. national security. These laws require PRC-based companies, wherever located, to comply with certain access and information requests upon demand from the PRC, and therefore could be used by the PRC to obtain business or other data from PRC-based companies involved in the connected vehicle supply chain. Companies operating under these laws frequently highlight the lack of transparency, consistency, clarity, and predictability of the enforcement of these laws, publicly stating that PRC laws relating to cybersecurity, data storage, or cryptography are not subject to the same degree of judicial accountability as they might be in other jurisdictions. In particular, BIS notes the PRC may utilize a suite of national security laws (*e.g.*, *Counter-Espionage Law of the People's Republic of China* [promulgated by the Standing Committee of the National People's Congress, Nov. 1, 2014, amended Apr. 26, 2023, effective July 1, 2023]; *National Security Law of the People's Republic of China* [promulgated by the Standing Committee of the National People's Congress,

July 1, 2015, effective July 1, 2015]; *National Intelligence Law of the People's Republic of China* [promulgated by the Standing Committee of the National People's Congress, June 27, 2017, effective June 28, 2017, amended Apr. 27, 2018]; *Anti-Terrorism Law of the People's Republic of China* [promulgated by the Standing Committee of the National People's Congress, Dec. 27, 2015, effective Jan. 1, 2016, amended Apr. 27, 2018]) to compel companies, including those in the connected vehicle supply chain, to support national security efforts—which are more broadly defined in the PRC than in the United States—or military agents upon request, including in some cases through the creation of backdoors and security vulnerabilities in products sold abroad, and in many cases, the PRC prohibits companies from disclosing that such a request was made. *See* U.S. Department of Homeland Security, "Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China," (Dec.2022), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf. Additionally, PRC authorities have established a regulatory system that effectively allows them to stockpile cyber vulnerabilities. Entities subject to these regulations, including automotive systems manufacturers, are required to report vulnerabilities upon discovery to PRC authorities before patching them. *See* Cyberspace Administration of China, "*Provisions on the Management of Security Vulnerabilities of Network Products,"* (Jul.2021), https://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm. This requirement drastically increases the ability of the PRC government and PRC-backed cyber actors to take action against the United States using connected hardware and its associated software by creating an accessible library of known and potentially unpatched vulnerabilities. And fourth, the PRC has demonstrated a high level of competency in cyber malfeasance. The recent Volt Typhoon action exemplified how PRC cyber actors pre-position themselves across U.S. critical infrastructure and military assets in order to, at a potential future date, launch an attack and impede U.S. decision making, induce social panic, and interfere with the deployment of U.S. military forces. *See*

Cybersecurity and Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," (Feb. 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a. A 2022 Annual Report to Congress by the U.S.-China Economic and Security Review Commission found that the PRC's ability and willingness to "weaponize" its own industries, particularly its cybersecurity industry, grants the country an asymmetric advantage over the United States; an argument that was further supported in reporting earlier this year that detailed the methods by which known government-affiliated cyber threat groups utilize private firms to carry out their attacks. *See* U.S.-China Economic and Security Review Commission, "2022 Annual Report to Congress," (Nov. 2022), https://www.uscc.gov/sites/default/files/2022-11/2022_Annual_Report_to_Congress.pdf; Christian Shepherd et al., "Leaked files from Chinese firms show vast international hacking efforts," The Washington Post (Feb. 22, 2024), https://www.washingtonpost.com/world/2024/02/21/china-hacking-leak-documents-isoon/. Additionally, a 2012 report from United States Senate Permanent Select Committee on Intelligence examining the national security risks posed by the PRC-based companies Huawei and ZTE specifically argued that there are numerous opportunities for PRC-based threat actors to insert malicious hardware or software components into ICTS products throughout the product development stage. *See* Permanent Select Committee on Intelligence, "*Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE"* (Oct. 2012), https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf. This risk has not diminished, as indicated by a study of designed vulnerabilities in products conducted by the Georgetown Security Studies Review, which outlines five years of persistent insertion of malicious code by PRC-based threat actors. *See* Georgetown Security Studies Review, "*Flawed by design electronics with pre-installed malware*" (May2018), https://georgetownsecuritystudiesreview.org/2018/05/23/flawed-

by-design-electronics-with-pre-installed-malware/. Given the above, the PRC's access to the U.S. connected vehicle supply chain through its growing automotive sector, military-civil fusion and other corporate governance policies, and legal institutions paired with its development of mature cyber espionage capabilities have increased the risk that the PRC could alter the systems in, or obtain and manipulate information to or about, market participants who use connected vehicle ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC.

2. Russia

The Russian state has prioritized the growth of its automotive manufacturing industry, instituted a legal and regulatory framework to compel company data sharing with the state, and maintained a long history of malicious cyber operations against the U.S. Under these circumstances, there is an increasing likelihood that Russia emerges as a supplier of connected vehicles technologies for the U.S. market, providing the Russian government a means of exploiting U.S. connected vehicles. Moreover, incorporating Russian hardware or software into the U.S. connected vehicle supply chain poses undue and unacceptable risks to U.S critical infrastructure and U.S. persons.

First, while Russia has historically been less active in the global automotive sector than the PRC, the Russian government has recently sought to revitalize its own domestic auto manufacturing industry following the exodus of foreign automakers after the imposition of significant additional sanctions in 2022. In 2024 alone, the Russian auto market is projected to experience a 15 percent increase in passenger vehicle sales, marking a noted uptick since the market crashed following sanctions and some Russian auto manufacturers have continued introducing new models even amid broader economic headwinds. *See* Reuters, "Russia's 2024 car sales forecast raised to 1.45 mln, units, AEB says," (Jul. 2024), https://www.reuters.com/business/autos-transportation/russias-2024-car-sales-forecast-raised-145-mln-units-aeb-says-2024-07-03. The void left by many foreign firms has made Russia a

valuable export market for Chinese auto manufacturers seeking to expand their presence globally with some Chinese auto brands seizing significant market share from Russian competitors accounting for almost 56 percent of domestic auto sales in August 2023. *See* Gleb Stolayrov and Alexander Marrow, "Exclusive: Chinese car sales boom in Russia levels off amid shaky local recovery," *Reuters* (Nov2023), https://www.reuters.com/business/autos-transportation/chinese-car-sales-boom-russia-levels-off-amid-shaky-local-recovery-2023-11-24/. In Russia, the revitalization of the domestic economy, in particular the domestic auto sector, has become a key focus of the government since the imposition of sanctions in recent years. The Russian government has released several plans pointing to a prioritization of the development of its domestic automotive market with a particular focus on research and development for new technology, including autonomous vehicles and V2X vehicle connectivity systems. *See* Russian Federation, *Order of the Government of the Russian Federation of December 28, 2022 No. 4261-r On Approval of the Strategy for the Development of the Automotive Industry of the Russian Federation until 2035* (Jan. 4, 2023), https://www.garant.ru/products/ipo/prime/doc/405963861/#1000 and *See* Russian Federation, *Order of the Government of the Russian Federation of August 23, 2021 No. 2290-r On Approval of the Concept for the Development of Electric Vehicle Production and the Transport Strategy of 2030*, (2023), http://static.government.ru/media/files/bW9wGZ2rDs3BkeZHf7ZsaxnlbJzQbJJt.pdf. The development of these interlocking national transportation and automotive industry strategies involved stakeholders from domestic automakers, technology sectors, and the Russian government, illustrating a coordinated effort across the Russian state and its domestic automotive industry. In order to extend the reach of the state into the Russian auto industry, in February 2024, Russia established a state-owned corporation named Rosavto that will act as liaison between government and industry and will develop production plans for vehicles and automotive spare parts, oversee the development of new models and technologies, and manage order

distribution, legislative initiatives, and workforce training. *See* Eugene Gerden, "New State Corporation to Oversee Russian Auto Industry," *Wards Auto* (Feb. 2024), https://www.wardsauto.com/regulatory/new-state-corporation-to-oversee-russian-auto-industry. Concerted efforts by the Russian government to grow the domestic Russian automotive industry increase the likelihood that Russian-manufactured VCS hardware or covered software will enter the U.S. connected vehicle supply chain, which, as described below, would present an undue or unacceptable risk to U.S. national security.

Second, like the PRC, the Russian government employs a suite of laws that enable it to compel domestic companies with overseas operations to provide data gleaned through foreign ventures or to surrender similar operational assets to the Russian state. These laws (*e.g.*, Russian Law Federal Security Service No. 40-FZ, "Operational-Investigative Activity" No. 144-FZ, 2014 Amdt. to No. 97-FZ) provide the Russian government direct control over Russian corporations' activities and facilities, including data or customer information, and mandate that companies cooperate with assisting counterintelligence actions as requested by the state, including the Federal Security Service of the Russian Federation (FSB). The FSB can, in some cases, mandate that companies allow the FSB to install equipment on their infrastructure or collect data. Firms that are required to facilitate this surveillance or intrusion activity can also be required to actively obfuscate such requests and must provide the state with any information essential to the decryption of any communications captured. Together, these laws enable the Russian state to collect and exploit sensitive data on or about U.S. persons via Russian businesses and, should Russian companies become more prominent in the connected vehicle supply chain, create a pathway by which the Russian government could secure wide-ranging access to the vast amounts of data collected and processed by Connected Vehicles in the United States. *See* Internet Governance, "Report of Peter B. Maggs," (Dec. 2017), https://www.internetgovernance.org/wp-content/uploads/12-7-Exhibit-AR-Part-6-Maggs-report.pdf. Public reports have consistently raised concerns about Russian government laws concerning data collection, citing a lack of

appropriate safeguards to prevent misuse, to include judicial or public oversight. More broadly, reports have repeatedly documented the uneven application of the rule of law, lack of judicial accountability, recurrent violations of judicial proceedings, and challenges with judicial independence. *See* Justin Sherman, "Russia is weaponizing its data laws against foreign organizations," Brookings, (Sept. 2022), https://www.brookings.edu/articles/russia-is-weaponizing-its-data-laws-against-foreign-organizations/; Evegeni Moyakine and A. Tabachnik, "Struggling to strike the right balance between interests at stake: The 'Yarovaya', 'Fake news' and 'Disrespect' laws as examples of ill-conceived legislation in the age of modern technology," *Computer Law & Security Review 40*, (Apr. 2021), https://www.sciencedirect.com/science/article/pii/S0267364920301175.

Third, apart from the access codified in Russia's legal framework, the country has a longstanding pattern of utilizing cyber operations to gain illicit access to systems that advance the strategic ends of Russian authorities. For example, in December 2020 the company SolarWinds announced it was the target of a two-year-long cyber operation perpetrated by Russian hackers in the Russian Foreign Intelligence Services (SVR). *See* U.S. Securities and Exchange Commission, "SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures," (Oct.2023), https://www.sec.gov/newsroom/press-releases/2023-227. The perpetrators of the SolarWinds supply chain attack used a software update to deliver its malware to the platform's users after Russian intelligence services obtained covert access to the computer systems on which the platform was installed and ultimately impacted more than 18,000 users, including more than 100 companies and nine U.S. Government agencies. This attack credibly demonstrates how Russian actors can infiltrate global enterprise systems via software updates and exemplifies how they could similarly leverage software as a means to exploit connected vehicles in the United States. Additionally, a 2023 Cyber Security Advisory suggests that exploitation of information technology firms and their software will continue to be a persistent tactic leveraged by the Russian government to collect

intelligence. *See* Joint Cyber Security Advisory, **"**Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally" (Dec. 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a. BIS has further identified Kaspersky Lab as an example of how Russia has leveraged software companies to give it the ability to collect and weaponize the personal information of Americans. *See* Bureau of Industry and Security, "*Final Determination: Case No. ICTS-2021-002, Kaspersky Lab, Inc."* (Jun. 2024), https://www.federalregister.gov/documents/2024/06/24/2024-13532/final-determination-case-no-icts-2021-002-kaspersky-lab-inc. These political, legal, and regulatory frameworks, combined with the PRC's and Russia's demonstrated capability to exploit ICTS supply chains through malicious cyber activity, exacerbate BIS's concern that the threats posed by these foreign adversaries could be directed at the U.S. connected vehicle supply chain, including integral systems such as VCS and ADS. The persistent connectivity and software-driven capabilities of VCS and ADS, combined with the vast amounts of data that traverse these systems, make them valuable and likely targets for the PRC and Russian governments to compromise.

c. Consequences

Taken together, VCS and ADS designed, developed, manufactured, or supplied by persons under the ownership, control, jurisdiction, or direction of the PRC or Russia manifest undue and unacceptable risks to United States national security in several ways. If left unaddressed, the interaction of threats and vulnerabilities could result in the exfiltration of sensitive U.S. persons' data to foreign adversaries or the remote or automated manipulation of Connected Vehicles by the PRC and Russia, among other concerns.

First, the integration of compromised VCS or ADS into a completed vehicle could undermine the reliability of a connected vehicle or its underlying control systems. Compromised components in VCS or ADS could result in increased frequency and severity of connected vehicle malfunctions that could in turn detrimentally impact U.S. national security, including the resiliency of U.S. critical infrastructure, or the safety of U.S. persons.

Given the persistent connectivity of VCS and ADS and the essential functions that they service in the operation of Connected Vehicles, these systems, if compromised and co-opted by an adversary, could serve as a node through which a foreign actor could probe or breach broader ICTS systems within the United States. According to research by Upstream, remote malicious cyber activities—which rely on network connectivity (e.g., Wi-Fi, Bluetooth, 3/4/5G networks)—have increased significantly in recent years and consistently outnumber malicious cyber activities carried out through physical access to devices since at least 2010, accounting for 95 percent of all malicious cyber activities in 2023. *See* Upstream, *Upstream's 2024 Global Automotive Cybersecurity Report* (2024), https://upstream.auto/reports/global-automotive-cybersecurity-report/. Considering the increasingly sophisticated methodologies employed by foreign adversaries to gain access to critical U.S. cyber infrastructure, compromised VCS and ADS, with their inherent connectivity, would easily present another attack surface for foreign adversaries to exploit. As detailed in the previous analysis of vulnerabilities inherent in VCS, adversaries with access to VCS, such as to telematics systems, could inject malicious code into a vehicle's operational systems. Additionally, such malware could be developed in such a way as to exploit vehicle connectivity to propagate itself across multiple systems as the vehicle travels and connects to those discrete systems. In this way, not only would the ICTS integral to Connected Vehicles be compromised, but vehicle systems could be exploited to spread malware with the intent of harming all ICTS systems to which a vehicle connects. *See* Anastasios Giannaros, et al. "Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain and Future Directions*," Journal of Cybersecurity and Privacy* 3.3 (2023).

Second, as discussed, both VCS and ADS have significant control over and access to critical vehicle functions, including steering, braking, speed control, ignition, and almost all other mechanical functions of the vehicle. Such extensive control over vehicle operations could enable a foreign adversary to use a compromised VCS or ADS component to hamper vehicle functions or even to manipulate a connected vehicle for malicious purposes. As VCS and ADS control or

link to integral vehicle functions, a foreign adversary could even exploit compromised VCS or ADS components to impair or disable a connected vehicle while in transit. Disabled, impaired, or otherwise improperly functioning vehicles could result in grave damage or impediment to critical infrastructure within the United States, or in physical harm to U.S. persons. A disabled, impaired, or erratically functioning Connected Vehicle, or potentially multiple Connected Vehicles all experiencing such problems simultaneously, could result not only in traffic patterns that would effectively block critical transportation arteries, but could cause collisions ultimately damaging transportation features (e.g., roadways, bridges, tunnels) and energy, telecommunications, and similar infrastructure situated near transportation systems. The potential consequences of widespread connected vehicle impairment could be particularly acute if the targets were fleet vehicles operating in support of infrastructure vital to transportation, energy, water, waste, telecommunications, and other essential services.

The risks to the resiliency of critical U.S. infrastructure posed by connected vehicle components designed, developed, manufactured, or supplied by persons that are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia are further compounded by the potential for VCS and ADS to collect data on infrastructure. Advances in VCS and ADS necessitate increasingly cutting-edge sensor suites incorporating radar, LiDAR, camera, sonar, and computer vision to gather information on the surrounding environment for both onboard computing and remote cloud computing to process data in informing vehicle operating decisions. This vast wealth of data, collected over time by multiple vehicles likely contains valuable information such as location data about critical U.S. infrastructure. For example, data gathered from GPS/GNSS systems in a connected vehicle could be cross-referenced and collated with a multitude of other data to produce information about the location, function, and operational trends of various transportation, energy, or other critical infrastructure. A foreign adversary could extract such critical infrastructure data using its control over designers, developers, manufacturers, or suppliers of VCS and ADS components subject to the

foreign adversary's ownership, control, jurisdiction, or direction, thereby increasing the risk and precision of attacks on such critical infrastructure.

Finally, given the volume of information collected by vehicles to support VCS and ADS operation, exploitation of these systems could enable an adversary to cull a tremendous amount of data on vehicle movement across the United States. This information could potentially include data generated on or from fleet vehicles used by emergency response, law enforcement, or the military. This data, and particularly all metadata and derived data that can be drawn from the raw data, can provide considerable insight into fleet size, composition, and capabilities, as well as information on organizational response times and response procedures. Such information would prove valuable to an adversary seeking to disrupt U.S. emergency response operations. Any potential risks to U.S. national security arising from disrupting emergency response activities are further compounded by the potential for an adversary to exploit access to VCS and ADS to leverage the persistent connectivity required for malign operations, including exploits to trigger improper engine shutdown, brake activation, or electrical system deactivation. Any of these actions have serious consequences for U.S. persons' health and safety. The PRC or Russia could use similar methods to target U.S. persons other than institutions, thereby imperiling the safety and security of individual U.S. citizens or residents. VCS and ADS, if corrupted by the producer at the direction of a foreign adversary, could improperly access driver mobile devices to collect, exfiltrate, and exploit personally identifiable information (PII) or even protected health information (PHI). It is also possible that a foreign adversary could use covert access to VCS and ADS to provide false or misleading information to a driver, causing degraded and dangerous vehicle operation conditions. Such tactics could be used either indiscriminately to sow panic and cause disruption, or to intentionally target specific drivers. Additionally, and as noted by the Office of the Director of National Intelligence in the 2024 National Counterintelligence Strategy, foreign adversaries, like the PRC and Russia, view this kind of PII and PHI as particularly valuable as it provides them "not only economic and R&D benefits, but also useful

[counterintelligence] information, as hostile intelligence services can use vulnerabilities gleaned from such data to target and blackmail individuals." *See* The Director of Nat'l Intelligence, *2024 National Counterintelligence Strategy* (Aug. 2024), https://www.dni.gov/files/NCSC/documents/features/NCSC_CI_Strategy-pages-20240730.pdf.

Even when such systems are not subject to compromise, companies owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, if occupying certain positions within the supply chain, may potentially legally gain access to their users' personal data. For example, one prominent Chinese auto manufacturer with operations in the United States publicly states in its U.S. privacy policy that the personal data it may collect (e.g., identifiers, customer records information, internet or other electronic network activity information, geolocation information, professional or employment-related information) is only stored in the United States "in principle," but goes on to note that personal data "may be transferred to our headquarters in China" for processing and storage. While the incorporation in the U.S. supply chain of VCS hardware and covered software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia poses one type of risk, transactions involving VCS hardware and covered software pose a separate risk when the connected vehicle manufacturer is, itself, owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, even when the connected vehicle manufacturer is located in the United States. connected vehicle manufacturers have privileged and direct access to all systems in the vehicle, including the VCS hardware and covered software. Not only are VCS hardware and covered software built to the connected vehicle manufacturers' specifications but prior to the sale of a completed connected vehicle, connected vehicle Manufacturers are able to exercise significant levels of control over that VCS hardware and covered software with little to no external oversight prior to the sale of the completed connected vehicle. Based on the foregoing, BIS assesses that ICTS transactions involving VCS hardware or covered software designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to

the jurisdiction or direction of the PRC or Russia—including transactions to supply the VCS hardware or covered software into the United States market as part of the sale of the completed connected vehicle—present undue or unacceptable risks to the national security of the United States within the meaning of E.O. 13873. BIS welcomes comment on the vulnerabilities and risks it has identified.

V. Discussion of the Proposed Rule and Request for Comments

BIS proposes a regulation that would—absent a general or specific authorization otherwise—(1) prohibit VCS hardware importers from knowingly importing into the United States certain hardware for VCS; (2) prohibit connected vehicle manufacturers from knowingly importing into the United States completed connected vehicles incorporating covered software; (3) prohibit connected vehicle manufacturers from knowingly selling within the United States completed connected vehicles that incorporate covered software; and (4) prohibit connected vehicle manufacturers who are persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia from knowingly Selling in the United States completed connected vehicles that incorporate VCS hardware or covered software (collectively, "Prohibited Transactions"). These prohibitions would apply to transactions when such VCS hardware or covered software is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

BIS anticipates that this rule would primarily impact market participants who could be considered VCS Hardware Importers or connected vehicle manufacturers, such as OEMs and importers of completed connected vehicles, as well as Tier 1 and Tier 2 suppliers of VCS Hardware. For these entities, three compliance mechanisms—Declarations of Conformity, general authorizations, and specific authorizations—are available, depending on whether the VCS hardware importer or connected vehicle manufacturer wishes to engage in an otherwise prohibited transaction. Importantly, because VCS hardware importers and connected vehicle manufacturers frequently offer many different types of products, any one of the three

mechanisms may not be available for their entire business. Rather, depending on the product, VCS hardware importers and connected vehicle manufacturers could be required to use a combination of these three mechanisms to meet their obligations under the rule.

First, Declarations of Conformity would have to be submitted to BIS by VCS hardware importers and connected vehicle manufacturers who have not engaged in a prohibited transaction, unless otherwise specified. Such VCS hardware importers and connected vehicle manufacturers would, in this Declaration of Conformity, certify, once per calendar year or model year (or whenever material changes occur) to BIS that the submitter has not engaged in a prohibited transaction and provide certain information on the import of VCS hardware and/or the import or sale of completed connected vehicles.

Second, a general authorization could be available for VCS hardware importers and/or connected vehicle manufacturers seeking to engage in an otherwise prohibited transaction, depending on the circumstances. A general authorization would allow the VCS hardware Importer and/or connected vehicle manufacturer to engage in the otherwise prohibited transaction, without the need to notify or seek approval from BIS. General authorizations would be available only in a narrow set of circumstances in which the conditions of the otherwise prohibited transaction appropriately mitigate the level of risk associated with the particular transaction. Such conditions would include, for example, when VCS hardware is imported from the PRC or Russia solely for testing purposes, or where the completed connected vehicle that incorporates VCS hardware or covered software from the PRC or Russia will be driven on public roads for fewer than 30 calendar days per year. Those availing themselves of a general authorization would be required to continuously monitor their use of the VCS hardware or completed connected vehicles covered by the General Authorization to ensure the authorization still applies. If a change would render the transaction ineligible for a general authorization, such as a change in the vehicle's use, the VCS hardware importer or connected vehicle manufacturer would be required to apply for a specific authorization and to cease engaging in such transaction

unless and until a Specific Authorization is granted. For example, if a completed connected vehiclethat incorporates covered software or VCS Hardware that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia is no longer used solely for display, research, or testing, the VCS hardware importer or the connected vehicle manufacturer would be required to seek a specific authorization. Similarly, if the VCS Hardware Importer or connected vehicle manufacturer meets or exceeds total model year production of 1,000 units, or if a completed connected vehiclethat incorporates covered software or VCS hardware that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia is to be used on public roadways for 30 or more days in any calendar year, the VCS hardware importer or connected vehicle manufacturer would be required to seek a specific authorization from BIS.

Lastly, for VCS hardware importers and connected vehicle manufacturers who wish to engage in a prohibited transaction, but do not otherwise qualify for a general authorization, a specific authorization from BIS would be required before they could proceed with the prohibited transaction. A specific authorization would only be available in circumstances where BIS determines, based on the information submitted by the applicant and other collected information, that the otherwise prohibited transaction does not present an undue or unacceptable risk to U.S. national security. However, as a condition of approving the specific authorization, BIS might impose certain requirements and mitigation measures upon the VCS hardware importers and connected vehicles manufacturers seeking to proceed with the prohibited transaction.

VCS hardware importers and connected vehicle manufacturers could appeal to the Under Secretary for Industry and Security (Under Secretary) any decision by BIS to deny an application for a Specific Authorization, suspend or revoke a previously granted specific authorization, or issue a written notification that a VCS hardware importer or connected vehicle manufacturer is ineligible for a general authorization. Further, the regulation would establish a method for VCS

hardware importers and connected vehicle Manufacturers to seek guidance from BIS, in the form of advisory opinions, on prospective transactions that may be prohibited. BIS also proposes to establish a process through which BIS may inform VCS hardware importers or connected vehicle manufacturers that certain of their activities could constitute a prohibited transaction.

In proposing this rule, BIS recognizes that Section 203(b) of IEEPA—i.e., the "Berman Amendment"—limits the scope of the authority to regulate or prohibit transactions relating to "information" or "informational materials." In relevant part, the Berman Amendment states that the "authority granted to the President by this section does not include the authority to regulate or prohibit, directly or indirectly . . . the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and newswire feeds." 50 U.S.C. 1702(b)(3). Consistent with the statute's text and purpose, as demonstrated by legislative history and context, as well as judicial interpretations, BIS understands the phrase "information or informational materials" to refer to expressive materials and mediums that may be carrying such expressive content. See, e.g., *United States v. Amirnazmi*, 645 F.3d 564, 586–87 (3d Cir. 2011). Accordingly, the Berman Amendment prevents BIS from regulating, directly or indirectly, the import or export of expressive materials. It does not, however, prevent BIS from imposing a regulation that is aimed at the functional capabilities of technology.

The proposed rule is consistent with the Berman Amendment. Its purpose is to regulate transactions involving certain hardware and software based on functional capabilities that can be exploited by foreign adversaries, not the exchange of ideas and expression that the Berman Amendment protects. As discussed in Section IV, VCS Hardware and covered software process and transmit data such as geolocation information or systems diagnostics reports, which are used to monitor and control the vehicle's safe operation, and that a foreign adversary could also

manipulate in ways that could impair or disable the vehicle's function, leading to dangerous outcomes that pose a harm to U.S. national security. Similarly, the functional data collected by Covered Software—such as high-definition mapping data of infrastructure and roadways—would pose serious risks to that critical infrastructure if collected and exploited by a foreign adversary. As a result, BIS has determined that the proposed prohibitions in this rule are consistent with the Berman Amendment, which was intended to protect materials involving the free exchange of ideas from regulation under IEEPA. BIS is considering whether and how to address the term "information or informational materials" within the context of the proposed rule and may consider further changes to the final rule to reflect our interpretation of this term. BIS welcomes comment on this issue.

Each section of the proposed rule is discussed below. BIS invites comments on all aspects of this proposed rule.

a. Definitions

1. Automated Driving System (ADS)

BIS proposes to define "Automated Driving System" to mean 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 ODD. This definition is consistent with the terminology industry uses for systems that operate at certain advanced levels of autonomy. It is also consistent with definitions issued by NHTSA. Specifically, this definition corresponds to automation levels 3, 4, and 5 as defined by SAE International standard J3016.

2. Completed Connected Vehicle

BIS proposes to define "completed connected vehicle" to mean a connected vehicle that requires no further manufacturing operations to perform its intended function. This definition is consistent with definitions issued by NHTSA. Additionally, for the purposes of this proposed definition, the integration of an ADS into a connected vehicle constitutes a manufacturing

operation for a Completed Connected Vehicle. BIS intends this caveat to clarify that a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, whose sole manufacturing or assembly operation is integrating ADS into an otherwise Completed Connected Vehicle, would be subject to the prohibitions in the rule and would need to obtain a Specific Authorization before importing or Selling that completed connected vehiclein the United States.

3. Connected Vehicle

BIS proposes to define "connected vehicle" to mean 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. Vehicles operated only on a rail line are not included in this definition. This definition incorporates the suggestions of commenters to the ANPRM, many of whom requested that the definition of connected vehicle specify the types of vehicles that would be covered.

4. Connected Vehicle Manufacturer

BIS proposes to define a "connected vehicle manufacturer" to mean 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.

5. Covered Software

BIS proposes to define "covered software" to mean the software-based components, in which there is a foreign interest, executed by the primary processing unit of the respective systems that are part of an item that supports the function of VCS or ADS at the vehicle level. covered software does not include firmware, which is characterized as software specifically programmed for a hardware device with a primary purpose of controlling, configuring, and communicating with that hardware device. At a minimum, this definition of covered software would include

operating systems such as a real-time operating system (RTOS), and general-purpose operating systems. An example of covered software within the ADS is, if included in the system, the machine learning software that performs the functions of object detection, classification, and decision making.

Covered software does not include open-source software. BIS understands open-source software as software that can be freely used, modified, and distributed by anyone, with both access to the source code and the ability to contribute to the software's development and improvement. Given these qualities of open-source software, it is not designed, developed, manufactured, or supplied by any attributable entity. Therefore, the inclusion of open-source software as a component of covered software is not subject to prohibition. However, if licensed open-source software is modified to create proprietary enterprise software for a specific use not meant for redistribution, the resulting software could be subject to prohibition if the person modifying the open-source software is owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. In addition to other aspects of this proposed rule, BIS specifically seeks comment on this definition.

6. FCC ID Number

BIS proposes to define "FCC ID Number" as the unique alphanumeric code identifying a product subject to certification by the Federal Communications Commission (FCC) composed of a (1) grantee code and (2) product code.

7. Foreign Interest

For the purposes of this rule, BIS is considering "foreign interest," when used with respect to property, as any interest in property, of any nature whatsoever, whether direct or indirect, by a non-U.S. person. Under this definition, a foreign interest can include, but is not limited to, an interest through ownership, intellectual property, contract—e.g., ongoing supply commitments such as maintenance, any license agreement related to the use of intellectual property—profit-sharing or fee arrangement, as well as any other cognizable interest. This definition is consistent

with the definition of "interest" used in the context of Office of Foreign Asset Control sanctions, which are, in relevant part, also established pursuant to the statutory requirements of IEEPA. *See* 31 CFR Chapter V, *and, e.g.*, 31 CFR 510.313, 535.312.

Consistent with IEEPA, BIS proposes to regulate only transactions involving property in which a foreign country or national thereof has any such interest. A transaction would be subject to the prohibitions in the proposed rule only if it involves ICTS, specifically VCS hardware or covered software, that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. VCS hardware importers and connected vehicle manufacturers wishing to engage in transactions that this rule proposes to prohibit would need to qualify for a general authorization or obtain a specific authorization. In order to provide sufficient visibility into the supply chains of VCS Hardware and covered software including to verify that the transaction does not involve VCS Hardware or covered software that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia (*see* Section V(c) of this notice and proposed Section 791.305), BIS is proposing to require that VCS hardware importers and connected vehicle manufacturers that import VCS hardware, or import or sell completed connected vehicles that contain covered software in which there is any other foreign interest, submit an annual Declaration of Conformity containing relevant details about the import or Sale. BIS seeks comment on this regulatory approach, including the necessity and efficacy of requiring Declarations of Conformity with respect to VCS hardware and covered software in which there is a foreign interest, though not a foreign adversary interest. BIS also seeks comment on the availability and efficacy of any alternative approach that would require a narrower set of VCS hardware importers and completed connected vehicle manufacturers to submit Declarations of Conformity, while still achieving the goals of the Declaration of Conformity requirement and addressing the declared emergency under Executive Order 13873.

With respect to VCS hardware that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, BIS proposes to regulate the importation of VCS hardware, making VCS hardware importers responsible for compliance.

With respect to Covered Software, based on discussions with connected vehicle manufacturers, automotive suppliers, and other stakeholders, BIS has come to understand that typically, ADS and VCS software are designed or developed to a connected vehicle manufacturer's specifications. ADS and VCS software is frequently designed, developed, or supplied by foreign persons, and those persons frequently retain a legally cognizable interest in the underlying software, even after it has been integrated into the connected vehicle. For example, foreign software developers may earn profits from use of their software; retain data access and sharing rights to the software; or have obligations to maintain and update the software. Such arrangements are among the types of interests that BIS contemplates as giving rise to an obligation to submit a Declaration of Conformity or, if the software designer, developer, or supplier is a person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, to qualify for a General Authorization or seek a Specific Authorization under the proposed rule. BIS therefore proposes to regulate covered software by regulating the importation or sale of completed connected vehicles, making connected vehicle Manufacturers responsible for compliance. BIS seeks comment on this understanding of foreign interests in covered software as well as other arrangements in which foreign designers, developers, or suppliers of covered software retain a cognizable legal interest in the software after it is integrated into a connected vehicle.

Finally, in addition to the general regulations related to VCS hardware and covered software described above, with respect to connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, BIS additionally proposes to regulate VCS hardware and covered software by regulating the sale of completed connected

vehicles that incorporate VCS hardware or covered software. In this circumstance, BIS understands from extensive engagement with connected vehicle manufacturers and automotive suppliers that persons who own, control, or direct the operations of the connected vehicle manufacturer would maintain an interest in the vehicle transactions that the connected vehicle manufacturer carries out. For example, this could include, but is not limited to, profit sharing agreements between a parent company and its U.S. subsidiary, or data sharing agreements between the same. BIS understands this to be standard for the automotive industry and would welcome comments on this issue. Additionally, because the PRC and Russian legal regimes discussed in Section IV of this notice could compel a PRC or Russia-based parent company of a connected vehicle manufacturer to provide those governments with information on or access to the operations of the U.S.-based connected vehicle manufacturer, BIS understands that the foreign parent company typically retains a legal right to access the data collected by the U.S. subsidiary, representing a foreign interest in that U.S. subsidiary and its connected vehicle sales.

BIS seeks comment on the nature of foreign interests in transactions related to the connected vehicle supply chain, including as described in the prohibitions outlined herein. BIS also seeks comment as to its understanding of the nature and presence of a Foreign Interest in property subject to the prohibitions described above, as well as whether there are other types of transactions that would involve Foreign Interests, as described above.

8. Hardware Bill of Materials

BIS proposes to define "Hardware Bill of Materials" or HBOM as a comprehensive list of parts, assemblies, documents, drawings, and components required to create a physical product. This term includes information identifying the manufacturer, related firmware, technical information, and descriptive information.

9. Import

BIS proposes to define "import" to mean, with respect to any article, the entry of such article into the United States Customs Territory. It does not include admission of an article from outside

the United States into a foreign-trade zone for storage pending further assembly in the foreign-trade zone, or shipment to a foreign country. This definition only applies to subpart D of 15 CFR part 791.

10. Item

BIS proposes to define "item" as a component or set of components with a specific function at the vehicle level. A system may also be considered an item if it implements a function. This definition is consistent with ISO/SAE Standard 21434.

11. Knowingly

BIS proposes to define "knowingly" to have the same meaning given to "knowledge" in the Export Administration Regulations (15 CFR 772.1). Knowledge of a circumstance (the term may be a variant, such as "know," "reason to know," or "reason to believe") includes not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence. Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person's willful avoidance of facts.

12. Model Year

Consistent with the definition used by NHTSA, BIS proposes to define "model year" as the year used to designate a discrete vehicle model, irrespective of the calendar year in which the vehicle was actually produced, provided that the production period does not exceed 24 months. Throughout this proposed rule, BIS refers to both calendar year and model year when referring to the import of VCS Hardware, particularly for the submission of Declarations of Conformity (791.305) and the implementation timeline (791.308 (Exemptions)). BIS generally understands that most VCS hardware is imported into the United States already destined for a known, specific model year of vehicle. BIS also understands that some VCS hardware units may be imported without being associated with a specific vehicle model year. As such, the proposed rule provides

separate timelines for each of these cases to accommodate business timelines for VCS hardware importers. BIS is particularly interested in comment on this approach.

13. Person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary

BIS proposes to define "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" to mean, (a) 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; (b) 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; (c) 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 (d) 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.

14. Prohibited Transactions

BIS proposes to define "prohibited transactions" as, collectively, the transactions described in §§ 791.302 (Prohibited VCS hardware transactions), 791.303 (Prohibited covered software transactions), or 791.304 (Related prohibited transactions). The term prohibited transactions

refers to the prohibitions on the knowing import of VCS hardware into the United States that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, as specified in section 791.302; the knowing Sale within, or import into, the United States of a completed connected vehicle containing covered software that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, as specified in § 791.303; and the knowing Sale of completed connected vehicles that incorporate VCS Hardware or covered software by connected vehicle Manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, as specified in § 791.304.

15. Sale

BIS proposes to define "sale," in the context of this subpart, as 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, as those terms are defined in 49 U.S.C. 30102. This definition also applies to the related terms such as sell or selling. This would include direct-to-consumer sales of completed connected vehicles from the connected vehicle manufacturer to the ultimate purchaser.

16. Software Bill of Materials

BIS proposes to define "Software Bill of Materials" or SBOM 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.

BIS understands that this definition generally conforms to industry standards. However, BIS is specifically seeking comment on the feasibility, technical burden, cost, and effectiveness of identifying and disclosing to BIS the listed SBOM attributes.

17. Vehicle Connectivity System

BIS proposes to define "Vehicle Connectivity System" or VCS as a hardware or software item for a completed connected vehicle that has the function of enabling the transmission, receipt, conversion, or processing of radio frequency communications at a frequency over 450 megahertz. This definition would exempt most remote keyless entry fobs and immobilizers and certain internal wireless sensors and relays. VCS software is included in the definition of Covered Software.

18. VCS Hardware

BIS proposes to define "VCS hardware" as the following software-enabled or programmable components and subcomponents that support the function of Vehicle Connectivity Systems or that are part of an item that supports the function of Vehicle Connectivity Systems: 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). VCS hardware would include aftermarket devices not contained in a completed connected vehicle at sale but that could be later integrated into or attached to the vehicle to perform VCS functions.

BIS believes this definition appropriately identifies the various components, contained within a TCU or other connected systems of a connected vehicle, that facilitate off-board data transmission, and, thus, are most likely to pose the risks identified in Section IV of this notice.

BIS specifically seeks comment on this list of components and the appropriateness of their inclusion to address the national security risks that BIS has identified in this notice.

19. VCS Hardware Importer

BIS proposes to define "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.

This definition would capture OEMs, and tier 1 and tier 2 suppliers importing VCS hardware into the United States. BIS specifically seeks comment on the scope of this definition, particularly regarding whether it captures the breadth of market participants dealing in VCS Hardware.

20. United States

BIS proposes to define "United States" to mean the United States of America, the States of the United States, the District of Columbia, and any commonwealth, territory, dependency, or possession of the United States, or any subdivision thereof, and the territorial sea of the United States.

b. Prohibitions on Certain Transactions Related to Connected Vehicles

1. Prohibited Transactions

Under the proposed rule, VCS hardware importers would be prohibited from knowingly importing into the United States any VCS hardware that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. BIS specifically seeks comment on this approach and whether additional components should be included in or excluded from this prohibition.

Connected vehicle manufacturers would be prohibited from knowingly Selling within the United States, or importing into the United States, completed connected vehicles that incorporate

covered software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

Connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia would also be prohibited from knowingly Selling in the United States completed connected vehicles that incorporate covered software or VCS hardware. As with other connected vehicle manufacturers, connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia participate in the design and development of VCS hardware and covered software, which are generally built to the manufacturers' specifications. However, this prohibition applies even if connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia were not involved in the design or development of the VCS Hardware and Covered Software. Their Sale of those completed connected vehicles constitutes the supply of VCS hardware and covered software and is thus captured by this prohibition. To be clear, BIS anticipates that because of the role connected vehicle manufacturers play in the design and development of the key components in connected vehicles, in many cases, this prohibition will be duplicative of the other prohibitions in this proposed rule. BIS seeks comments on the efficacy of all of the proposed prohibitions detailed above.

As noted above, for the purposes of this proposed rule, BIS defines the term "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" to mean (a) 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; (b) 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; (c) 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 (d) 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.

To provide further clarity regarding transactions involving VCS hardware and covered software that would be prohibited, BIS offers the following examples of persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC and Russia:

Example 1: Company A, incorporated in the United States, is a wholly owned subsidiary of Company B. Company B is a state-owned enterprise of the PRC or Russia. Because Company B is a state-owned enterprise, Company A would be considered "owned by" the PRC or Russia.

Example 2: Company A is a joint venture between Company B and Company C where Company C owns a majority share of Company A. Company B is a corporation incorporated in a third-party jurisdiction. Company C is a state-owned enterprise of the PRC or Russia. Company A would be considered "owned by" the PRC or Russia.

Example 3: Company A is majority owned in aggregate by multiple state-owned enterprises and state-owned investment funds of the PRC or Russia. Company A would be considered "owned by" the PRC or Russia.

Example 4: Company A, incorporated in the United States, is a subsidiary of Company B. Company B is a private company incorporated in the PRC or Russia with its principal place of business in the PRC or Russia. Because Company B is subject to the jurisdiction of the PRC or Russia, Company B's subsidiary, Company A, is controlled by an entity subject to the

jurisdiction of the PRC or Russia and would be considered "controlled by" and "subject to the direction of" the PRC or Russia.

Example 5: Company A is a multinational company where a majority of the voting power is held by Company B, a PRC or Russian government investment fund. Company A would be "controlled by" and "subject to the direction of" the PRC or Russia.

Example 6: Company A is a holding company organized in a tax-advantaged jurisdiction. Company A is publicly listed on a stock exchange and its corporate voting structure is characterized by Class A and Class B shares, Class B shares having ten times the voting power of Class A shares. If the aggregate voting power of shareholders subject to the jurisdiction of the PRC or Russia holding either Class A and Class B shares constitutes a majority or a dominant minority of total voting power, then Company A would be "controlled by" and "subject to the direction of" the PRC or Russia.

Example 7: Company A, a company that is organized under the laws of the PRC 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 the PRC or Russia.

Example 8: Company A is an entity incorporated in a third country and Company B is an entity incorporated in the PRC or Russia. Company A and Company B create a new joint venture, Company C, to design, develop, and manufacture a new product. Company A and Company B own minority shares of the joint venture while Company D, a holding company wholly owned by a PRC citizen, owns the largest minority share. If aggregate voting power of Company B and Company D constitutes majority or dominant minority voting share, Company C would be "controlled by" and "subject to the direction of" the PRC or Russia.

Example 9: 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, the PRC 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" the PRC or Russia.

Example 10: The PRC or Russian government, through an investment fund, acquires a 1% special management share in Company A. This share grants the PRC or Russian government the right to appoint a director to the board of Company A and veto certain key business decisions, such as major strategic changes or mergers. This share allows the government to influence Company A's operations and strategy. Company A would be "controlled by" the PRC or Russia.

Example 11: Company A maintains its principal place of business in the PRC or Russia. Company A would be "subject to the jurisdiction" of the PRC or Russia.

Example 12: Company A is a publicly listed U.S. corporate entity. Company A has a wholly owned subsidiary, Company B, that is organized under the laws of the PRC or Russia and manufactures goods in the PRC or Russia. Because Company B is organized under the laws of the PRC or Russia, Company B would be subject to the jurisdiction of the PRC or Russia. However, Company A is not subject to the jurisdiction of the PRC or Russia by nature of its subsidiary, Company B, being "subject to the jurisdiction" of the PRC or Russia.

Example 13: 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 PRC corporation, has known ties to the government of the PRC, 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 PRC 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 PRC 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 PRC corporate entities, and Person X's close ties to the PRC government indicate that Company A would be "subject to the direction" of the PRC.

BIS seeks comment on whether the definition of, and examples provided to illuminate, who is a "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary," provides sufficient clarity regarding the circumstances under which the rule's prohibitions might apply.

For additional clarity in determining whether a transaction involving VCS hardware or covered software designed, developed, manufactured, or supplied by entities described above would be prohibited under the proposed rule, BIS offers the below examples. In offering these examples, BIS emphasizes that 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 the PRC 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:

Example 14: A U.S. person has a contractual relationship with a foreign person to import a cellular module, and the cellular module will later be integrated into a VCS for a completed connected vehicle. The U.S. person is, under the proposed rule, a VCS hardware importer. The U.S. person knows the cellular module was manufactured at a facility located in the PRC or Russia and is being imported through a third country. Since the entity manufacturing the module would, at a minimum, be "subject to the jurisdiction" of the PRC or Russia, the import of the module would be a prohibited transaction under the proposed rule, unless it qualifies for a general authorization or a specific authorization from BIS.

Example 15: A U.S. person imports a TCU that was assembled in a third country, but that contains a microcontroller that is manufactured in the PRC or Russia and is Sold to the third-country assembler of the TCU. The U.S. person knows that the microcontroller was manufactured by an entity located in the PRC or Russia. As the microcontroller is included in the definition of VCS hardware, the import of the TCU for a completed connected vehiclewould be a prohibited transaction under the proposed rule unless it qualifies for a general authorization, or a specific authorization granted by BIS.

Example 16: A U.S. person imports a completed connected vehicle, making the U.S. person a connected vehicle manufacturer under the proposed rule's definition. The completed connected vehicle contains a TCU that operates software supporting off-vehicle connectivity above 450 MHz, and that software is designed, developed, or otherwise supplied (in whole or in part) by an entity located in the PRC or Russia. Under the proposed rule, the import of the completed connected vehicle would be prohibited, unless it was authorized by a general authorization or a Specific Authorization.

Example 17: A U.S. person who is a connected vehicle manufacturer that manufactures or assembles completed connected vehicles in the United States Sells to a dealer within the United States a completed connected vehicle in which the vehicle's ADS software for object detection, classification, and decision making is proprietary software designed, developed, or supplied by an entity in the PRC or Russia. The Sale or transfer of the completed connected vehicle would be a prohibited transaction under the proposed rule unless it qualifies for a general authorization or specific authorization granted by BIS.

Example 18: A U.S. person who is a connected vehicle manufacturer utilizes foreign VCS and ADS software development teams through various subsidiaries, joint ventures, and contract arrangements, some of which retain servicing obligations, contractual and licensing rights, and other interests in the software they have developed. One of those software development teams is located in the PRC or Russia, and as such, that software team is subject to the jurisdiction of the

PRC or Russia. Given the role of PRC or Russian developers in the creation of the VCS or ADS software (covered software), the sale of a completed connected vehicle within the United States that integrates this proprietary covered software, would be a prohibited transaction under the proposed rule, unless it qualifies for a general authorization or specific authorization granted by BIS.

Example 19: A U.S. person who is a connected vehicle manufacturer utilizes VCS and ADS software development teams around the world through various subsidiaries, joint ventures, and contract arrangements. One of those software development teams is comprised of individuals who are PRC or Russian citizens working in a foreign jurisdiction other than the PRC or Russia for a company that is not owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. Although the individuals technically meet the definition of "person owned by, controlled by, or subject to the direction of a foreign adversary," the sole fact that PRC or Russian citizens work on the connected vehicle manufacturer's software development would not make the Sale of a completed connected vehicle within the United States that integrates this VCS or ADS software a Prohibited Transaction under the proposed rule.

Example 20: Company A, which is a wholly owned subsidiary of a foreign corporation in which a PRC or Russian entity owns a controlling interest, imports completed connected vehicles that incorporate covered software and VCS hardware, none of which was originally designed, developed, manufactured, or supplied by an entity owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. In such rare circumstance where Company A did not participate in the design or development of the covered software or VCS hardware, Company A would submit (once per Model Year) a Declaration of Conformity for the import of the completed connected vehicles containing covered software and VCS hardware. However, any subsequent sale by Company A of such completed connected vehicle in the United States would be prohibited. For example, Company A subsequently Sells such completed connected vehicles to a dealer in the United States. Because Company A is a person controlled by the PRC or Russia

and has direct privileged access to the VCS Hardware and covered software prior to the sale, the knowing sale by Company A of the completed connected vehicle with VCS hardware and covered software would be a prohibited transaction under the proposed rule, and a specific authorization from BIS would be required before engaging in such a transaction.

Example 21: Company A, a wholly owned subsidiary of a PRC or Russia corporation manufactures completed connected vehicles in the United States. The completed connected vehicles that Company A manufactures incorporate covered software and VCS hardware provided by Company B, a company that is not owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. Because Company A is owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, participated in the design and development of the covered software or VCS hardware, and in any event, has direct and privileged access to its completed connected vehicles—including the incorporated covered software and VCS hardware—Company A's sale of the completed connected vehicles is a prohibited transaction under the proposed rule, and a specific authorization from BIS would be required before engaging in such a transaction.

c. Compliance

1. Declaration of Conformity

BIS proposes to require VCS Hardware Importers and connected vehicle manufacturers engaged in specified transactions to submit Declarations of Conformity to BIS certifying that they have not engaged in a prohibited transaction. Under the proposed rule, declarants would be responsible for submitting information to BIS, including documentation collected from suppliers of components of VCS hardware and from suppliers of covered software, to verify compliance with the regulations. These requirements include obtaining and analyzing the HBOMs for VCS hardware and the SBOMs for covered software and providing documentation of the steps the declarant took to verify that the transactions comply with the provisions of the rule. In an effort to facilitate compliance, BIS is not currently proposing to mandate particular due diligence

requirements but would rather allow VCS hardware importers and connected vehicle Manufacturers to provide evidence of their own efforts tailored to their unique operations. BIS seeks comment on this approach.

The proposed rule generally contemplates that Declarations of Conformity would be submitted in three instances by persons not engaged in prohibited transactions: (1) Declarations submitted by VCS hardware importers; (2) Declarations submitted by connected vehicle manufacturers importing completed connected vehicles containing covered software into the United States; and (3) Declarations submitted by connected vehicle manufacturers selling completed connected vehicles in the United States that they have manufactured or assembled in the United States and which contain covered software, so long as there is a continuing foreign interest in the covered software. Persons required to submit a Declaration of Conformity need do so 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. VCS hardware importers or connected vehicle manufacturers engaging in multiple transactions that require submissions of Declarations of Conformity under separate paragraphs of § 791.305 may, if they prefer, submit a single compiled Declaration of Conformity containing all required information for all transactions. 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.

BIS believes that Declarations of Conformity will be an important tool for advancing the goals of this proposed rule, and addressing the emergency declared in E.O. 13873. Declarations of Conformity will first and foremost provide BIS with a means to verify VCS hardware importers' and completed connected vehicle manufacturers' compliance with the proposed prohibitions. Through extensive engagement with connected vehicle manufacturers and

automotive suppliers, BIS has come to understand that connected vehicle supply chains are complex and often opaque, with potentially hundreds of suppliers for a single connected vehicle in a given model year. Such complexity and opacity could result in the incorporation into connected vehicles of VCS hardware and covered software that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries, without the full knowledge of the connected vehicle manufacturer. While connected vehicle manufacturers typically have strong relationships with their immediate suppliers, to include the development of years-long supply contracts that span entire vehicle generations, their understanding of the deeper supply chain (to include who is supplying their suppliers) is substantially weaker. Additionally, while the COVID-19 pandemic and associated supply chain crisis forced connected vehicle manufacturers to more critically evaluate their hardware supply chains, illumination of software supply chains remains largely unachieved. Consequently, BIS believes that the requirement to submit annual Declarations of Conformity will serve as an important mechanism for ensuring 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 the proposed rule's prohibitions on the incorporation of VCS Hardware or covered software that has been designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

BIS also believes that the collection of annual Declarations of Conformity from connected vehicle manufacturers and VCS hardware importers would facilitate enforcement of the proposed rule, including by allowing BIS to proactively identify red flags and potential violations of the proposed prohibitions. For example, BIS may rely on the broad perspective provided by the Declarations of Conformity from multiple connected vehicle manufacturers and VCS hardware importers to identify previously undetected participation by PRC or Russian designers, developers, manufacturers, or suppliers that are subject to the prohibitions of this

proposed rule yet remain entrenched in the U.S. connected vehicle supply chain. Additionally, these Declarations of Conformity would allow BIS to maintain an understanding of technological advancements and changes in the U.S. connected vehicle industry—both in hardware and software—and consequently enable BIS to propose updates to the rule as needed to maximize its effectiveness in mitigating the undue and unacceptable risks posed by the PRC and Russia while minimizing burden on industry.

The sections below explain in greater detail the types of Declaration of Conformity that would be required under the proposed rule. BIS seeks comment on this regulatory approach, including the necessity and efficacy of requiring Declarations of Conformity with respect to VCS hardware and covered software in which there is a Foreign Interest. BIS also seeks comment on the availability and efficacy of any alternative approach that would require a narrower set of VCS Hardware Importers and completed connected vehicle manufacturers to submit Declarations of Conformity, while still achieving the goals of the Declaration of Conformity requirement and addressing the declared emergency under E.O. 13873.

i. Import of VCS Hardware

The Declaration of Conformity described in § 791.305(a)(1) would require VCS hardware Importers to provide information on the specific VCS hardware that the declarant plans to import into the United States for a given model year, or, for units not associated with a model year, a given calendar year. BIS proposes to require the Declaration of Conformity to contain the FCC ID number(s) of the VCS hardware, and, if applicable, any subcomponents in the VCS hardware that also have an FCC ID number. FCC regulations at 47 CFR 2.925 require any electronic device that emits RF waves, including those imported into the United States, to have an FCC ID number, which is used to identify and certify that the device meets the necessary regulatory standards for wireless communication. The proposed rule would additionally require VCS Hardware Importers to report all third-party information technology external endpoints to which the VCS Hardware is programmed to connect, including the country in which said endpoint is

located and/or the identity and location of the service provider. This would include any third-party that is not the VCS hardware importer nor the final recipient, such as the connected vehicle manufacturer that integrates the VCS hardware and receives data on an episodic or ongoing basis from the VCS hardware. Additionally, VCS hardware importers would be required to submit an HBOM as part of the Declaration of Conformity. BIS would expect, consistent with the proposed definition for this term, this HBOM to include a comprehensive list of parts and technical information, including the provenance of subcomponents contained within the VCS hardware.

ii. Import of Completed Connected Vehicles

The Declaration of Conformity described in section 791.305(a)(2) would require connected vehicle manufacturers that import completed connected vehicles, including U.S.-based OEMs and foreign-headquartered OEMs with operations in the United States, to provide information to BIS on the make, model, and trim (if known) of the imported group of completed connected vehicles and the covered software contained within the completed connected vehicles. BIS proposes to require declarants to submit an SBOM for the covered software related to both VCS and ADS. The minimum requirements for the SBOM are author's name, timestamp, supplier name, component name, version string, component hash, package URL, unique identifier, and dependency relationships to other software components. Declarants may submit additional SBOM information as evidence demonstrating the covered software is not sourced from PRC or Russian-linked entities. BIS seeks comment on all aspects of this SBOM requirement.

iii. Manufacture or Assembly of completed connected vehicles for Sale in the United States

Similarly, this proposed rule, as described in section 791.305(a)(3), would require connected vehicle Manufacturers that manufacture or assemble completed connected vehicles for sale in the United States to submit a Declaration of Conformity that includes information on the make, model, and trim of the group of completed connected vehicles and the covered software contained within the completed connected vehicles that the connected vehicle manufacturer will sell for a Model Year. BIS emphasizes that this requirement would apply only to connected

vehicle manufacturers whose vehicles incorporate covered software in which there is a foreign interest. Connected vehicle manufacturers who manufacture or assemble completed connected vehicles in the United States and whose vehicles contain no covered software in which there is a foreign interest would not be required to submit a Declaration of Conformity. However, given the global nature of automotive software supply chains, BIS anticipates that nearly all connected vehicle manufacturers of completed connected vehicles for Sale in the United States would be required to submit an annual Declaration of Conformity covering all completed connected vehicles by make, model, and trim to be manufactured for Sale in the United States for each Model Year. As detailed above, this requirement would include the submission of an SBOM for covered software incorporated into the group of completed connected vehicles.

iv. Procedures to Submit Declarations of Conformity

VCS Hardware Importers and connected vehicle manufacturers submitting a Declaration of Conformity under this rule would be required to submit the Declaration of Conformity to BIS annually, 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 model year, or 60 days prior to the import of VCS hardware covered by the Declaration of Conformity. VCS hardware importers and connected vehicle manufacturers may, at their discretion, submit a combined Declaration of Conformity, or may submit separate Declarations of Conformity (e.g., one Declaration covering import of VCS hardware and another covering import of completed connected vehicles). Declarations of Conformity covering both the import or manufacture of completed connected vehicles and the import of VCS Hardware should be submitted by the earlier of the two reporting dates. connected vehicle manufacturers that would submit a Declaration of Conformity for the import of a group of completed connected vehicles into the United States should not submit a Declaration of Conformity related to the subsequent Sale of that same group of Completed Connected Vehicles. In the event of material changes that impact the content of the Declaration of Conformity, VCS hardware importers or connected vehicle manufacturers would be required

to submit an updated Declaration of Conformity and an updated HBOM or SBOM within 30 days of such a change. Such changes may include changes in the suppliers of key subcomponents or functional aspects of the VCS hardware or covered software incorporated in the completed connected vehicle. BIS would make a web portal available on its website (https://www.bis.gov) through which VCS Hardware Importers and connected vehicle manufacturers may submit Declarations of Conformity.

2. General Authorizations

General Authorizations would allow certain VCS Hardware Importers and connected vehicle manufacturers to engage in otherwise prohibited transactions without the need to notify BIS prior to engaging in the transaction. connected vehicle manufacturers or VCS hardware importers (and entities under common control, including parents) who produce small quantities of completed connected vehicles or VCS hardware, which the proposed rule defines as fewer than 1,000 units in a calendar year, would be eligible for a general authorization. This is in line with requirements for high-volume and low-volume manufacturers found in 49 CFR part 565. BIS specifically seeks comment on this threshold for both completed connected vehicles and VCS Hardware. connected vehicle manufacturers would be eligible for a general authorization if the completed connected vehicle is otherwise subject to a prohibition but will be used on public roadways fewer than 30 days in any calendar year. For purposes of this general authorization, each use of a completed connected vehicle on public roadways on a distinct calendar day will count toward the 30-day limit, regardless of the duration of a vehicle's use on a particular day. VCS hardware importers and connected vehicle manufacturers would also qualify for a general authorization for otherwise prohibited transactions involving completed connected vehicles incorporating covered software or VCS hardware if the completed connected vehicles are used only for testing display, or research purposes and not on public roads in the United States. Lastly, VCS hardware importers or connected vehicle manufacturers would qualify for a general authorization for the importation of completed connected vehicles incorporating covered software or the importation

of VCS Hardware solely for the purposes of repair, alteration, or competition off public roads, and the vehicle or hardware will be reexported from the United States within one year of the time of import.

BIS proposes to allow persons using General Authorizations to self-certify their compliance with the applicable General Authorization. As such, these persons would not need to submit documentation to BIS but would be required to gather and maintain full records for a period of 10 years documenting compliance for all completed connected vehicles and VCS hardware covered by the general authorization. Furthermore, persons availing themselves of a general authorization would be required to continuously monitor for any changes that render a transaction ineligible for continued reliance on the general authorization. A VCS hardware importer or connected vehicle manufacturer that is no longer eligible for a general authorization would need to apply for and receive a specific authorization before engaging in an otherwise prohibited transaction. For example, connected vehicle manufacturers who import a certain model or trim of completed connected vehicles containing covered software that are originally used for display or testing purposes must seek a specific authorization before importing that model or trim of completed connected vehicle for more general use in the United States.

A connected vehicle manufacturer or VCS hardware importer that is a subsidiary, joint venture, affiliate, or other entity subject to the ownership, control, jurisdiction, or direction of the PRC or Russia would be ineligible for general authorizations and would be required to apply for a specific authorization before engaging in an otherwise prohibited transaction.

3. Specific Authorizations

VCS hardware importers and connected vehicle manufacturers wishing to engage in an otherwise prohibited transaction who are ineligible for an exemption or general authorization would have to apply for and receive a specific authorization to engage in the otherwise prohibited transaction. The purpose of specific authorizations is to allow BIS on a case-by-case basis to determine the nature and scope of the undue or unacceptable risk to U.S. national

security posed by transactions involving VCS hardware and covered software, including the extent of foreign adversary involvement in the transactions, as well as potential mitigations.

VCS hardware importers and connected vehicle manufacturers must not engage in an otherwise prohibited transaction until BIS grants the application for a specific authorization. If a party engages in a prohibited transaction prior to receiving a specific authorization from BIS, that transaction would constitute a violation of the regulation. Specific authorization requests will be reviewed on a case-by-case basis, and the time to reach a decision on an application for a specific authorization will vary based on the complexity of the case. However, 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.

Applications for a specific authorization must contain complete information on the proposed transaction, including every party involved, an overview of the covered software and/or the VCS hardware designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, the intended use of the covered software and/or VCS hardware, and documentation to support the information contained in the application. Persons seeking a specific authorization would submit an application via a web portal that would be available on the BIS website. Applicants should take care to submit to BIS only one copy of an application pertaining to each transaction for which they seek specific authorization to avoid processing delays. BIS may request additional information from an applicant about any matter related to the specific authorization request. In rare situations, as part of its review of an application for specific authorization, BIS may, in its sole discretion, request an oral briefing by the applicant and any other relevant parties. At any point between initial submission of an application for specific authorization and a final decision issued by BIS, an applicant may submit additional information to bolster the application or provide clarity on any aspect thereof.

When reviewing applications for a specific authorization, BIS will consider the factors that may pose undue or unacceptable risks, particularly as they relate to transactions that could result in the exfiltration of connected vehicle or U.S. persons' data, or the remote manipulation or operation of a connected vehicle. Examples of factors that BIS may consider include: the applicant's ability to limit PRC 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 or proposals the applicant offers to implement as a way to mitigate undue or unacceptable risk.

BIS's decision regarding any application for specific authorization will apply only to the specific parties and transaction outlined in the application and described in the decision notice. Additionally, the decision notice from BIS to the applicant(s) may contain any conditions that must be met by the parties for a transaction to be authorized. Such conditions, which are subject to revision by BIS, may include technical controls (e.g., software validation) or operational controls (e.g., physical and logical access monitoring procedures), that are either permanent or temporary. These controls will focus on the supply chain element that involves a link to a foreign adversary to mitigate any undue or unacceptable risk posed by the transaction. For connected vehicle manufacturers owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, a specific authorization may include a requirement that all VCS hardware and covered software be assembled and integrated into the connected vehicle in the United States. In the approval letter for specific authorization, BIS will determine the effective date and duration of the authorization on a case-by-case basis.

While applicants denied authorizations would not be precluded from submitting new applications for specific authorizations with regard to different transactions (involving different parties and/or different covered software or VCS hardware), BIS will reconsider a previously

denied application for a specific authorization only if the applicant demonstrates a material change in circumstances.

4. Exemptions

Transactions by VCS hardware importers and connected vehicle manufacturers would be exempt from the proposed prohibitions for a limited period. BIS proposes a shorter implementation period for transactions involving covered software and proposes a longer implementation period for transactions involving VCS hardware to allow market participants adequate time to establish alternative supply chains if necessary. This reflects BIS's understanding, and numerous public comments underscoring, that hardware supply chains for Connected Vehicles are complex and require multiple years to alter. VCS hardware importers would be permitted to engage in otherwise prohibited transactions involving VCS Hardware and would also be exempt from a requirement to submit a Declaration of Conformity for transactions not otherwise prohibited so long as: (1) for VCS hardware units not associated with a vehicle model year, the import of the VCS hardware takes place prior to January 1, 2029; or (2) the VCS hardware is integrated into a connected vehicle (completed or incomplete) or destined for a connected vehicle with a model year prior to 2030. Beginning January 1, 2029, any VCS hardware importer seeking to engage in a transaction subject to the VCS hardware prohibitions in § 791.302 (other than the import of a connected vehicle with a model year prior to 2030) would be required to obtain a specific authorization if the transaction is not otherwise permitted by a general authorization. Furthermore, VCS hardware importers seeking to import VCS hardware beginning on January 1, 2029, or VCS Hardware in completed connected vehicles or that is destined for connected vehicles starting with Model Year 203, would be required to submit an annual Declaration of Conformity to BIS, unless obligated to seek a Specific Authorization. Connected vehicle manufacturers would be permitted to engage in otherwise Prohibited Transactions involving covered software designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the

PRC or Russia, so long as the completed connected vehicle that is imported or sold is of a model year prior to 2027. Beginning Model Year 2027 (as imported into or sold in the United States), any connected vehicle manufacturer seeking to engage in a prohibited transaction involving covered software specified in section 791.303 would be required to obtain a specific authorization if the transaction is not otherwise permitted by a general authorization. Furthermore, connected vehicle manufacturers would be required to submit an applicable Declaration of Conformity for imports or Sales of all completed connected vehicles beginning in Model Year 2027.Connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia would be permitted to engage in otherwise prohibited transactions so long as the completed connected vehiclethat is Sold is of a Model Year prior to 2027. Beginning Model Year 2027 (as Sold in the United States), these particular connected vehicle manufacturers seeking to engage in a prohibited transaction specified in § 791.304 would be required to obtain a specific authorization if the transaction is not otherwise permitted by a general authorization.

5. Appeals

BIS proposes to create a mechanism by which any person whose application for a specific authorization is denied, whose specific authorization is suspended or revoked, or who has received a written notification of ineligibility for a general authorization may appeal that decision to the Under Secretary. Appeals must be submitted in writing by email or mail to the Office of the Under Secretary within 45 days of the date on the notice of the adverse administrative action by BIS. The appeal must detail how the party submitting the appeal has been directly and adversely affected by BIS's action, and the reasons that BIS's action should be reversed or otherwise modified. The Under Secretary, at his or her discretion, may delegate to the Deputy Under Secretary for Industry and Security or another BIS official the review of appeals, including arranging, at the official's discretion, informal hearings with relevant parties regarding the appeal.

Appellants may submit supplementary information in support of their appeal, whether sua sponte or at the request of the Under Secretary or the designated official, but, though the Under Secretary or designated official generally would not consider additional information submitted sua sponte more than 30 days after submission of the original appeal. If the Under Secretary or designated official requests supplementary information, appellants will have no more than 30 calendar days to respond to the request. Appellants may also request an in-person informal hearing in writing at the time of submission. A hearing is not required, and the Under Secretary or designated official may, at his or her discretion, grant or deny a request for an informal hearing.

6. Advisory Opinions

In response to public comments regarding the ANPRM, BIS proposes to include a mechanism for BIS to issue advisory opinions, similar to the process outlined in the Export Administration Regulations (EAR). BIS anticipates this process will provide connected vehicle manufacturers, VCS hardware importers, and other interested parties with greater clarity about how to comply with the proposed rule on an as-needed basis. As with the EAR, BIS emphasizes that advisory opinions provided under this proposed rule would in no way serve as evidence that the ICTS transaction addressed in the opinion is not subject to the jurisdiction of another U.S. Government agency. BIS may publish on its website an advisory opinion that may be of broad interest to the public, with redactions where necessary to protect Confidential Business Information. To solicit an advisory opinion from BIS, persons would be required to submit a written request to BIS by email or through a portal that will be available on the BIS website. BIS will not accept advisory opinion requests submitted by mail. A request for an advisory opinion must contain contact information for the submitter as well as all current information on the prospective transaction to assist BIS in making a determination. This would include technical details on the involved VCS hardware or covered software, information on the completed connected vehicle (if applicable), the SBOM and/or HBOM for the covered software and/or VCS

hardware, and any other supporting materials that the submitter assesses will assist BIS in determining if the transaction may be prohibited by this rule. Persons seeking an advisory opinion are encouraged to submit as much pertinent information as possible in the initial request for an advisory opinion, but BIS may request more information as needed to formulate its opinion. BIS will only consider advisory opinion requests for actual, not hypothetical, prospective transactions in which all parties, as opposed to anonymous parties, are identified. Additionally, parties may only rely on an advisory opinion when engaging in a transaction if the original Advisory Opinion request contained complete and accurate information and only so long as such information remains accurate following the issuance of the Advisory Opinion.

7. "Is-Informed" Notices

BIS could notify connected vehicle manufacturers or VCS hardware importers, either through direct letters or through a *Federal Register* notice meant to inform a broader set of persons, that a transaction involving certain covered software, VCS hardware, or entities requires a specific authorization because it would constitute a Prohibited Transaction according to the terms of this proposed rule. Any person who engages in a transaction covered by an "Is-Informed" notice without first receiving a Specific Authorization from BIS would have knowledge that such transaction is prohibited and would therefore be in violation of the rule. Is-Informed notices may only be delivered by or at the direction of the Under Secretary or a BIS employee designated by the Under Secretary.

8. Recordkeeping and Reporting Requirements

BIS proposes to require connected vehicle manufacturers and VCS hardware importers to maintain complete records related to any transaction for which a Declaration of Conformity, general authorization, or specific authorization would be required by this rule, for a period of ten years. This recordkeeping requirement applies regardless of whether the transaction is subject to a general authorization, specific authorization, or whether the connected vehicle manufacturer or VCS hardware importer has not yet sought an authorization. BIS would expect said records to

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, relevant correspondence, and all other files specified in sections 791.312 and 791.313 to assess compliance with the rule.

All 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 said transaction was carried out under a general authorization, specific authorization, or without an authorization from BIS. As such, BIS would be allowed to request business records, before, during, or after the transaction in question has taken place.

d. Enforcement

1. Penalties

IEEPA authorizes this rulemaking. Thus, persons who violate, attempt to violate, conspire to violate, or knowingly cause a violation of this rule, if finalized, may be subject to civil and/or criminal penalties under IEEPA (50 U.S.C. 1705), depending on the circumstances of the violation. Potential violations of this proposed rule that would be subject to penalties include engaging in a prohibited transaction without an applicable general authorization or specific authorization, or failure to abide by the conditions enumerated in a specific authorization. Willfully providing false or fictitious information to the U.S. Government may be subject to criminal fines, imprisonment, or both. A civil penalty may be imposed on any person who violates, attempts to violate, conspires to violate, or causes a violation of any authorization, order, regulation, or prohibition issued under IEEPA.

Under the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, the specific maximum civil penalty will be adjusted by notice in the *Federal Register* effective each calendar year by the Office of the Secretary of the Department of Commerce. At the time of

publishing of this proposed rule, the maximum civil penalty for violations of IEEPA is $368,136 per violation and the maximum criminal penalty is $1,000,000.

Under the proposed rule, should BIS have reason to believe that a violation has occurred and intends to issue a civil monetary penalty, it will inform the alleged violator through a written notice of the intent to impose a penalty ("Pre-Penalty Notice"). BIS will generally transmit the Pre-Penalty Notice electronically but may additionally issue a mailed notice. The recipient of a Pre-Penalty Notice may respond in writing to BIS to provide additional information or otherwise contest the penalty. BIS must receive this response within 30 days of the transmission of the original pre-penalty notice. A response to a pre-penalty notice does not constitute a formal appeal, but it allows the recipient of the pre-penalty notice to contest facts set forth by BIS in the pre-penalty notice, provide exculpatory evidence, or otherwise respond to the pre-penalty notice. BIS may seek to initiate settlement discussions in the pre-penalty notice or may conduct separate outreach following transmission of the pre-penalty notice. Recipients of a pre-penalty notice may additionally request to initiate settlement discussions in their response to BIS or may conduct separate outreach to do so.

Following the delivery of the pre-penalty notice and after considering any responses from the alleged violator, BIS will inform the alleged violator in writing as to whether it has found that a violation in fact occurred. Should BIS find that a violation has indeed taken place and no settlement has been reached, BIS will issue a final penalty notice to the violator specifying the violation and determining the specific civil monetary penalty to be imposed. This penalty may not be appealed following the procedures in section 791.309, but is a final agency action that the violator may contest in the appropriate U.S. District Court.

Should a violator fail to pay the penalty as specified in the final penalty notice or fail to make alternative payment arrangements approved by BIS, BIS may refer the matter to the Department of Treasury for administrative collection or to the Department of Justice for collection via civil suit in U.S. District Court.

2. Finding a Violation

Under the proposed rule, there may be cases in which BIS determines that a violation has taken place but that a civil monetary penalty is not appropriate. In such cases, BIS would issue a finding of violation that identifies the violation. The finding of violation could also contain an administrative response other than a civil monetary penalty, such as an order to cease and desist from conduct or activities that are prohibited by the proposed rule. Consistent with the procedures listed above regarding a pre-penalty notice, recipients of a finding of violation may file a response within 30 days contesting the facts of the finding of violation and/or providing information relevant to BIS's determination of whether a violation has occurred. BIS will consider any new information and inform the party in writing whether a violation has or has not occurred. A recipient that does not respond within 30 days of receipt of the finding of violation will be deemed to have waived the right to respond. any action taken in a finding of violation issued by BIS constitutes a final agency action that is not subject to appeal following the procedures in section 791.309.

3. Severability

BIS intends for the provisions of this proposed rule, as finalized to be severable from each other. If a court holds that any provision in a final 15 CFR part 791, subpart D, is invalid or unenforceable, BIS intends that the remaining provisions of a final 15 CFR part 791, subpart D, as relevant, would continue in effect to the greatest extent possible. In addition, if a court holds that any such provision is invalid or unenforceable as to a particular person or circumstance, BIS intends that the provision would remain in effect as to any other person or circumstance. Depending on the circumstances and the scope of the court's order, BIS believes that the remaining provisions of a final rule likely could continue to function sensibly independent of any provision or application held invalid or unenforceable. For example, the prohibitions related to transactions involving VCS Hardware could continue to apply as intended, even if a court finds that the prohibitions on transactions involving ADS are invalid. Similarly, the proposed rule

could be applied with respect to relevant hardware and software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC, even if a court finds its application with respect to relevant hardware and software from Russian-linked persons is invalid.

e. Classification

1. Executive Order 12866

Executive Order 12866, as reaffirmed by Executive Order 13563 and amended by Executive Order 14094, directs agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributed impacts, and equity). This proposed rule has been designated a significant regulatory action by the Office of Information and Regulatory Affairs (OIRA) under section 3(f)(1) of Executive Order 12866, as amended by Executive Order 14094.

2. Unfunded Mandates Reform Act of 1995

This proposed rule would not produce a federal mandate (under the regulatory provisions of title II of the Unfunded Mandates Reform Act of 1995) for state, local, and tribal governments or the private sector.

3. Executive Order 13132 (Federalism)

This proposed rule does not contain policies having federalism implications requiring preparations of a Federalism Summary Impact Statement.

4. Executive Order 12630 (Governmental Actions and Interference with Constitutionally Protected Property Rights)

This proposed rule does not contain policies that have takings implications.

5. Executive Order 13175 (Consultation and Coordination with Indian Tribes)

The Department has analyzed this proposed rule under Executive Order 13175 and has determined that the action would not have a substantial direct effect on one or more Indian tribes,

would not impose substantial direct compliance costs on Indian tribal governments, and would not preempt tribal law.

6. National Environmental Policy Act

The Department has reviewed this rulemaking action for the purposes of the National Environmental Policy Act (42 U.S.C. 4321, *et seq.*). It has been determined that this proposed rule would not have a significant impact on the quality of the human environment.

7. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3501, *et seq.*) (PRA) provides that an agency generally cannot conduct or sponsor a collection of information, and no person is required to respond nor be subject to a penalty for failure to comply with a collection of information subject to the requirements of the PRA, unless that collection has obtained OMB approval and displays a currently valid Office of Management and Budget (OMB) Control Number.

This proposed rule will create new information collection requirements, which are subject to review and approval by OMB under the PRA. Specifically, this proposed rule would require connected vehicle manufacturers and VCS hardware importers to submit annual Declarations of Conformity certifying that their import of VCS hardware and/or import or manufacture of completed connected vehicles does not involve hardware or software subject to the prohibitions in this proposed rule. Additional requirements for the Declarations of Conformity include supplying technical information regarding the hardware or software in question and providing a Bill of Materials for applicable software, hardware, or both.

Moreover, entities seeking specific authorizations from BIS to engage in otherwise prohibited transactions will have to file information with the Department, submissions of which are also subject to the PRA. Applications for a specific authorization would require, but are not limited to, a description of the nature of the otherwise prohibited transaction(s). For entities that are covered by a General Authorization, a self-certification, without need to notify BIS, would be

required (*see* Section VI of the NPRM). BIS proposes to require connected vehicle manufacturers and VCS hardware importers to maintain complete records related to any transaction for which a Declaration of Conformity, general authorization, or specific authorization would be required by this rule for a period of ten years, consistent with IEEPA's statute of limitations. These records would include any transaction for which the connected vehicle manufacturer or VCS hardware importer has not yet sought an authorization. BIS expects said records to include all information submitted in applications, as well as business records related to the execution of any ICTS transaction subject to the rule, such as contracts, import records, bills of sale, and all other files BIS may deem pertinent in assessing compliance with this proposed rule. Lastly, entities seeking an advisory opinion from BIS would have to file information with the Department, though this is an optional process for parties looking for additional clarity on proposed transactions. BIS anticipates that this collection would be largely similar to its program in administering 15 CFR 748.3, as it would require similar information and the process for submission is analogous. BIS seeks comment on how many entities would request an advisory opinion in order to better understand the associated costs.

BIS estimates that the initial burden placed on applicable entities would be 180 to 240 hours. This estimate takes into account the one-time initial cost (in hours) per entity to comply with the rule, including reading and understanding the rule's provisions. Every subsequent year, BIS anticipates that the total annual cost burden (in hours) for applicable entities to implement the rule would be 100 to 500 hours.

BIS assesses that there are 42 to 281 entities potentially impacted by the proposed rule and that the initial cost burden for these entities is between $30,964 and $38,554. This estimate takes into account the one-time initial cost per entity to comply with the rule, including reading and understanding the rule's provisions. Every subsequent year, BIS anticipates that the total annual cost burden for applicable entities to implement the rule will be $16,133 to $80,667 a year (average of operations manager, engineer, and lawyer hourly salaries in Table 2 [$484/hour / 3 =

$161.33] * [100 and 500 hours]). The annual cost burden placed on impacted entities includes (but is not limited to) producing the necessary HBOMs and SBOMs and documenting due diligence efforts. These hour and cost estimates are subject to variations among responsible entities due to application type. Declarations of Conformity will need to be submitted annually at minimum, while Specific Authorizations will need to be updated on an as-needed basis.

The estimated annual federal salary cost to the U.S. Government is $1,130,000 [500 Declaration of Conformity/Specific Authorization notifications per year * two staff at a GS-13 salary ($113/hour * 2 = $226/hour) * average of 10 hours each to review each notification]. The $113 per staff member per hour cost estimate for this information collection is consistent with the GS-scale salary data for a GS-13 Step 1 (*https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2024/DCB.pdf*) multiplied by a factor of 2 to include the cost of benefits and overhead.

The total estimated annual cost to the U.S. Government is $1,437,982.00. The calculation is as follows: Federal Employee Salaries (2 full-time employees) [$1,130,000.00] + Federal Government Overhead @ 20% [$226,000.00] + Legal Support (GS-15 Step 1 salary (multiplied by 2 to include the cost of benefits and overhead) @ 25%) [$81,982.00] = $1,437,982.00.

BIS requests comments on the information collection and recordkeeping requirements associated with this proposed rule. These comments will help BIS:

i. Evaluate whether the information collection is necessary for the proper performance of our agency's functions, including whether the information will have practical utility;

ii. Evaluate the accuracy of our estimate of the burden of the information collection, including the validity of the methodology and assumptions used;

iii. Enhance the quality, utility, and clarity of the information to be collected; and

iv. Minimize the burden of the information collection on those who are to respond (such as through the use of appropriate automated, electronic, mechanical, or other technological

collection techniques or other forms of information technology, e.g., permitting electronic submission of responses).

8. Regulatory Flexibility Act

In compliance with Section 603 of the Regulatory Flexibility Act (RFA), 5 U.S.C. 601–612, the Department has prepared an initial regulatory flexibility analysis (IRFA) for this proposed rule. The IRFA describes the economic impacts the proposed action may have on small entities. The Department seeks comments on all aspects of the IRFA.

1. *A description of the reasons why action by the agency is being considered.* Connected Vehicles contain a growing number of connected components. While these components provide greater safety and convenience through features like Wi-Fi, Bluetooth, cellular telecommunication, and satellite connectivity, the incorporation of progressively complex hardware and software systems enabling vehicle connectivity has also increased the attack surfaces through which malign actors may exploit vulnerabilities to gain access to a vehicle. ICTS integral to Connected Vehicles present an undue or unacceptable risk to U.S. national security when those systems are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. Furthermore, the PRC and Russia are able to leverage legal and regulatory regimes to compel private companies subject to their jurisdiction, including carmakers and vehicle suppliers, to cooperate with state security and intelligences services. Cooperation can include providing data, logical access, encryption keys, and other vital technical information, as well as by installing backdoors or bugs on equipment or in software updates, ultimately making vehicle equipment exploitable by foreign adversaries. Such privileged access potentially enables the PRC and Russia to exfiltrate sensitive data collected by Connected Vehicles through their components and allow remote manipulation for vehicles driven by U.S. persons.

2. *A succinct statement of the objectives of, and legal basis for, the proposed rule.* The Department is proposing this rule pursuant to authority under the International Emergency

Economic Powers Act (IEEPA) (50 U.S.C. 1701, *et seq.*), the National Emergencies Act (NEA) (50 U.S.C. 1601, *et seq*.), and Section 301 of Title 3, United States Code, and in accordance with E.O. 13873, "Securing the Information and Communications Technology and Services Supply Chain," 84 FR 22689 (May 17, 2019), which delegated to the Secretary of Commerce (Secretary) certain authorities provided to the President by IEEPA, the NEA, and Section 301 of Title 3 of the United States Code. In accordance with the National Emergencies Act, the President has declared each year since E.O. 13873 was published that the national emergency declared in E.O. 13873 regarding the ICTS supply chain continues to remain in effect.

To address identified risks to national security from ICTS transactions, E.O. 13873 directs the Secretary (in consultation with other agency heads identified in E.O. 13873) to review any ICTS transaction, defined as any acquisition, importation, transfer, installation, dealing in, or use of any ICTS by any person, or with respect to any property, subject to United States jurisdiction, where the transaction involves any property in which a foreign country or national has any interest. When the Secretary, in consultation with the appropriate agency heads, finds that an ICTS transaction or class of ICTS transactions pose undue risks (including of sabotage, subversion, or catastrophic effects on the security and resiliency of U.S. critical infrastructure), or unacceptable risks to national security or the security and safety of U.S. persons, the Secretary may identify the ICTS transaction as prohibited by Section 1 of E.O. 13873 or impose mitigation measures on the ICTS transaction or class of ICTS transactions reviewed. E.O. 13873 additionally provides that the Secretary issue rules establishing criteria by which particular technologies or market participants may be categorically included in or categorically excluded from prohibitions established pursuant to the E.O.

3. *A description of and, where feasible, an estimate of the number of small entities to which the proposed rule will apply.* BIS anticipates that the entities primarily responsible for compliance with this regulation will be connected vehicle manufacturers and VCS hardware importers. BIS assesses, based on publicly available information, that the U.S. connected vehicle

market is dominated by a small set of manufacturers, few of which would be considered "small entities" under the Small Business Administration's definitions. The Small Business Administration small business size standard for NAICS 336110: Automobile and Light Duty Motor Vehicle Manufacturing and NAICS 336120: Heavy Duty Truck Manufacturing is 1,500 employees or fewer. However, BIS has limited data on how many of these suppliers engage in covered software and VCS hardware transactions, and therefore cannot estimate how many of these suppliers qualify as small entities. BIS specifically seeks comments on the number of suppliers engaged in covered software and VCS Hardware transactions in the United States, as well as the percentage of those entities that might or could qualify as small entities.

4. *A description of the projected reporting, recordkeeping, and other compliance requirements of the proposed rule, including an estimate of the classes of small entities that will be subject to the requirement and the type of professional skills necessary for preparation of the report or record.* As stated above, connected vehicle manufacturers and VCS hardware importers will bear the majority of the proposed rule's compliance costs. BIS estimates that the recordkeeping and compliance burden placed on responsible small entities would involve operations managers, engineers, and lawyers. On an annual basis, these entities will need to, at minimum and if applicable, submit a Declaration of Conformity certifying that their import of VCS hardware and/or import or manufacture of completed connected vehicles does not involve hardware or software subject to the prohibitions in this proposed rule. The Declaration of Conformity would also include technical information regarding the hardware or software in question and a Bill of Materials for applicable software, hardware, or both.

BIS proposes to require connected vehicle manufacturers and VCS hardware importers to maintain complete records related to any transaction for which a Declaration of Conformity, general authorization, or specific authorization would be required by this rule, for a period of ten years, consistent with IEEPA's statute of limitations. These records would be expected to assist BIS's enforcement efforts for the prohibitions in the proposed rule. The required records would

include those related to any transaction that is subject to a general authorization (including records of any entities producing fewer than 1,000 connected vehicle or VCS hardware units in a calendar year), any transaction that is subject to a specific authorization, and any transaction involving covered software or VCS Hardware for which the connected vehicle manufacturer or VCS hardware importer has not yet sought an authorization. BIS expects such records to include all information submitted in applications, as well as business records related to the execution of any ICTS transaction subject to the rule, such as contracts, import records, bills of sale, and all other files BIS may deem pertinent in assessing compliance with this proposed rule.

Because small entities could avail themselves of a general authorization, the maintenance of records in support of such authorization would be the only compliance requirement. These records would serve as the small entities' self-certification, which does not need to be submitted to BIS. A general authorization would allow the VCS hardware importer and/or connected vehicle manufacturer to engage in the otherwise prohibited transaction, without the need to notify or seek approval from BIS. General Authorizations would be available only in a narrow set of circumstances in which the conditions of the otherwise prohibited transaction appropriately mitigate the level of risk associated with the particular transaction. Such conditions would include, for example, when VCS hardware is imported from the PRC or Russia solely for testing purposes, or where the completed connected vehicle that incorporates VCS hardware or covered software from the PRC or Russia will not be driven on public roads for more than 30 calendar days per year. Those availing themselves of a general authorization would be required to continuously monitor their use of the VCS hardware or completed connected vehicles covered by the general authorization to ensure the authorization still applies. If a change would render the transaction ineligible for a general authorization, such as a change in the vehicle's use, the VCS hardware importer or connected vehicle manufacturer would be required to apply for a specific authorization and to cease engaging in such transaction unless and until a specific authorization is granted. For example, if a completed connected vehicle that incorporates covered software or

VCS Hardware that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia is no longer engaged in display, research, or testing, the VCS hardware importer or the connected vehicle manufacturer would be required to seek a specific authorization. Similarly, if the VCS Hardware Importer or connected vehicle manufacturer exceeds total model year production of 1,000 units, or if a completed connected vehicle that incorporates covered software or VCS hardware that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia is to be used on public roadways for 30 or more days in any calendar year, the VCS hardware importer or connected vehicle manufacturer would be required to seek a specific authorization from BIS.

5. *An identification, to the extent practicable, of all relevant Federal rules that may duplicate, overlap, or conflict with the proposed rule.* This rulemaking does not duplicate or conflict with any Federal rules.

6. *A description of any significant alternatives to the proposed rule that accomplish the stated objectives of Executive Order 13984 and Executive Order 14110 and applicable statutes and that would minimize any significant economic impact of the proposed rule on small entities.* The Department has proposed what it believes to be "the least restrictive means necessary [by] tailor[ing] the prohibition to address the undue or unacceptable risk" (*see* 15 CFR part 791.109(c)) and believes that the proposed rule will materially address significant risks for the United States or U.S. persons while balancing the overall compliance costs of the rule and minimizing the impact on small entities. Below is a description of alternatives considered by the Department; the Department invites comment on these alternatives.

No-action alternative: While the alternative of taking no action would be less costly for connected vehicle manufacturers and VCS hardware importers, the no-action alternative is not preferred because the risks presented by foreign adversary involvement in the ICTS of the U.S.

connected vehicle market could lead to catastrophic negative events for U.S. national security, including the security of U.S. critical infrastructure, and U.S. persons.

More stringent alternatives: The Department considered several more stringent regulatory approaches, including regulating additional connected vehicle component systems not included in this proposed rule. For example, the Department considered the risks posed by various connected vehicle component systems, including ADS, telematics, battery management systems (BMS), automated driver assistance systems (ADAS), vehicle operating systems (OS), and satellite or cellular telecommunication systems. The Department currently believes the best approach to address the risks posed by connected vehicles and connected vehicle components from foreign adversary nations is to focus the scope of the NPRM on PRC- and Russian-supplied VCS hardware (which encompasses both telematics and satellite or cellular telecommunication systems) and covered software. Other systems under consideration, such as ADAS, seem to have a low risk of data exfiltration or, in the case of vehicle OS, would involve regulation that is expected to be extremely burdensome on industry.

Preferred alternative: The proposed rule is the preferred alternative. BIS assesses that the regulatory approach outlined in this proposed rule would have the highest net benefit for connected vehicle manufacturers, VCS hardware importers, and consumers. BIS currently believes the provisions in the proposed rule are also to be, for the reasons articulated above and in the NPRM's preamble, "the least restrictive means necessary…to address the undue or unacceptable risk" presented by covered software and VCS hardware in connected vehicles.

List of Subjects in 15 CFR part 791

Business and industry, Communications, Computer technology, Critical infrastructure, Executive orders, Foreign Persons, Investigations, National security, Penalties, Technology, Telecommunications

Elizabeth L.D. Cannon,
Executive Director,

Office of Information and Communications Technology and Services,
Bureau of Industry and Security, United States Department of Commerce

For the reasons set out in the preamble, 15 CFR part 791, is proposed to be amended as follows:

15 CFR PART 791 - SECURING THE INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES SUPPLY CHAIN

1. The authority citation for part 791 continues to read as follows:

Authority: 50 U.S.C. 1701 *et seq.*; 50 U.S.C. 1601 *et seq.*; E.O. 13873, 84 FR 22689; E.O. 14034, 86 FR 31423.

2. Amend part 791 by adding subpart D, consisting of § 791.300 through § 791.319, to read as follows:

Subpart D — ICTS Supply Chain: Connected Vehicles

Sec.

§ 791.300 Purpose and scope.

The inclusion in Connected Vehicles of certain ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of certain

foreign adversaries poses undue or unacceptable risks to U.S. national security. To address these undue or unacceptable risks, it is the purpose of this subpart to:

(a) Prohibit ICTS transactions that involve certain software and hardware that, are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the People's Republic of China (PRC) or the Russian Federation (Russia), as defined in § 791.4 and that enable connected vehicle Automated Driving Systems or Vehicle Connectivity Systems, as defined in this subpart;

(b) Implement compliance mechanisms such as Declarations of Conformity to ensure that no Prohibited Transactions, as defined in this subpart, have occurred;

(c) Provide general authorizations and a mechanism for specific authorizations for certain transactions that are otherwise prohibited by this subpart, but where any undue or unacceptable risks to national security can be reasonably mitigated, based on defined criteria and conditions; and

(d) Incentivize connected vehicle manufacturers, VCS hardware importers, and related suppliers to adopt measures to help secure the U.S. ICTS supply chain for connected vehicles.

§ 791.301 Definitions.

The following definitions apply only to this subpart, 15 CFR part 791 subpart D. For additional definitions applicable to all of part 791, *see* 15 CFR 791.2. If a term is defined differently in this subpart than in 15 CFR 791.2, the definition listed in this section will apply to this subpart.

Automated Driving System means 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).

Completed connected vehicle means a connected vehicle that requires no further manufacturing operations to perform its intended function. For the purposes of this subpart, the

integration of an Automated Driving System into a connected vehicle constitutes a manufacturing operation for a completed connected vehicle.

Connected vehicle means 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. Vehicles operated only on a rail line are not included in this definition.

Connected vehicle manufacturer means 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.

Covered software means the software-based components, in which there is a foreign interest, executed by the primary processing unit of the respective systems that are part of an item that supports the function of Vehicle Connectivity Systems or Automated Driving Systems at the vehicle level. Covered software does not include firmware, which is characterized as software specifically programmed for a hardware device with a primary purpose of controlling, configuring, and communicating with that hardware device. Covered software also does not include open-source software that can be freely used, modified, and distributed by anyone, with both access to the source code and the ability to contribute to the software's development and improvement unless that open-source software has been modified for proprietary purposes and not redistributed or shared.

FCC ID Number means the unique alphanumeric code identifying a product subject to certification by the Federal Communications Commission composed of a:

(1) Grantee code; and

(2) Product code.

Foreign interest, for purposes of this subpart, means any interest in property of any nature whatsoever, whether direct or indirect, by a non-U.S. person.

Hardware Bill of Materials (HBOM) means 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.

Import means, in the context of this subpart, with respect to any article, the entry of such article into the United States Customs Territory. It does not include admission of an article from outside the United States into a foreign-trade zone for storage pending further assembly in the foreign-trade zone or shipment to a foreign country.

Item means a component or set of components with a specific function at the vehicle level. A system may also be considered an item if it implements a function.

Knowingly means 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.

Model year means the year used to designate a discrete vehicle model, irrespective of the calendar year in which the vehicle was actually produced, provided that the production period does not exceed 24 months.

Prohibited transactions mean, collectively, the transactions described in 791.302 (Prohibited VCS Hardware Transactions), 791.303 (Prohibited Covered Software Transactions), or 791.304 (Related Prohibited Transactions) of this subpart.

Person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary means:

(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 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, as those terms are defined in 49 U.S.C. 30102. This definition also applies to the related terms such as *Sell* or *Selling*.

Software Bill of Materials (SBOM) means 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.

Vehicle Connectivity System (VCS) means 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.

VCS hardware means the following software-enabled or programmable components and subcomponents that support the function of Vehicle Connectivity Systems or are part of an item that supports the function of Vehicle Connectivity Systems: 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).

VCS hardware importer means 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.

United States means the United States of America, the States of the United States, the District of Columbia, and any commonwealth, territory, dependency, or possession of the United States, or any subdivision thereof, and the territorial sea of the United States.

§ 791.302 Prohibited VCS hardware transactions.

(a) VCS hardware importers are prohibited from knowingly importing VCS hardware that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

(b) In the context of this subpart, VCS hardware will not be considered to be designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC 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 the VCS hardware.

§ 791.303 Prohibited covered software transactions.

(a) Connected vehicle manufacturers are prohibited from knowingly importing into the United States completed connected vehicles that incorporate covered software, designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

(b) Connected vehicle manufacturers are prohibited from knowingly selling in the United States completed connected vehicles that incorporate covered software, designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

(c) In the context of this subpart, covered software will not be considered to be designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC 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 the Covered Software.

§ 791.304 Related prohibited transactions.

Connected vehicle manufacturers who are persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, are prohibited from knowingly selling in the United States completed connected vehicles that incorporate VCS hardware or covered software.

§ 791.305 Declaration of Conformity.

(a) *Requirements*--(1) *Import of VCS hardware:* A VCS hardware importer may not import VCS Hardware as part of a transaction that is not otherwise prohibited by this subpart without

first submitting to the Bureau of Industry and Security (BIS) a Declaration of Conformity, unless otherwise specified by this subpart. The Declaration of Conformity shall include:

(i) The name and address of VCS hardware importer;

(ii) A certification that the declarant has not knowingly engaged in a prohibited VCS hardware transaction;

(iii) The FCC ID Number associated with the VCS hardware and, if applicable, of the subcomponents contained therein;

(iv) A list of third-party external endpoints to which the VCS hardware connects, including the country where each endpoint is located and/or the identity and location of the service provider;

(v) If known, the make, model, and trim of the completed connected vehicles for which the VCS hardware is intended;

(vi) A HBOM for the VCS hardware that is the subject of the Declaration of Conformity;

(vii) Documentation of the VCS hardware importer's due diligence efforts, to include independent or hired third-party research, to ensure the VCS hardware listed in the HBOM is not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia;

(viii) If applicable, an indication of whether the submission is an update to a prior Declaration of Conformity and the date of the last submission;

(ix) Identifying information for an individual point of contact (including name, email address, and phone number); and,

(x) Any additional material information the VCS hardware importer would like to submit.

(2) *Import of completed connected vehicles:* A connected vehicle manufacturer may not import completed connected vehicles containing covered software as part of a transaction that is not otherwise prohibited by this subpart without first submitting to BIS a Declaration of

Conformity, unless otherwise specified by this subpart. The Declaration of Conformity shall include:

(i) The name and address of the connected vehicle manufacturer;

(ii) A certification that the declarant has not knowingly engaged in a prohibited covered software transaction;

(iii) The make, model, trim, and Vehicle Identification Number (VIN) series applicable to the completed connected vehicles;

(iv) A SBOM for the covered software that is the subject of the Declaration of Conformity. At a minimum, the SBOM must include author's name, timestamp, supplier name, component name, version string, component hash, package URL, unique identifier, and dependency relationships to other software components.

(v) Documentation of the connected vehicle manufacturer's due diligence efforts, to include independent or hired third-party research, to ensure that the covered software listed in the SBOM is not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia;

(vi) If applicable, an indication of whether the submission is an update to a prior Declaration of Conformity and the date of the last submission;

(vii) Identifying information for an individual point of contact (including name, email address, and phone number); and

(viii) Any additional material information the connected vehicle manufacturer would like to submit.

(3) *Sale of completed connected vehicles manufactured in the United States*: Connected vehicle manufacturers that manufacture or assemble completed connected vehicles in the United States that incorporate covered software as part of a transaction that is not otherwise prohibited by this subpart, may not Sell completed connected vehicles in the United States without first submitting to BIS a Declaration of Conformity, unless otherwise specified by this subpart. If

there is no Foreign Interest in the covered software that is incorporated in completed connected vehicles manufactured or assembled in the United States, the connected vehicle manufacturer need not submit a Declaration of Conformity. If submitting a Declaration of Conformity, it shall include:

(i) The name and address of the connected vehicle manufacturer;

(ii) A certification that there is a foreign interest in the covered software that is incorporated in the completed connected vehicles that will be Sold in the United States;

(iii) A certification that the declarant has not knowingly engaged in a prohibited covered software Transaction;

(iv) The make, model, trim, and VIN series applicable to the completed connected vehicles;

(v) A SBOM for the covered software that is the subject of the Declaration of Conformity. At a minimum, the SBOM must include author's name, timestamp, supplier name, component name, version string, component hash, package URL, unique identifier, and dependency relationships to other software components.

(vi) Documentation of the connected vehicle manufacturer's due diligence efforts, to include independent or hired third-party research, to ensure the covered software listed in the SBOM is not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia;

(vii) If applicable, an indication of whether the submission is an update to a prior Declaration of Conformity and the date of the last submission;

(viii) Identifying information for an individual point of contact (including name, email address, and phone number); and

(ix) Any additional material information the connected vehicle manufacturer would like to submit.

(b) *Procedures to submit Declarations of Conformity.* connected vehicle manufacturers and VCS Hardware Importers shall submit Declarations of Conformity annually as specified in this

section and any time there is a material change that makes a prior Declaration of Conformity or associated HBOM or SBOM no longer accurate.

(1) Connected Vehicles Manufacturers seeking to import or manufacture for Sale in the United States a completed connected vehicle containing covered software shall submit a Declaration of Conformity 60 days prior to the first import or first sale of each model year of completed connected vehicles, grouped by make, model, and trim.

(2) VCS hardware importers seeking to import any VCS hardware shall submit a Declaration of Conformity 60 days prior to the first import of VCS hardware for each model year for units associated with a vehicle model year, or calendar year for units not associated with a vehicle model year. VCS hardware importers may submit a single Declaration of Conformity detailing all VCS Hardware models that will be imported in the Model Year or calendar year.

(3) Entities that are both connected vehicle manufacturers and VCS hardware importers may, but are not required to, submit a single compiled Declaration of Conformity detailing all required information specified in 791.305 of this subpart. Any compiled Declaration of Conformity shall be submitted 60 days prior to the first import or first sale of the model year of completed connected vehicles or 60 days prior to the first import of VCS hardware, whichever occurs first.

(4) Declarants must notify BIS of any material change in the contents of a previously submitted Declaration of Conformity by submitting a revised Declaration of Conformity within 30 days following any such changes.

(c) Declarations of Conformity must be delivered to BIS using an official electronic reporting option as specified by BIS on its website (https://www.bis.gov).

(d) *Connected vehicle introduced by means of a fraudulent or false declaration.* Any person who engages in a prohibited VCS hardware transaction or a prohibited covered software transaction and submits a false or fraudulent Declaration of Conformity made without reasonable cause to believe the truth of the declaration, may incur penalties as defined in § 791.314.

§ 791.306 General authorizations.

(a) VCS hardware importers and connected vehicle manufacturers may qualify for a general authorization if they meet the stated requirements or conditions to engage in otherwise prohibited transactions. Persons availing themselves of any general authorization are required to maintain records documenting each otherwise prohibited transaction for a period of 10 years as specified in § 791.312.

(b) *General course of procedure.* VCS hardware importers and connected vehicle manufacturers may self-certify, without need to notify BIS, that they meet the requirements for one or more of the following general authorizations:

(1) The connected vehicle manufacturer or VCS hardware importer and entities under common control, including parents, engaging in an otherwise prohibited transaction produces a total model year production of completed connected vehicles containing covered software or total model year production of VCS hardware is less than 1,000 units;

(2) The completed connected vehicle that incorporates covered software or VCS hardware will be used on public roadways on fewer than 30 calendar days in any calendar year;

(3) The completed connected vehicle that incorporates covered software or the VCS hardware will be used solely for the purpose of display, testing, or research, and will not be used on public roadways; or

(4) The completed connected vehicle that incorporates covered software or the VCS hardware 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;

(c) *Change in use*. In the event of any change in the use of a completed connected vehicle or VCS hardware associated with a general authorization, a VCS hardware importer or connected vehicle manufacturer availing itself of a general authorization must determine if it still qualifies for the general authorization or if it must apply for a specific authorization.

(d) *Inspection.* VCS hardware importers and connected vehicle manufacturers availing themselves of a general authorization are subject to audit and inspection by BIS.

(e) *Restrictions.* VCS Hardware importers and connected vehicle manufacturers shall not avail themselves of any general authorization if any one or more of the following apply:

(1) BIS has notified the VCS hardware importer or connected vehicle manufacturer that it is not eligible for a general authorization.

(2) The VCS Hardware Importer or connected vehicle manufacturer is a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

§ 791.307 Specific authorizations.

(a) BIS may provide Specific Authorizations permitting a VCS hardware importer or connected vehicle manufacturer to engage in otherwise prohibited transactions. Persons receiving a specific authorization are required to maintain records for a period of 10 years as required in § 791.312 and submit reports and statements in accordance with the instructions specified in each specific authorization.

(b) *General course of procedure*. Prohibited transactions subject to this subpart, and that are not otherwise permitted under an exemption or a general authorization, may be permitted under a specific authorization. It is the policy of BIS not to grant applications for specific authorizations for transactions that are permitted by a general authorization.

(c) *Applications for specific authorizations.* Applications for specific authorizations shall include, at a minimum, a description of the nature of the otherwise prohibited transaction(s), including the following:

(1) The identity of the parties engaged in the transaction, including relevant corporate identifiers and information sufficient to identify the ultimate beneficial ownership of the transacting parties;

(2) An overview of the VCS hardware or covered software that is designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia;

(3) If known, the make, model, and trim of the completed connected vehicle in which the VCS hardware or covered software will be integrated;

(4) The intended function of the VCS hardware or covered software;

(5) Documentation to support the information contained in the application, including ISO/SAE 21434 Threat Analysis and Risk Assessments, to include an assessment on the applicant's ability to limit PRC 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 with respect to the VCS hardware or covered software; other actions and proposals such as technical controls (i.e., software validation) or operational controls (i.e., physical and logical access monitoring procedures), the applicant intends to take to mitigate undue or unacceptable risk; and

(6) Any other information that BIS may request after receipt of the initial application for a Specific Authorization.

(d) *Application submission procedures.* A VCS hardware importer or connected vehicle manufacturer who seeks to engage in an otherwise prohibited transaction must submit an application for specific authorization in writing prior to engaging in the transaction and await a decision from BIS prior to engaging in the transaction. This application must be delivered to BIS using an official electronic reporting option as specified by BIS on its website (https://www.bis.gov).

(e) *Additional conditions.* Only one application for a specific authorization should be submitted to BIS for each otherwise prohibited transaction; multiple parties submitting an application for a specific authorization for the same transaction may result in processing delays.

(f) *Information to be supplied*. An applicant may be required to furnish additional information as BIS deems necessary to assist in making a decision. The applicant may present additional information concerning an application for a specific authorization at any time before BIS makes its decision with respect to the application.

(g) *Review and decisions.* Applications for specific authorization will be reviewed on a case-by-case basis and 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. Such review may include an evaluation of the 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 foreign adversary involvement in the design, development, manufacture, or supply of the VCS hardware or covered software; the applicant's ability to limit PRC 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; other actions and proposals the applicant intends to take to mitigate undue or unacceptable risk. BIS will advise each applicant of the decision respecting the filed application.

(h) *Processing period.* BIS shall respond to any application for a specific authorization with a status update and a request for additional information or documents, if any, within 90 days after receipt of the application.

(i) *Scope.* (1) Unless otherwise specified in the authorization, a specific authorization permits the transaction only:

(i) Between the parties identified in the specific authorization;

(ii) With respect to the otherwise prohibited transaction(s) described in the authorization; and

(iii) If the conditions specified in the specific authorization are satisfied. The applicant must inform any other parties identified in the specific authorization of the authorization's scope and specific conditions.

(2) Any specific authorization obtained based on a false or misleading representation in the application or in any document submitted in connection with the application under this section

shall be deemed void as of the date of issuance, and the applicant may incur penalties as specified in § 791.314.

(3) As a condition for the issuance of any specific authorization, the applicant may be required to file reports with respect to the otherwise prohibited transactions authorized by the specific authorization in such form and at such times and places as may be prescribed in the specific authorization or otherwise communicated to the applicant by BIS. Reports should be sent in accordance with the instructions provided in the applicable specific authorization.

(j) *Effect of denial.* BIS's denial of a specific authorization may be appealed as described in § 791.309 and does not preclude parties from filing an application for a specific authorization for a separate otherwise prohibited transaction. The applicant may at any time request, by written correspondence, reconsideration of the denial of an application based on new material facts or changed circumstances.

(k) *Effect of specific authorization.* (1) No specific authorization issued under this subpart, or otherwise issued by BIS, permits or validates any prohibited transaction effected prior to the issuance of such specific authorization unless specifically provided for in the specific authorization.

(2) No regulation, ruling, instruction, or authorization permits any prohibited transaction under this subpart unless the regulation, ruling, instruction or Authorization is issued by BIS and specifically refers to this subpart. No regulation, ruling, instruction, or authorization referring to this subpart shall be deemed to permit any prohibited transaction prohibited by any provision of this subpart unless the regulation, ruling, instruction, or authorization specifically refers to such provision. Any specific authorization permitting any otherwise prohibited transaction has the effect of removing those prohibitions from the transaction, but only to the extent specifically stated by the terms of the specific authorization. Unless the specific authorization otherwise specifies, such an authorization does not create any right, duty, obligation, claim, or interest in, or with respect to, any property that would not otherwise exist under ordinary principles of law.

(3) Nothing contained in this subpart shall be construed to supersede the requirements established under any other provision of law or to relieve a person from any requirement to obtain an authorization from another department or agency of the U.S. Government in compliance with applicable laws and regulations subject to the jurisdiction of that department or agency.

(l) *Amendment, modification, or rescission.* Except as otherwise provided by law, any Specific Authorization or instructions issued thereunder may be amended, modified, or rescinded by BIS at any time.

§ 791.308 Exemptions.

(a) VCS hardware importers may engage in prohibited transactions described in § 791.302 without an authorization as required under §§ 791.306 and 791.307, and are exempt from submitting Declarations of Conformity with respect to all other transactions, as described in § 791.305 provided that:

(1) For VCS Hardware units not associated with a vehicle model year, the import of the VCS hardware occurs prior to January 1, 2029; or

(2) The VCS hardware is associated with a vehicle model year prior to 2030 or the VCS hardware is imported as part of a connected vehicle with a model year prior to 2030.

(b) Connected vehicle manufacturers may engage in prohibited transactions described in § 791.303 without authorization as required under §§ 791.306 or 791.307 and are exempt from submitting Declarations of Conformity with respect to all other transactions, as described in § 791.305, provided that the completed connected vehicle that incorporates covered software described in § 791.303(a)(1) was manufactured prior to Model Year 2027.

(c) Connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia may engage in prohibited transactions described in section 791.304 without Authorization as required under §§ 791.306 or 791.307, and are exempt from submitting Declarations of Conformity to all other transactions, provided that the

completed connected vehicle that incorporates VCS hardware and/or covered software was manufactured prior to Model Year 2027.

§ 791.309 Appeals.

(a) *Scope.* Any person directly and adversely affected by any of the listed administrative actions taken by BIS pursuant to this subpart may appeal to the Under Secretary for reconsideration of that administrative action. Only the following types of administrative actions are subject to the appeals procedures described in this subpart:

(1) Denial of an application for specific authorization;

(2) Suspension or revocation of an issued specific authorization; or

(3) Determination of ineligibility for a general authorization.

(b) *Designated appeals reviewer and coordinator.* The Under Secretary may delegate to the Deputy Under Secretary of Commerce for Industry and Security or to another BIS official the authority to review and decide the appeal, and to exercise any other function of the Under Secretary under this section. In addition, the Under Secretary may designate any employee of BIS to be an appeals coordinator to assist in the review and processing of an appeal under this subpart.

(c) *Appeals procedures*. An appeal under this subpart must be submitted to the Under Secretary by email or at the following address: Bureau of Industry and Security, U.S. Department of Commerce, Room 3898, 14th Street and Pennsylvania Avenue, N.W. Washington, DC 20230 not later than 45 days after the date appearing on the written notice of administrative action. The appeal must include a full written statement in support of the appellant's position. The appeal must include a precise statement of the reasons that the appellant believes that the administrative action has a direct and adverse effect and should be reversed or modified. The Under Secretary or the designated official may request additional information that would be helpful in resolving the appeal and may accept additional submissions. The Under

Secretary or the designated official will not ordinarily accept any submission filed sua sponte more than 30 days after the filing of the appeal.

(d) *Request for informal hearing.* In addition to the written statement submitted in support of an appeal, an appellant may request, in writing, at the time an appeal is filed, an opportunity for an informal hearing. A hearing is not required, and the Under Secretary or the designated official may grant or deny a request for an informal hearing at the Under Secretary or the designated official's sole discretion. Any hearings will be held in the District of Columbia unless the Under Secretary or the designated official determines, based upon good cause shown, that another location would be preferable.

(e) *Informal hearing procedures.* If a hearing request is granted, the Under Secretary or the designated official may provide an opportunity for the appellant to make an oral presentation at an informal hearing based on the materials previously submitted by the appellant or made available by the Department. The Under Secretary or the designated official may require that any facts in controversy be covered by an affidavit or testimony given under oath or affirmation. The rules of evidence prevailing in courts of law do not apply, and all evidentiary material deemed by the Under Secretary or the designated official to be relevant and material to the proceeding, and not unduly repetitious, will be received and considered. The Under Secretary or the designated official has the authority to limit the number of people attending the hearing, to impose any time or other limitations deemed reasonable, and to determine all procedural questions. A transcript of an informal hearing shall not be made, unless the Under Secretary or the designated official determines that the national interest or other good cause warrants it, or the appellant requests a transcript. If the appellant requests, and the Under Secretary or the designated official approves the taking of, a transcript, the appellant will be responsible for paying all expenses related to production of the transcript. Any person designated by the Under Secretary to conduct an informal hearing shall submit a written report containing a summary of the hearing and recommended action to the Under Secretary.

(f) *Decisions.* In addition to the documents specifically submitted in connection with the appeal, the Under Secretary or the designated official may consider any recommendations, reports, or other relevant documents available to BIS in determining the appeal, but shall not be bound by any such information, nor prevented from considering any other relevant information, or consulting with any other person or groups, in making a decision. The Under Secretary or the designated official may adopt any other procedures deemed necessary and reasonable for considering an appeal, including by providing the appellant with an interim or proposed decision and offering the appellant an opportunity to provide comments. The Under Secretary or the designated official shall decide an appeal within a reasonable time after receipt of the appeal. The decision shall be issued to the appellant in writing and contain a statement of the reasons for the action and address any arguments contrary to the decision presented by the appellant. The decision of the Under Secretary or the designated official shall be final.

(g) *Effect of appeal.* Acceptance and consideration of an appeal shall not affect any administrative action, pending or in effect, unless the Under Secretary or the designated official, upon request by the appellant and with opportunity for a response, grants a stay.

§ 791.310 Advisory opinions.

(a) VCS hardware importers and connected vehicle manufacturers may request an advisory opinion from BIS as to whether a prospective transaction is subject to a prohibition in this subpart. The entire transaction that is the subject of the advisory opinion request must be an actual, as opposed to hypothetical, transaction and involve disclosed, as opposed to anonymous, parties to the transaction.

(b) Advisory opinion requests must be made in writing, and may be delivered to BIS by email, through the BIS website, or by any other means that BIS may prescribe.

(c) Persons submitting advisory opinion requests are encouraged to provide as much information as possible to assist BIS in making a determination, to include the following information:

(1) The name, title, and telephone and email address of the person to contact;

(2) The submitter's complete address comprised of street address, city, state, country, and postal code;

(3) All available information identifying the parties to the prospective transaction;

(4) Complete information regarding the VCS hardware and/or covered software and any descriptive literature, brochures, technical specifications, or papers that provide sufficient technical detail to enable BIS to verify whether the prospective transaction would constitute a prohibited transaction as defined in this subpart;

(5) For connected vehicle manufacturers: the make, model, and trim level, or other identifying information number of the completed connected vehicle;

(6) For VCS hardware Importers: the identification of the system; and, if known, the make, model, and trim of the group of completed connected vehicles for which the equipment is intended;

(7) An SBOM and/or an HBOM; and

(8) Any other information that the submitter believes to be material to the prospective transaction.

(d) Each person that submits an advisory opinion request shall provide any additional information or documents that BIS may thereafter request in its review of the matter.

(e) Each advisory opinion can be relied upon by the requesting party or parties to the extent the disclosures made pursuant to this subpart were accurate and complete and to the extent the disclosures continue accurately and completely to reflect circumstances after the date of the issuance of the advisory opinion. An advisory opinion will not restrict enforcement actions by any agency other than BIS. It will not affect a requesting party's obligations to any other agency or under any statutory or regulatory provision other than those specifically discussed in the Advisory Opinion.

(f) BIS may publish on its website an advisory opinion that may be of broad interest to the public, with redactions where necessary to protect confidential business information.

§ 791.311 "Is-Informed" notices.

(a) BIS may inform VCS hardware importers or connected vehicle manufacturers either individually by specific notice or, for larger groups, through a separate notice published in the *Federal Register*, that a specific authorization is required because an activity could constitute a prohibited transaction.

(b) Specific notice that a specific authorization is required may be given only by, or at the direction of, the Under Secretary or a BIS official designated by the Under Secretary.

§ 791.312 Recordkeeping.

Except as otherwise provided, VCS hardware importers and connected vehicle manufacturers shall keep a full and accurate record of each transaction engaged in for which a Declaration of Conformity, general authorization, or specific authorization would be required under sections 791.305, 791.306, or 791.307, regardless of whether these transactions are effected pursuant to a general authorization, specific authorization, or otherwise, and such record shall be available for examination for at least 10 years after the date of such transactions.

§ 791.313 Reports to be furnished on demand.

(a) VCS hardware importers and connected vehicle manufacturers are required to furnish under oath, in the form of reports or as otherwise specified by BIS, from time to time and at any time as may be required by BIS, complete information relative to any transaction involving the import of VCS hardware or the import or Sale of completed connected vehicles incorporating covered software, regardless of whether such transaction is effected pursuant to an authorization or otherwise, subject to the provisions of this subpart. BIS may require that such reports include the production of any books, contracts, letters, papers, or other hard copy or electronic documents relating to any transactions, in the custody or control of the persons required to make such reports. BIS may, through any person or agency, conduct investigations, hold hearings,

administer oaths, examine witnesses, receive evidence, take depositions, and require by subpoena the attendance and testimony of witnesses and the production of any books, contracts, letters, papers, and other hard copy or electronic documents relating to any matter under investigation, regardless of whether any report has been required or filed in connection therewith.

(b) For purposes of paragraph (a) of this section, the term "document" includes any written, recorded, or graphic matter or other means of preserving thought or expression (including in electronic format), and all tangible things stored in any medium from which information can be processed, transcribed, or obtained directly or indirectly, including correspondence, memoranda, notes, messages, contemporaneous communications such as text and instant messages, letters, emails, spreadsheets, metadata, contracts, bulletins, diaries, chronological data, minutes, books, reports, examinations, charts, ledgers, books of account, invoices, air waybills, bills of lading, worksheets, receipts, printouts, papers, schedules, affidavits, presentations, transcripts, surveys, graphic representations of any kind, drawings, photographs, graphs, video or sound recordings, and motion pictures or other film.

(c) Persons providing documents to BIS pursuant to this section must submit documents electronically. Acceptable formats include Portable Document Format (PDF) and Microsoft Excel. Files with embedded, encrypted, or password protected content will not be accepted.

§ 791.314 Penalties.

(a) Section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) (IEEPA) is applicable to violations of the provisions of any general authorization, Specific authorization, regulation, order, directive, instruction, or prohibition issued by or pursuant to the direction or authorization of the Secretary of Commerce (Secretary) pursuant to this subpart or otherwise under IEEPA.

(1) A civil penalty not to exceed the amount set forth in section 206 of IEEPA may be imposed on any person who violates, attempts to violate, conspires to violate, or causes a

violation of any exemption, general authorization, specific authorization, regulation, order, directive, instruction, or prohibition issued under this subpart.

(2) A person who willfully commits, willfully attempts to commit, willfully conspires to commit, or aids or abets in the commission of a violation of any exemption, general authorization, specific authorization, regulation, order, directive, instruction, or prohibition issued under this subpart is subject to criminal penalties and may, upon conviction, be fined not more than $1,000,000, or if a natural person, be imprisoned for not more than 20 years, or both.

(b) The civil penalties provided in IEEPA are subject to adjustment pursuant to the Federal Civil Penalties Inflation Adjustment Act of 1990 (Pub. L. 101-410, as amended, 28 U.S.C. 2461 note).

(c) The criminal penalties provided in IEEPA are subject to adjustment pursuant to 18 U.S.C. 3571.

(d) Pursuant to 18 U.S.C. 1001, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the U.S. Government, knowingly and willfully falsifies, conceals, or covers up by any trick, scheme, or device a material fact; or makes any materially false, fictitious, or fraudulent statement or representation; or makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry shall be fined under title 18, United States Code, imprisoned, or both.

(e) Violations of this subpart may also be subject to other applicable laws.

§ 791.315 Pre-penalty notice; settlement.

(a) *When required*. If BIS has reason to believe that there has occurred a violation of any provision of this subpart or a violation of the provisions of any exemption, general authorization, specific authorization, regulation, order, directive, instruction, or prohibition issued by or pursuant to the direction or authorization of the Secretary pursuant to this subpart or otherwise under IEEPA and determines that a civil monetary penalty is warranted, BIS will issue a pre-penalty notice informing the alleged violator of BIS's intent to impose a monetary penalty. A

Pre-Penalty Notice shall be in writing and issued electronically to the alleged violator. The pre-penalty notice may be issued whether or not another agency has taken any action with respect to the matter.

(b) *Response*--(1) *Right to respond.* An alleged violator may respond to a Pre-Penalty Notice in writing to BIS.

(2) *Deadline for response*. A response to a Pre-Penalty Notice must be made within 30 days as set forth below. The failure to submit a response within 30 days shall be deemed to be a waiver of the right to respond.

(i) *Computation of time for response*. A response to a Pre-Penalty Notice must be electronically transmitted on or before the 30th day after the date of delivery by BIS.

(ii) *Extensions of time for response*. If a due date falls on a federal holiday or weekend, that due date is extended to include the following business day. Any other extensions of time will be granted, at the discretion of BIS, only upon specific request to BIS.

(3) *Form and method of response.* A response to a pre-penalty notice need not be in any particular form, but it must be typewritten and signed by the alleged violator or a representative thereof, contain information sufficient to indicate that it is in response to the pre-penalty notice, and include the BIS identification number listed on the pre-penalty notice. A digital signature is acceptable.

(4) *Information that should be included in response*. Any response should set forth in detail why the alleged violator either believes that a violation of the provisions of this subpart did not occur and/or why a civil monetary penalty is otherwise unwarranted under the circumstances. The response should include all documentary or other evidence available to the alleged violator that supports the arguments set forth in the response. BIS will consider all relevant materials submitted in the response.

(c) *Settlement.* Settlement discussions may be initiated by BIS, the alleged violator, or the alleged violator's authorized representative.

(d) *Representation.* A representative of the alleged violator may act on behalf of the alleged violator, but any oral communication with BIS prior to a written submission regarding the specific allegations contained in the pre-penalty notice must be preceded by a written letter of representation, unless the pre-penalty notice was served upon the alleged violator in care of the representative.

§ 791.316 Penalty imposition.

(a) If, after considering any written response to the pre-penalty notice and any relevant facts, BIS determines that there was a violation by the alleged violator named in the pre-penalty notice and that a civil monetary penalty is appropriate, BIS may issue a penalty notice to the violator containing a determination of the violation and the imposition of the monetary penalty.

(b) The issuance of the penalty notice shall constitute final agency action. The violator may seek judicial review of that final agency action in federal district court.

§ 791.317 Administrative collection; referral to United States Department of Justice.

In the event that the violator does not pay the penalty imposed pursuant to this subpart or make payment arrangements acceptable to BIS, the matter may be referred for administrative collection measures by the Department of the Treasury or to the United States Department of Justice for appropriate action to recover the penalty in a civil suit in a federal district court.

§ 791.318 Finding of Violation.

(a) *When issued.* (1) BIS may issue an initial finding of violation that identifies a violation if BIS:

(i) Determines that there has occurred a violation of any provision of this subpart, or a violation of the provisions of any exemption, general authorization, specific authorization, regulation, order, directive, instruction, or prohibition issued by or pursuant to the direction or authorization of the Secretary pursuant to this subpart or otherwise under IEEPA;

(ii) Considers it important to document the occurrence of a violation; and

(iii) Concludes that an administrative response is warranted but that a civil monetary penalty is not the most appropriate response.

(2) An initial finding of violation shall be in writing and may be issued whether or not another agency has taken any action with respect to the matter.

(b) *Response*--(1) *Right to respond*. An alleged violator may contest an initial Finding of Violation by providing a written response to BIS.

(2) *Deadline for response; default determination*. A response to an initial Finding of Violation must be made within 30 days as set forth in paragraphs (b)(2)(i) and (ii) of this section. The failure to submit a response within 30 days shall be deemed to be a waiver of the right to respond, and the initial Finding of Violation will become final and will constitute final agency action. The violator may seek judicial review of that final agency action in federal district court.

(i) *Computation of time for response*. A response to an initial finding of violation must be electronically transmitted on or before the 30th day after the date of delivery by BIS.

(ii) *Extensions of time for response*. If a due date falls on a federal holiday or weekend, that due date is extended to include the following business day. Any other extensions of time will be granted, at the discretion of BIS, only upon specific request to BIS.

(3) *Form and method of response*. A response to an initial finding of violation need not be in any particular form, but it must be typewritten and signed by the alleged violator or a representative thereof, contain information sufficient to indicate that it is in response to the initial finding of violation, and include the BIS identification number listed on the initial finding of violation. A digital signature is acceptable.

(4) *Information that should be included in response*. Any response should set forth in detail why the alleged violator either believes that a violation of the provisions of this subpart did not occur and/or why a finding of violation is otherwise unwarranted under the circumstances. The response should include all documentary or other evidence available to the alleged violator that

supports the arguments set forth in the response. BIS will consider all relevant materials submitted in the response.

(c) *Determination*--(1) *Determination that a finding of violation is warranted*. If, after considering the response, BIS determines that a final finding of violation should be issued, BIS will issue a final finding of violation that will inform the violator of its decision. Any action taken in a final finding of violation shall constitute final agency action. The violator has the right to seek judicial review of that final agency action in federal district court.

(2) *Determination that a finding of violation is not warranted*. If, after considering the response, BIS determines a finding of violation is not warranted, then BIS will inform the alleged violator of its decision not to issue a final finding of violation.

§ 791.319 Severability

If any provision of this subpart is held to be invalid or unenforceable by its terms, or as applied to any person or circumstance, or stayed pending further agency action or judicial review, the provision is to be construed so as to continue to give the maximum effect to the provision permitted by law, unless such holding will be one of utter invalidity or unenforceability, in which event the provision will be severable from this part and will not affect the remainder thereof.

[FR Doc. 2024-21903 Filed: 9/23/2024 8:45 am; Publication Date: 9/26/2024]