BILLING CODE: 3510-33

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

15 CFR Part 791

[Docket No. 250107-0005]

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: Final rule.

SUMMARY: This final rule, published by the Department of Commerce's (Department) Bureau of Industry and Security (BIS), sets forth regulations and procedures 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 that are integral to connected vehicles as defined herein.

DATES: This final rule goes into effect on [INSERT DATE 60 DAYS FROM DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

FOR FURTHER INFORMATION CONTACT: Marc Coldiron, U.S. Department of Commerce, telephone: (202) 482-3678. For media inquiries: 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 final rule, BIS prohibits 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 and the Macau Special Administrative Region, (PRC); or the Russian Federation (Russia). It follows an advance notice of proposed rulemaking (ANPRM), 89 FR 15066 (March 1, 2024), and a notice of proposed rulemaking (NPRM), 89 FR 79088 (September 26, 2024). In the ANPRM, 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 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. The NPRM proposed a rule to address the undue or unacceptable risks identified in the ANPRM and solicited public comment. BIS has considered the comments received during both rounds of public comment, and is making revisions, from the proposed rule, that address significant portions of that feedback.

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 that the Secretary, in consultation with relevant agency heads, has determined involve foreign adversary ICTS and pose certain risks to

U.S. national security, including U.S. technology and critical infrastructure, or the security and safety of U.S. persons. 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, which, pursuant to E.O. 13873's implementing regulations at 15 CFR 791.4 are the PRC, Republic of Cuba (Cuba), Islamic Republic of Iran (Iran), Democratic People's Republic of Korea (North Korea), Russia, and Venezuelan politician Nicolás Maduro (Maduro Regime); 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."

Factors A through C are collectively referred to as "undue or unacceptable risks." In addition, section 1(b) of E.O. 13873 grants the Secretary the authority to design or negotiate mitigation measures to allow an otherwise prohibited transaction.

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 regulations 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 and foreign adversaries may exploit vulnerabilities to gain access to a vehicle. As BIS outlined in its March 1, 2024, ANPRM and its September 26, 2024, NPRM, certain 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 a foreign adversary.

In the *Securing the Information and Communications Technology and Services Supply Chain* interim final rule, 86 FR 4909 (Jan. 19, 2021), the Secretary determined that certain foreign governments or foreign non-government persons—the PRC, Cuba, Iran, North Korea, Russia, and the Maduro Regime—constitute foreign adversaries for purposes of E.O. 13873 and regulations 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 final rule intends to reflect the most up-to-date designations of foreign adversaries). Additionally, section 2(b) of E.O. 13873 provides that the Secretary may issue rules that identify particular technologies or countries with respect to transactions involving ICTS that warrant particular scrutiny. For the purposes of this final 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 undue and unacceptable risks to U.S. national security because of these adversaries' legal, political, and regulatory regimes, combined with their current and anticipated growth and involvement in the connected vehicles sector.

As discussed below, 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 their 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 and hardware, could enable those foreign adversaries to (1) exfiltrate sensitive data collected by connected vehicles and (2) 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 can facilitate the exfiltration of data and remote manipulation of connected vehicles by the PRC and Russia pose undue or unacceptable risks to U.S. national security and to the safety and security of U.S. persons. These risks, moreover, present an urgent national security risk to the safety and security of technology used in the United States and to U.S. persons.

The PRC has pre-positioned malware on U.S. information technology and critical infrastructure networks. The PRC has also set objectives for the completion of the People's Liberation Army's (PLA) modernization and other military and technology goals by 2027, which—in light of the PLA's military-civil fusion strategy and the growing prevalence of PRC dual-use technologies in U.S. commercial supply chains, including in the auto industry—presents additional risks to U.S. national security. Mounting evidence of threats such as these to U.S. critical infrastructure, data security, and broader national security necessitates this urgent action by the U.S. government to address the risk of foreign adversary supply chains in the connected vehicles sector.

a. Overview of the Advance Notice of Proposed Rulemaking (ANPRM)

BIS issued an ANPRM, 89 FR 15066 (Mar. 1, 2024), seeking public comment to inform a rulemaking that would address the undue or unacceptable risks posed by a class of transactions that involve 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 the ANPRM, BIS posed 35 questions to the public for comment and feedback. The questions related to potential definitions used in the rulemaking, the degree of foreign adversary involvement in the connected vehicle supply chain, which systems should be the focus of a potential rulemaking, and what the economic impacts of a potential rulemaking might be, among other questions. BIS identified six systems as the potential focus for a future rule: (1) vehicle operating systems (OS), (2) telematics systems, (3) advanced driver assistance systems (ADAS), (4) automated driving systems (ADS), (5) satellite or cellular telecommunications systems, and (6) battery management systems (BMS). BIS received 57 comment submissions in response to the ANPRM from a variety of parties, including original equipment manufacturers (OEMs), component suppliers, two foreign governments, nonprofit organizations, and individual respondents. Five comments contained Confidential Business Information (CBI), and one comment was retracted at the request of the commenter. The comments generally urged BIS to narrow the scope of a future regulation and to limit the systems to be regulated to only those posing significant national security risks. Commenters also urged BIS to provide industry stakeholders with sufficient lead time to comply. BIS considered each comment in developing the NPRM outlined in the next section.

b. Overview of the Notice of Proposed Rulemaking (NPRM)

BIS then issued an NPRM, 89 FR 79088 (Sept. 26, 2024), that identified a smaller subset of systems in connected vehicles that pose the most significant undue or unacceptable risk to national security when designed, developed, manufactured, or supplied by persons owned by,

controlled by, or subject to the jurisdiction or direction of the PRC or Russia. Below is a summary of the proposed rule.

Regulated Systems

The proposed rule identified (1) VCS, which is composed of the hardware and software that enable a connected vehicle to communicate off-board above 450 MHz, and (2) ADS, as subject to regulation by BIS. This determination was based, in part, on public comments requesting BIS narrow the scope of the rule, as a regulation that impacted all six of the listed automotive systems would be overbroad. The ANPRM listed ADS, operating systems, telematic systems, automated driving assistance systems, satellite and communication systems, and battery management systems as potential automotive systems that could be regulated in the subsequent proposed rule. Public comment as well as BIS's analysis suggested that automotive telematics functions were one of the primary means for a foreign adversary to exploit automotive data and actuation systems. BIS also determined, based on public comment as well as internal analysis, that the term "telematics" generally refers to systems that operate on cellular band protocols. As BIS intended to regulate multiple automotive connectivity systems, not just automotive cellular systems, BIS chose to use the broader term of "VCS" to encompass cellular, Wi-Fi, Bluetooth, and potentially satellite communications. The NPRM proposed to regulate both the hardware and software in VCS and solely the software in ADS.

Prohibited Transactions

The NPRM proposed to (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, which was defined in the NPRM as certain software that supports the function of VCS or ADS; and (3) prohibit connected vehicle manufacturers from knowingly selling within the United States completed connected vehicles that incorporate software that supports the function of VCS or ADS. These prohibitions included in the NPRM applied when such VCS hardware or

covered software was designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. The NPRM also proposed to (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, even when that hardware or software did not have a nexus to the PRC or Russia.

Declarations of Conformity

The NPRM proposed that VCS hardware importers and connected vehicle manufacturers would submit to BIS, once per calendar year or model year, Declarations of Conformity attesting that they had not engaged in prohibited transactions involving VCS hardware or covered software. The NPRM would have mandated that VCS hardware importers and connected vehicle manufacturers submit a substantial amount of information with their Declarations of Conformity, including a hardware bill of materials (HBOM) or software bill of materials (SBOM), and a list of external endpoints to which the VCS hardware connected. In the final rule, BIS has changed the Declarations of Conformity requirement to clarify the certification, narrow the information required to be submitted, and add recordkeeping requirements.

Authorizations

The NPRM enumerated general authorizations under which a regulated entity would be permitted to engage in an otherwise prohibited transaction without need to notify BIS. Under the NPRM, general authorizations would have been available to small business VCS hardware importers and connected vehicle manufacturers. Specifically, general authorizations applied if (1) the connected vehicle manufacturer or VCS hardware importer produced fewer than 1,000 connected vehicles or VCS hardware units; (2) the completed connected vehicle was used on public roadways for fewer than 30 calendar days in a year; (3) the completed connected vehicle or VCS hardware was used solely for purposes of display, testing, or research; or (4) the completed connected vehicle was imported solely for repair, alteration, or competition off public

roads and would have been exported within one year of import. In the final rule, BIS has revised the general authorizations provision so that the above-mentioned general authorizations are not provided in the rule text itself. Instead, BIS will issue general authorizations through its website and the *Federal Register*.

The NPRM also provided a process for specific authorizations. Following an application to and approval from BIS, a specific authorization granted VCS hardware importers and connected vehicle manufacturers the ability to engage in otherwise prohibited transactions not eligible for a general authorization, subject to certain conditions imposed by BIS.

Exemptions

The NPRM permitted VCS hardware importers to engage in otherwise prohibited transactions involving VCS hardware and exempted them from certain requirements so long as: (1) for VCS hardware not associated with a model year, the import of the VCS hardware had taken place prior to January 1, 2029; or (2) the VCS hardware unit was associated with a vehicle model year prior to 2030 or the VCS hardware was integrated into a connected vehicle (completed or incomplete) with a model year prior to 2030. In the NPRM, connected vehicle manufacturers were permitted to engage in otherwise prohibited transactions involving covered software and exempt from certain requirements so long as the completed connected vehicle that was imported, or sold within the United States, was of a model year prior to 2027. Lastly, connected vehicle manufacturers that are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia were permitted to sell completed connected vehicles with a model year prior to 2027 that incorporated VCS hardware or covered software. The final rule includes new exemptions for parts that are imported for the purpose of warranty or repair of a completed connected vehicle with a model year prior to 2030.

Advisory Opinions, Is-Informed Notices, and Appeals

The NPRM provided an advisory opinion mechanism by which regulated entities could seek guidance from BIS as to whether specific prospective transactions were subject to the proposed

rule's prohibitions. The mechanism included in the NPRM applied to actual, as opposed to hypothetical, transactions in which all parties are identified. Additionally, the NPRM permitted BIS to issue certain "Is-Informed" notices to VCS hardware importers and connected vehicle manufacturers to inform them that a specific authorization was required for an activity. The NPRM also included an appeal process by which any person whose application for a specific authorization was denied, whose specific authorization was suspended or revoked, or who received a written notification of ineligibility for a general authorization could appeal that decision to the Under Secretary for Industry and Security (Under Secretary). In the final rule, BIS has added a 60-day timeline for BIS to respond to advisory opinion requests and clarified procedural requirements of submitting an appeal request.

Recordkeeping and Reporting

The NPRM proposed that regulated entities keep a "full and accurate record" for a period of 10 years after each transaction for which a Declaration of Conformity, general authorization, or specific authorization was required, regardless of whether the transaction was effected pursuant to such an authorization. In the NPRM, VCS hardware importers and connected vehicle manufacturers were required to furnish "complete information" relevant to any transaction involving the import of VCS hardware or covered software, irrespective of any authorization granted by BIS.

Violations

The NPRM additionally outlined the framework by which BIS determined a violation took place, the procedure by which BIS notified an affected party of such a violation (including the party's right to respond or to settle), the specific penalties BIS was permitted to impose on violators, and the administrative collection of those penalties.

c. Overview of Final Rule

The final rule benefits from the responses received during the public comment periods for the ANPRM and the NPRM 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. As stated in the NPRM, determining the scope of the prohibitions required a balancing of 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. For a detailed discussion of how the final rule has changed from the NPRM, refer to Section V: Discussion of the Final Rule and Section VI: Revisions from the Proposed Rule and Response to Comments.

III. Comments on the Notice of Proposed Rulemaking

BIS received 101 comments on the NPRM.[1] Many commenters agreed with BIS's risk assessment of foreign adversary connected vehicle technology as described in Section IV of the NPRM and supported the decision to address these risks through supply chain regulation. Commenters' concerns with the NPRM centered on the broad scope of the regulation and the potentially onerous and disruptive nature of the compliance process, particularly the submission of Declarations of Conformity. Some commenters disagreed with the NPRM's inclusion of the commercial vehicle market, arguing that definitions proposed in the NPRM did not as easily apply to this sector compared to the passenger vehicle market. Commenters also warned that the wide scope of the NPRM across the connected vehicle market may have significant economic impact and that the current implementation timeline could not easily be met by industry.

Commenters requested that BIS implement alternative methods of compliance, such as a self-certification model; provide greater detail on the HBOM and SBOM submission requirements; and describe how BIS intends to protect any submitted data. Commenters also voiced apprehension over any requirement to share proprietary information with customers and the government. For a more thorough discussion of the comment submissions and BIS's responses, please see Section IV: Risks Associated with Vehicle Connectivity Systems and Automated

[1] This includes four written submissions received after the close of the public comment period, all of which were considered and posted on regulations.gov.

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 and Section V: Discussion of the Final Rule.

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.

BIS received multiple comments related to the risks stemming from VCS and ADS when designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. Commenters agreed with the risks posed by PRC and Russian involvement in the connected vehicle supply chain as laid out in the NPRM, and BIS reiterates those same risks in this section. For instance, one commenter acknowledged that allowing adversarial suppliers into the automotive supply chain poses direct threats to data integrity, consumer safety, and national security. In contrast, another commenter critiqued the proposed rule as overly broad and characterized the threats as hypothetical in nature, underscoring that PRC and Russian companies are incentivized to avoid exploiting vulnerabilities in connected vehicles in order to avoid conflict. BIS recognizes that many of the risks laid out in the NPRM and final rule are forward-looking, and this rulemaking is an attempt to proactively address these risks before PRC and Russian actors are able to leverage them to harm U.S. national security. Moreover, while BIS agrees that action by the PRC or Russia to leverage vulnerabilities in VCS or ADS could feasibly cause undesired conflict, the strategic benefit of exploiting vulnerabilities may outweigh other types of harm it causes and thus is unlikely to preclude such an action altogether from the perspective of the PRC and Russia. Another commenter highlighted that the rule does not apply retroactively to address any of the data already collected by connected vehicle manufacturers that may have already been legitimately transferred to the PRC or other foreign adversaries and may be informing foreign intelligence analysis. BIS recognizes that some connected vehicle and component manufacturers

may already transfer vehicle data abroad, a point that is reiterated later in this final rule. However, BIS believes that retroactive application of this rule would not reduce or alleviate any of the harm that has already occurred as a result of foreign intelligence organizations gaining access to that data. Following consideration of the comments received on the NPRM, and further consideration of the risks and vulnerabilities associated with various ICTS components that are critical to the operation of connected vehicles, BIS has decided to retain the proposed rule's focus 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 adversaries—the PRC and Russia. Below, BIS provides its findings of the undue and unacceptable risks associated with these particular systems, and these particular foreign adversaries, following this latest round of public comments.

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 units (TCU), cellular modems and antennas, and other automotive components—that integrate various radio frequency (RF) 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 Global Positioning Systems (GPS), accelerometers, gyroscopes, BMS, and other Electronic Control Units via wired networks like Controller Area Network (CAN) bus, Local Interconnect Network (LIN), FlexRay, Automotive Ethernet and 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. Sensing systems, such as radar, audio, video, or Light Detection and Ranging (LiDAR) hardware and software, are not VCS. Based on a number of comments to the proposed rule, BIS recognizes a national security risk posed by LiDAR, but it concludes that focusing this regulation on VCS hardware and software systems, which ultimately enable the external communication of end-point sensors, is an appropriate scope at this time. For a more thorough discussion on the exclusion of PRC or Russian LiDAR from this rule, please see Section VI below.

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 connected vehicle network. Each access point may present multiple new software vulnerabilities for adversaries to exploit. *See* Cabell Hodge, Konrad Hauk, Shivam Gupta, and Jess Bennett, Vehicle Cybersecurity Threats and Mitigation Approaches, *National Renewable Energy Laboratory*, at 4-5 (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 where software functionality can be accessed and altered, 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 chipmaker's processor. This malicious software unlocked features to manipulate the vehicle, such as acceleration and heated seats. Upstream, *2024 Global Automotive Cybersecurity Report*, at 62 (Feb. 2024), https://upstream.auto/reports/global-

automotive-cybersecurity-report. The software also provided access to private user data 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 id*. 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 & Infrastructure Security Agency, *Defending Against Software Supply Chain Attacks,* at 6 (Apr. 2021), https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508.pdf; 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. The primary standard setting organization for automotive autonomy is the global mobility standard-setting body SAE International. SAE International sets standards that affect many aspects of automotive production and maintenance, often in concert with the International Standards Organization (ISO). SAE International's *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles* (SAE J3016) is the current industry norm for evaluating standard levels of vehicle autonomy. 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. Level 4 requires the ability to complete all driving functions on a sustained basis within defined operational design domains (ODDs), while Level 5 requires the ability to complete all driving functions unconditionally. 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* SAE J3016_02104, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, *SAE International*, at 31-32 (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 (OEDCR). OEDCR 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 id.* at 17; Edward Griffor, David Wollman, and Christopher Greer, Automated Driving System Safety Measures Part 1: Operating Envelope Specification, *NIST Special Publication 1900-301*, at 2 (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. For example, a user of a vehicle, or even an OEM purchaser of ADS likely does not know the sum total of what data the ADS was trained on, or how, specifically, the ADS makes its decisions. It is not possible to find single lines of code that dictate how an ADS responds to specific scenarios in modern ADS systems. Rather, leading ADS are controlled by complex software that can include a neural net that references training data and previous decisions to instantaneously decide on an action in a driving setting. This opacity and lack of understanding of how the system actually reacts is inherently vulnerable to poisoned data injection or specific scenario-based failures. 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 electronic control units (ECUs) responsible for engine control, traction control, door locks, climate control, battery management, powertrain, airbags, cameras, and radar functionalities. These ECUs also communicate via overlaid communication networking protocols such as a CAN bus, 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, at 508-513, (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 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. This could lead to disablement or compromise of other vehicles or of transportation infrastructure, affecting the movement of goods and the physical safety of drivers. *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; 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 capability 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 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* subsection IV.b. As such, direct access to an ADS afforded to a malicious actor or foreign adversary 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*

Several commenters agreed that PRC laws compel compliance with government requests, thereby making some companies subject to the direction of the PRC government. One commenter provided additional detail about the linkages between prominent Chinese companies, the PRC military, and the global automotive industry. Two commenters noted that current investments by Chinese companies in Mexico may allow effective "backdoor" access to the American auto market. One commenter specifically pointed to the risks posed by Chinese-developed buses with connectivity features as posing a particular threat to U.S. national security. While commercial vehicles such as buses are not in the scope of this final rule, BIS intends to propose a new rule specifically tailored to the commercial vehicle sector in order to address substantial national security risks. Another commenter agreed with the Department's actions, specifically as it related to addressing the large amounts of data collected by connected vehicles already being transmitted to the PRC, regardless of the vehicle's physical location. In response to commenters' agreement with the nature of PRC and Russian legal and regulatory landscapes, BIS is reiterating its legal and risk analyses in this final rule. Moreover, BIS thanks commenters for providing additional information that clarifies the linkages between the PRC state, military, and the broader economy. In light of concerns raised by commenters regarding PRC companies' investments in Mexico, BIS reiterates that PRC investments in Mexico's auto sector risk creating additional potential nexus points between PRC connected vehicle suppliers and U.S. automakers and consumers. Similarly, BIS agrees with commenters' concerns that the PRC-linked entities already collect large amounts of data, including from vehicles which are currently located in the

United States. These concerns directly underscore the importance and necessity of this rulemaking.

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. As discussed further, 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. In addition, unlike other foreign adversaries, the PRC and Russia 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 that has become increasingly integrated into the ICTS supply chains of global automakers, providing the PRC automotive sector with 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; Matthew Funaiole, et al., China Accelerates Construction of 'Ro-Ro' Vessels, with Potential Military Implications, *Center for Strategic and International Studies* (Oct. 11, 2023), https://chinapower.csis.org/analysis/china-construct-ro-ro-vessels-military-implications/ (describing the involvement of Chinese automakers in the production of "ro-ro" vessels and the dual-use applications of ro-ro vessels, including clear evidence that the PRC

military intends to utilize ro-ros to support military operations). Moreover, the PRC possesses advanced cyber espionage capacities that it exercises through both state and non-state cyber actors, exacerbating such risks. *See* Simon Handler, The 5x5-China's cyber operations, *The Atlantic Council* (Jan. 2023), https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/.

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 technological innovation and sustainable development of the automobile market, including new energy vehicles and connected vehicle software and hardware systems, as key priorities. *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*, at 22-23 (May 2021), https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf. For many years, the state has pursued 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. The PRC automotive sector's growth is also led in part by several prominent state-owned firms, some of which began as military equipment suppliers (*e.g.*, Dongfeng, Sichuan Auto Works, Shanxi Auto Works). *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, at 14 (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/; 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. *See* Daisuke Wakabayashi and Claire Fu, China E.V. Makers Rush In and Upend a Country's Entire Auto Market, *The New York Times* (Jul. 30, 2024*),* https://www.nytimes.com/2024/07/30/business/chinese-electric-vehicles-thailand.html; Daniel Leussink, BYD's Global expansion push runs into stiff Japan test, *Reuters* (Sept. 4, 2024), https://www.reuters.com/business/autos-transportation/byds-global-expansion-push-runs-into-stiff-japan-test-2024-09-05/; China's BYD starts construction on manufacturing complex in Brazil, *Reuters* (Mar. 5, 2024), https://www.reuters.com/business/autos-transportation/chinas-byd-starts-construction-manufacturing-complex-brazil-2024-03-06/.

The global expansion of the PRC auto sector's operations in foreign markets and recent foreign investment announcements indicate that Chinese automakers could attempt to enter the U.S. market via exports from third-party countries. Exports from third-party countries of vehicles with Chinese ICTS would expand the scope of the risk that Chinese ICTS poses to U.S. national security. *See* Paul Wiseman, Prospect of low-priced Chinese EVs reaching US from Mexico poses threat to automakers, *The Associated Press* (June 27, 2024), https://www.ap.org/news-

highlights/spotlights/2024/prospect-of-low-priced-chinese-evs-reaching-us-from-mexico-poses-threat-to-automakers/; Daina Beth Solomon, Chinese automaker BYD looking for Mexico plant location, executive says, *Reuters* (Feb. 28, 2024), https://www.reuters.com/business/autos-transportation/chinese-carmaker-byd-launches-low-cost-dolphin-mini-ev-mexico-2024-02-28/. 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). *See id.* Therefore, the PRC's growing presence within the global auto sector, particularly via operations in third-party countries, is expected to expand the number of potential nexus points between PRC connected vehicle suppliers and U.S. automakers and consumers, further undermining U.S. national security.

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. The military-civil fusion strategy prioritizes specific information and communication technologies and services that are integral to connected vehicle supply chains (*e.g.*, telecommunications, artificial intelligence). *See* Ben Murphy, Translation for 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*, at 11 and 36 (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 (IP) 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*, at 6-10 (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. For example, the PRC intervenes in the auto market 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, of the PRC's expansive 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. The PRC pursues its broad national security and geopolitical objectives 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; Ministry of Civil Affairs of the People's Republic of China, *National Security Law of the People's Republic of China,* Arts. 25 and 77, promulgated by the 12th National People's Congress on July 1, 2015, https://www.mca.gov.cn/zt/n2643/n2647/c1662004999979993333/content.html. 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,* (July 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.

Fourth, the PRC has demonstrated a high level of competency in cyber malfeasance. For instance, PRC state-sponsored cyber group Volt Typhoon has proven capable of infiltrating the

IT networks of critical U.S. infrastructure using sophisticated tactics, techniques, and procedures such as Living Off the Land Techniques to pre-position themselves across U.S. critical infrastructure and military assets to carry out advanced reconnaissance in IT systems. At a later point, once advanced reconnaissance is conducted, they are then capable of launching cyberattacks to impede U.S. decision making, induce social panic, and interfere with the deployment of U.S. military forces. *See* Cybersecurity & Infrastructure Security Agency, *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, at 1-5 (Feb. 2024), https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf. 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. This argument is supported by public reporting detailing 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*, at 11 and 14-15 (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 the 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,* at 3 (Oct. 2012),

https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf. This risk is further demonstrated 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* Ryan Neauhard, Flawed by design electronics with pre-installed malware, *Georgetown Security Studies Review,* at 2 (May 23, 2018), 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, present a significant risk that the PRC could alter the systems in or obtain and manipulate data 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 United States. 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. Incorporating Russian hardware or software into the U.S. connected vehicle supply chain, therefore, poses undue and unacceptable risks to U.S persons and critical infrastructure.

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 domestic auto manufacturing industry following the exodus of foreign automakers after the imposition of significant additional

sanctions in 2022 in response to the conflict in Ukraine. In 2024 alone, the Russian auto market is projected to experience a 15 percent increase in passenger vehicle sales, marking a notable uptick since the Russian market crashed in 2022 following the imposition of sanctions, and some Russian auto manufacturers have continued introducing new models even amid broader economic headwinds. *See* Russia's 2024 car sales forecast raised to 1.45mln, units, AEB says, *Reuters* (July 3, 2024), https://www.reuters.com/business/autos-transportation/russias-2024-car-sales-forecast-raised-145-mln-units-aeb-says-2024-07-03. Russia's domestic auto sector has begun to show signs of resilience, with at least one automaker releasing a new, primarily domestically developed model since the imposition of Western sanctions, even as other domestically sold models are manufactured in the PRC but undergo final assembly in Russia. *See* Gleb Stolyarov and Alexander Marrow, Focus: Made in Russia? Chinese cars drive a revival of Russia's auto factories, *Reuters* (July 20, 2023), https://www.reuters.com/business/autos-transportation/made-russia-chinese-cars-drive-revival-russias-auto-factories-2023-07-20/. In Russia, the revitalization of the domestic economy, particularly the domestic auto sector, has become a key focus of the Russian government since the imposition of sanctions in recent years. The Russian government has released several plans that prioritize the development of its domestic automotive market with a particular focus on research and development of new technology, including autonomous vehicles and V2X ("Vehicle to Everything") 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; 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

involves 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. Rosavto 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. Further, Russia has demonstrated resilience against Western sanction and export control regimes while also continuing to grow its electric vehicle market. See Carnegie Endowment, *Why Russia Has Been So Resilient to Western Export Controls*, (Mar. 2024), https://carnegieendowment.org/research/2024/03/why-russia-has-been-so-resilient-to-western-export-controls?lang=en. According to market reporting, the Russian electric vehicle market has had a robust performance, with double digit growth in output and sales, largely driven by a surge in the sector's exports. *See* Russia Automotive Market Report – Analysing EVE Trends and Car Sales Volume Data, *Global Monitor* (retrieved Nov. 2024), https://www.globalmonitor.us/product/russia-automotive-market. Projections suggested that with the support of the government, the electric vehicle subsector is poised for further growth. *See id*. Concerted efforts by the Russian government to develop the domestic Russian automotive industry, a growing electric vehicle market, and resilience to western sanction and export control regimes increase the likelihood that Russia-linked connected vehicle technology, such as VCS hardware or covered software, will enter the U.S. connected vehicle supply chain, which, as described below, presents an undue or unacceptable risk to U.S. national security. Given these factors, BIS is taking proactive measures to mitigate any risk posed by Russia's influence over

the U.S. connected vehicle supply chain and to prevent Russia from gaining increasing influence over the U.S. connected vehicle supply chain in the future.

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) allow the Russian government direct control over Russian corporations' activities and facilities, including data or customer information, and mandate that companies assist with 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 through 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, including 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,* at 40 (Apr. 2021), https://www.sciencedirect.com/science/article/pii/S0267364920301175.

Third, apart from the risks presented by the Russian government access as 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 malware to the platform's users after Russian intelligence services obtained covert access to the computer systems on which the platform was installed. The attack 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 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*, at 3 (Dec. 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a. BIS has further identified Kaspersky Lab as an example of the risks imposed by Russia's ability to leverage software companies to allow Russia 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. (June 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 demonstrated capabilities of Russia to exploit ICTS supply chains through malicious cyber activity, exacerbate BIS's concern that the threats posed by Russia 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 Russian government 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 and to the safety and security of U.S. persons 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 serve in the operation of connected vehicles, these systems, if compromised and co-opted by an adversary, could serve as the nodes through which a foreign actor could probe or breach broader ICTS systems within the United States. 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 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*, at 505 (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 could result in physical harm to U.S. persons. A

disabled, impaired, or erratically functioning connected vehicle, or potentially multiple connected vehicles all experiencing problems simultaneously, could cause traffic patterns that would effectively block critical transportation arteries. This scenario could also cause collisions, ultimately damaging transportation features (*e.g.*, roadways, bridges, tunnels), 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. *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,* at 515 (2023); Luis Hernandez, et al., Applications of Cloud Computing in Intelligent Vehicles, *Journal of Artificial Intelligence and Machine Learning in Management*, at 12-13 (2022). 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 or global navigation satellite systems (GNSS) 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. *See* Cybersecurity & Infrastructure Security Agency, *Autonomous Ground Vehicle Security Guide: Transportation Sector*, at 1 (2021),

https://www.cisa.gov/sites/default/files/publications/Autonomous%2520Ground%2520Vehicles%2520Security%2520Guide.pdf; Cybersecurity & Infrastructure Security Agency, *Cybersecurity and Physical Security Convergence*, at 1 (2020), https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520and%2520Physical%2520Security%2520Convergence_508_01.05.2021.pdf. 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 would have serious consequences for U.S. persons' health and safety. 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 operational 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 its 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.

V. Discussion of the Final Rule

This final rule prohibits —absent a general or specific authorization otherwise—(1) VCS hardware importers from knowingly importing into the United States certain hardware for VCS (section 791.302, "Prohibited VCS hardware transactions"), (2) connected vehicle manufacturers from knowingly importing into the United States completed connected vehicles incorporating covered software, and (3) connected vehicle manufacturers from knowingly selling within the United States completed connected vehicles that incorporate covered software (section 791.303, "Prohibited covered software transactions"). These prohibitions 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. The rule also (4) prohibits 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 (section 791.304, "Related prohibited transactions"), regardless of whether 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 (collectively, "prohibited transactions").

This rule primarily impacts 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 one and tier two 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 are required to be submitted to BIS by VCS hardware importers and connected vehicle manufacturers prior to importing VCS hardware or importing or selling completed connected vehicles that incorporate covered software, certifying that the VCS hardware or covered software was not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia (section 791.305, "Declaration of Conformity"). The Declarations of Conformity require VCS hardware importers and connected vehicle manufacturers to certify to BIS, once a year or whenever material changes occur, that they are not engaging in prohibited transactions and provide certain information on the import of VCS hardware and/or the import or sale of completed connected vehicles as relevant.

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 (section 791.306, "General authorizations"). General authorizations are 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 type of transaction. In determining whether to issue a general authorization, BIS may consider any information or material BIS deems relevant and appropriate, classified or unclassified, from any Federal department or agency, or from any other source. BIS will publish general authorizations issued pursuant to this subpart on its website (https://www.bis.gov/OICTS) and will also publish them in the *Federal Register*. Those availing themselves of a general authorization are 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 renders the transaction ineligible for a general authorization, such as a change in the vehicle's use, the VCS hardware importer or connected vehicle manufacturer is required to apply for a specific authorization and cease engaging in such transaction unless and until a specific authorization is granted.

Lastly, a specific authorization may be permitted 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 from BIS (section 791.307, "Specific authorizations"). Such VCS hardware importers and connected vehicle manufacturers are required to pause engaging in these transactions before they may proceed with the prohibited transaction under a specific authorization. A specific authorization will only be available in circumstances where BIS determines, based on the information submitted by the applicant as well as any information or material BIS deems relevant and appropriate, classified or unclassified, from any Federal department or agency, or from any other source, 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 can appeal any of the following BIS decisions to the Under Secretary: the determination that a VCS hardware importer

or connected vehicle manufacturer is ineligible for a general authorization, the denial of an application for a specific authorization, or the suspension or revocation of a previously granted specific authorization (section 791.309, "Appeals"). Further, the regulation establishes a method for VCS hardware importers and connected vehicle manufacturers to seek guidance on prospective transactions that may be prohibited through a BIS advisory opinion (section 791.310, "Advisory opinions"). BIS may also share guidance on its website for VCS hardware importers or connected vehicle manufacturers that certain activities could constitute a prohibited transaction.

In issuing 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 interprets the phrase "information or informational materials" to be limited to expressive material, consistent with the purpose of 50 U.S.C. 1702(b)(3) to protect materials involving the free exchange of ideas from regulation under IEEPA and with IEEPA's broader purpose to limit material support to adversaries. A broader interpretation of the term would enable adversaries and countries of concern to use non-expressive data to undermine our national security.

In the NPRM, BIS explained this regulation is consistent with the Berman Amendment. BIS sought comment on this issue, including whether and how to address the term "information or

informational materials" in the final rule. One commenter claimed that the prohibitions included in the rule could extend beyond IEEPA's intended purpose and result in litigation risk for BIS. Therefore, according to the commenter, BIS should clarify what types of information sharing will be allowed in light of the IEEPA limitations included in the Berman Amendment. One commenter requested clarification on what types of information sharing will be allowed under the rule, including documentation of technology designs. Another commenter asked about "the information/materials—including technology design documentation—that will be permitted or required when the Berman Amendment applies." In response, BIS notes that this rule does not add any restrictions on the sharing of technology designs, technical documentation, or similar information, nor does it remove any restrictions that may exist under any other regulation (*e.g.*, export controls). Additionally, while this rule requires regulated parties to maintain documentation relevant to their compliance with this rule, it does not prescribe any specific requirements as to what that documentation must consist of. BIS did not receive any comments requesting that specific provisions relating to information or informational materials be added to the rule.

This final 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 to restrict the import or export of expressive speech and communicative works and mediums that may be carrying such expressive content. 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 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. This final rule "balances

IEEPA's competing purposes" in "restricting material support for hostile regimes while encouraging the robust interchange of information." *United States v. Amirnazmi*, 645 F.3d 564, 587 (3d Cir. 2011). Thus, BIS has determined that the prohibitions in this rule are consistent with the Berman Amendment. To the extent that any parties believe that a transaction governed by this rule qualifies as "information or informational materials" that is exempt under 50 U.S.C. 1702(b)(3), they can seek clarification using the administrative processes for seeking an advisory opinion.

VI. Revisions from the Proposed Rule and Response to Comments

Each section of the final rule is discussed below, including BIS's consideration of comments received in response to the NPRM.

a. *Definitions*

BIS received a variety of comments regarding the definitions listed in the NPRM. In the following sections, BIS summarizes and responds to those comments, outlines the definitions for this final rule, and for some definitions, provides additional interpretation to assist readers in understanding the final definition (see section 791.301, "Definitions"). BIS notes that multiple commenters requested BIS include definitions for terms that are already defined within 15 CFR 791.1, such as U.S. person. In response, BIS emphasizes that definitions contained in 15 CFR 791.1 apply to this subpart, except where the same term is defined differently in this rule.

1. Automated Driving System

In the NPRM, BIS proposed *Automated Driving System (ADS)* 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. After considering commenters' feedback, BIS has chosen to retain this definition in the final rule.

Many commenters requested clarity on the definition of *ADS*, particularly urging BIS to explicitly reference SAE International's J3016 standard in the definition. Commenters also

recommended that BIS explicitly exclude Levels 1 and 2 of the SAE J3016 standard or plainly state that the regulation does not capture ADAS in the definition. Similarly, BIS received feedback to incorporate language that excludes hardware and software that are not capable of performing the entire dynamic driving task and to provide examples of these exclusions, such as steering, braking, acceleration, and speed.

BIS declines to include a reference to the current version of SAE J3016 at this time and believes that the current definition adequately covers only those systems that would fall into SAE categorization Level 3 and above. However, this does not preclude BIS from amending this rule in the future to make explicit reference to the current version (April 2021) or any future version of J3016. BIS emphasizes that in enforcing this rule, it will only consider Automated Driving Systems that meet the full definition of this rule to be in scope, and BIS believes that the details regarding the specifics of Levels 3, 4, and 5 systems contained within J3016 are useful guidance for connected vehicle manufacturers to determine if their products fall within scope. Following the effective date of this rule, entities that seek clarification if a specific piece of software is subject to the prohibitions of this rule may submit a request for an advisory opinion from BIS. Further, in response to commenters requesting that BIS explicitly state that ADAS is out of scope, BIS believes this to be unnecessary as the definition aligns with SAE J3016, which differentiates between ADAS and ADS.

Comments contained various positions on the specific exclusion or inclusion of LiDAR and other sensing systems within the prohibitions. Several commenters advised BIS to identify examples of specific components that are outside the scope of the prohibitions, such as radar and camera technology. Others advocated for the inclusion of ADS sensor technology in the prohibitions and explained that BIS should explicitly scope the prohibitions to include cameras, radar, LiDAR, Time of Flight internal sensors, ultrasonic sensors, and microphones. Commenters pointed out that LiDAR is proliferating across critical infrastructure industries and heavily sourced by foreign adversaries, further urging that LiDAR, in particular, should fall in scope of

the prohibitions, including LiDAR hardware, software for sensor control, and perception software.

BIS maintains its position from the NPRM that this rulemaking will address only ADS software and not the multiple hardware systems that support or directly enable ADS operation. BIS agrees that proliferation of LiDAR and other sensing technologies from entities with a foreign adversary nexus throughout multiple critical infrastructure sectors may pose a threat to national security. However, within the limited scope of the automotive sector, and with this initial rulemaking, BIS assesses that a prohibition that focuses specifically on transactions that provide ADS software is appropriate at this time to mitigate the national security risks that they present while limiting the supply chain and economic impact. As stated in the NPRM, BIS is proposing to regulate ADS software rather than the hardware components of ADAS and ADS so as to reduce unnecessary economic impacts and supply disruption. The hardware that enables ADAS and ADS varies widely between different OEMs. 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. 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. Commenters should also refer to the discussion below on covered software for greater detail on BIS's decision to omit LiDAR from this rule. BIS's decision not to focus on sensing technologies in this rule does not preclude BIS from addressing them in a subsequent rulemaking.

Commenters recommended providing definitions for terms within the *ADS* definition, such as "operational design domain." BIS declines to specify a definition for operational design domain as it believes this to be an industry standard term in the autonomous vehicle sector that refers to

operating conditions under which an ADS or feature thereof is specifically designed to function. Additionally, BIS hopes to provide industry with additional flexibility to interpret these terms within the contexts of their own technologies, reducing the compliance burden of the rule. However, BIS emphasizes that the related definitions in J3016 are useful guidance for industry and interested entities.

One commenter also advised removing "for a completed connected vehicle" from the definition of *ADS* and adding an "ADS-equipped vehicle" to the definition to avoid industry confusion because not all connected vehicles will have ADS. BIS maintains that the ADS-related prohibitions of the rule affect only completed connected vehicles that are equipped with ADS by the nature of how the covered software prohibition is crafted, and therefore narrowing the definition of ADS to remove "for a completed connected vehicle" is not necessary.

Commenters noted that the ADS definition includes hardware, while the prohibited transactions do not include ADS hardware. The ADS definition captures the whole of ADS, including hardware, while the regulation prohibits only ADS software and does not prohibit ADS hardware. Commenters advised removing "hardware" from the definition of ADS or providing language that clarifies that the definition of ADS generally describes what an ADS is, but not necessarily what aspects of the system are regulated by this rule. After consideration, BIS declines this suggestion. In the interest of maintaining a harmonized definition that is consistent with other Federal regulations and with industry standards such as NHTSA's Second Amended Standing General Order 2021-01 and SAE J3016, BIS maintains that inclusion of "hardware" in the definition of ADS is appropriate, even though this does not mean that the hardware of an ADS system is regulated. The structure of the covered software definition and the covered software prohibitions are the only instances of a use of the ADS definition and make clear that ADS hardware is not prohibited when designed, developed, manufactured, or supplied by entities owned by, controlled by, or subject to the jurisdiction or direction of the PRC.

One commenter requested that BIS clarify that ADS software that carries out only a single function, such as parking, be excluded from the definition of ADS. While BIS generally believes that systems that are not capable of executing the entire dynamic driving task (as required by the definition of ADS) are not covered by this regulation, BIS declines to amend the definition in this rule as such a determination would be highly fact specific. BIS emphasizes that persons seeking greater clarity may, upon the effective date of this rule, seek an advisory opinion from BIS regarding a specific transaction involving ADS software.

2. Completed Connected Vehicle

In the NPRM, BIS proposed to define *completed connected vehicle* as follows: "a connected vehicle that requires no further manufacturing operations to perform its intended function. For the purposes of this subpart, the integration of an ADS into a connected vehicle constitutes a manufacturing operation for a completed connected vehicle." BIS chose to retain this definition of *completed connected vehicle* in the final rule based on comments, further research, and other changes to the regulation.

Some commenters, particularly from the commercial vehicle sector, argued that the proposed rule did not provide a clear definition of completed vehicle within the context of the commercial market. As discussed in the following section addressing the definition of connected vehicle, BIS recognizes the substantial compliance concerns associated with the complex commercial vehicle sector and has determined that the commercial vehicle sector will not be covered by this rulemaking. Recognizing there are substantial national security concerns in the commercial vehicle market, BIS intends to issue a new proposed rule specifically tailored to this sector.

One commenter urged BIS to substitute a new definition for "ADS-equipped connected vehicle" instead of "completed connected vehicle" in order to avoid implying that all connected vehicles contain ADS software. BIS recognizes that not all connected vehicles are ADS-equipped. However, BIS declines this suggestion because the prohibitions resulting from the regulation pertain to completed connected vehicles, as defined by the regulation, and BIS does

not want to engender confusion or suggest that the prohibitions pertain only to products equipped with ADS. Therefore, BIS chooses not to integrate this recommendation into the final rule.

3. Connected Vehicle

In the NPRM, BIS proposed *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. BIS modified its definition in the final rule based on comments from the public.

A few commenters requested clarifications or refinements for BIS's definition of a "connected vehicle." Some commenters highlighted that other regulatory bodies, such as National Highway Traffic Safety Administration (NHTSA) and the Environmental Protection Agency (EPA), often implement separate rulemaking efforts for light/passenger vehicles and heavy/commercial vehicles. BIS has opted to exclude commercial vehicles from the final rule. As discussed elsewhere, BIS emphasizes that the national security risks associated with PRC or Russian VCS and ADS in commercial vehicles are grave, and BIS's decision to exclude commercial vehicles from this rulemaking in no way implies that these risks are lesser than in the passenger vehicle market. Rather, BIS intends to propose a separate regulation tailored to the commercial sector in the coming months.

Specifically, BIS has amended the definition of "connected vehicle," for the purposes of this rule, to exclude vehicles with a gross vehicle weight rating (GVWR) of over 10,000 pounds, which generally aligns with the weight delineation included in definitions used by other government agencies (including the Federal Motor Carrier Safety Administration) and by industry to delineate between passenger and commercial vehicles.

One commenter also requested that BIS clarify that recreational vehicles (RVs) are not included in the definition of a "connected vehicle." BIS declines to amend the definition as it believes RVs will largely be excluded from the regulation. First, as amended, RVs weighing over 10,000 pounds will not be captured by this rule and will instead be subject to an intended future rule covering commercial vehicles. Second, as the commenter noted, BIS intends to issue a general authorization pertaining to vehicles used on public roads for fewer than 30 days a year, which could capture additional RVs that weigh under 10,001 pounds, if manufacturers are able to verify their RVs are eligible. Manufacturers availing themselves of any future general authorization need not notify BIS of its use nor apply for the authorization, contrary to the comment's suggestion. In the future, BIS may consider whether a general authorization that specifically addresses RVs would be appropriate.

One commenter requested that BIS explicitly exclude agricultural equipment, construction equipment, and mining equipment from the definition of "connected vehicle." BIS does not believe this modification necessary as it believes the existing definition of "connected vehicle," which mandates that the vehicle must be manufactured "primarily for use on public streets, roads, and highways," and under 10,001 pounds, sufficiently excludes these vehicles from the provisions of the rule. Another commenter urged BIS to clarify that the rule does not apply to entities importing VCS hardware intended for integration into vehicles that are not covered by this rule. BIS believes that modifications to the definition of VCS and VCS hardware address this comment.

Commenters urged BIS to amend the definition of "connected vehicle" to clarify that Personal Delivery Devices (PDDs) and bicycles are not captured by the rule. BIS does not believe this modification is necessary as it does not believe PDDs nor bicycles meet the definition of a connected vehicle. PDDs and bicycles primarily operate in shoulders of roads, bike lanes, and sidewalks, which BIS does not believe meets the definition of "manufactured primarily for use on public streets, roads, and highways." The exclusion of these devices from

this regulation is further in line with Federal and State-level interpretations that have also excluded PDDs from the definition of motor vehicle and related policies.

Commenters asked that BIS clarify whether a "connected vehicle" includes a motorcycle. One commenter offered the definition of motorcycle from 40 CFR 205.151: "[A]ny motor vehicle, other than a tractor, that: (i) [h]as two or three wheels; (ii) [h]as a curb mass less than or equal to 680 kg (1499 lb); and (iii) [i]s capable, with an 80 kg (176 lb) driver, of achieving a maximum speed of at least 24 km/h (15 mph) over a level paved surface." BIS understands and acknowledges that this definition of motorcycle fits into its definition of "connected vehicle" in this rule, meaning that motorcycles are subject to this regulation, and BIS believes that an additional definition is unnecessary to improve ease of administration of this rule. Further, BIS notes that vehicles such as electric scooters and e-bicycles are not "manufactured primarily for use on public streets, roads, and highways," given that in most jurisdictions such vehicles cannot be ridden legally on public highways and many roads. Therefore, BIS assesses that the definitions provided are scoped appropriately.

One commenter asked BIS to clarify that the regulation does not apply to VCS hardware importers and connected vehicle manufacturers that import covered hardware intended for assembly into vehicles that are not covered by the definition of connected vehicle. In response, BIS confirms that transactions involving covered software and VCS hardware that are not integrated into a connected vehicle are not subject to this regulation. VCS hardware importers and connected vehicle manufacturers executing covered software and VCS hardware transactions that are intended to be incorporated into a connected vehicle, as defined in the final rule, are subject to this regulation.

BIS has chosen 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. For the purposes of this subpart, a connected vehicle with a gross vehicle weight rating of more than 4,536 kilograms or 10,000 pounds is not included in this definition.

The primary change from the definition in the proposed rule is the inclusion of a weight constraint. This final rule has been narrowed to address vehicles under 10,001 pounds (which largely apply to the passenger vehicle market). BIS intends to supplement this rulemaking with an additional rule to address vehicles over 10,000 pounds (which largely applies to the commercial vehicle market), given the national security risks.

4. Connected Vehicle Manufacturer

In the NPRM, BIS proposed "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. Based on feedback from commenters, BIS has amended its definition of "connected vehicle manufacturer" in the final rule.

Commenters advised BIS to be more specific about who is responsible for reporting to BIS under this regulation. Commenters recommended that BIS clarify that contracting with another party to manufacture or assemble a completed connected vehicle that integrates one's own ADS or VCS for one's own business is out of scope of the regulation. BIS declines to do so. Through modifications to the *connected vehicle manufacturer* definition, BIS specifies that a person whose sole manufacturing or assembly operation is integrating ADS into an otherwise completed connected vehicle would qualify such a person as being a "connected vehicle manufacturer." BIS also included changes to the definition of *sale* to ensure that these contracting operations are within scope of the regulation. As discussed further below relating to the modifications to the definition of *sale*, BIS has determined that contracting operations could, but may not necessarily, be a sale under the terms of this rule.

Commenters encouraged BIS to consider whether 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, should be subject to the prohibitions in the rule and need to obtain a specific authorization before importing or selling that completed connected vehicle in the United States. BIS determined that such integration of ADS software into a completed connected vehicle by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia is an extension of the national security risk relating to covered software and intended to be restricted. In response, BIS clarifies that ADS integration into an otherwise completed connected vehicle is subject to this regulation and has updated the definition of connected vehicle manufacturer in the final rule to reflect this.

Commenters also encouraged BIS to make third-party manufacturers or assemblers operating on behalf of a U.S. entity, regardless of the origin of the ADS or VCS, exempt from this regulation. BIS rejects this request and has updated the regulation to clarify that third-party manufacturers who are persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia are subject to this rule. Third-party manufacturers are an integral aspect to a connected vehicle manufacturer's overall manufacturing operations; therefore, if such third parties were persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, this would continue to perpetuate the national security risks that this rule is seeking to address.

In the final rule, BIS has chosen to define a *connected vehicle manufacturer* to mean a U.S. person who:

(1) Manufactures or assembles completed connected vehicles in the United States for sale in the United States;

(2) Imports connected vehicles for sale in the United States; and/or

(3) Integrates ADS software on a completed connected vehicle for sale in the United States.

A connected vehicle manufacturer may also be a VCS hardware importer, as defined herein, if VCS hardware has already been installed in a connected vehicle when the connected vehicle manufacturer imports it.

This modified definition clarifies BIS's intention to capture entities who purchase otherwise completed (and compliant) connected vehicles from a third party and then integrate their proprietary ADS on the vehicle to enable autonomous driving. For example, a U.S. person who purchases completed connected vehicles from a U.S. connected vehicle manufacturer (even if those vehicles do not contain PRC or Russian VCS hardware or ADS software) and then integrates its own ADS software on the vehicles would be performing a manufacturing operation and would be explicitly captured as a connected vehicle manufacturer under this amended definition. If that U.S. person is an entity owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, it would require a specific authorization to sell those vehicles in the United States, which includes transferring those vehicles for commercial operations. The modified definition also clarifies that the first paragraph of the definition, which relates to persons who manufacture or assemble completed connected vehicles in the United States, applies only if the vehicles are intended for sale in the United States (not for export and sale abroad).

5. Covered Software

In the NPRM, BIS proposed to define *covered software* as "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." Based on comments, BIS changed its definition of *covered software* to better align with industry practices.

Commenters commonly sought more guidance on the layers of software regulated under the rule. Commenters requested examples regarding how covered software applies to the software stack for VCS and ADS. Common feedback urged BIS to define software-based components that fall in and out of scope of the regulation, such as application, firmware, middleware, and system software. Commenters also encouraged BIS to provide a definition of these layers of software, particularly emphasizing that a definition was needed for firmware. Commenters advocated for the exclusion of embedded software (*e.g.*, middleware and system software) because the application software more directly facilitates external communications, and the embedded software is not divisible or distinguishable from hardware. Commenters also suggested that regulating embedded software would introduce more complex supply chain bottlenecks and prevent many companies from meeting the covered software prohibition within a year's time.

In response to these comments, BIS has added specificity to the *covered software* definition to explicitly include application, middleware, and system software, while continuing to exclude firmware. BIS has also included a description of firmware. BIS declined to generally exclude embedded software from the definition, because doing so would exclude certain software that could pose a national security risk. Rather, BIS has chosen to classify software along "application," "system," "middleware," and "firmware" categories. To determine whether particular embedded software is excluded from the definition, parties should consider whether the embedded software leverages specific code executed by the primary processing unit or units of the system. This requirement may exclude embedded software systems that are executed on ancillary surface modules or processors, depending on the specific architecture of the VCS.

Two commenters recommended that BIS limit covered software to *only* the application layer. BIS rejects this feedback. BIS intends covered software to include application software, operating system software and a library of established functions which are generally referred to

as “middleware.” BIS chose to include operating system and middleware function software in the definition of “covered software” because if either the operating system or middleware functions are compromised, the resulting application would not execute securely. So long as the software in question is application, operating system, or middleware executed by the primary processing unit of the subject system, it would likely be covered software unless otherwise excluded.

One commenter requested that BIS define the term “primary processing unit” in the “covered software” definition. BIS declines to incorporate an explicit definition in the regulatory text because a definition is unnecessary; unlike other specialized terms defined in the final rule, “primary processing unit” is a generally widely understood term. To provide additional interpretive guidance on the term, BIS intends the term “primary processing unit” to encompass the central or graphics computing unit of a system responsible for running both the application(s) and the associated operating system that directly enable VCS or ADS on the vehicle. Commenters supported the exclusion of open-source software from the rule and requested BIS align the definition of open-source software with the definitions from the National Defense Authorization Act (NDAA) of 2019, CISA 2023 Open-Software Security Roadmap, and the Open Source Initiative. Commenters also wanted BIS to clarify if open-source software modified by Russian or Chinese entities falls under scope of the regulation. BIS accepts the recommendation of multiple commenters to align the definition of open-source software with that of the 2019 NDAA. Further, BIS added certain clarifying clauses to the 2019 NDAA definition to address advances in artificial intelligence and the evolution of the use of the term “open-source” in artificial intelligence applications by including “in its entirety” to the definition. However, BIS declines to limit the open-source software exclusion by the geographical location of specific administrators or contributors to open-source projects or libraries. BIS is not well placed to arbitrate the validity of individual open-source contributors and rather relies on the inherent structure and transparency of open-source software to identify potential security compromises by malicious actors. BIS excludes open-source software from

covered software and characterizes it as software for which the human-readable source code is available in its entirety for use, study, re-use, modification, enhancement, and redistribution by the users of such software unless that open-source software has been modified for proprietary purposes and not redistributed or shared.

In addition to BIS being more specific about the definition of *covered software*, commenters requested that BIS explicitly scope out different software components. Some commenters recommended modifying the definition to cover only component software of ADS and VCS. These commenters argued that tying the covered software to the hardware helps narrow the scope and removes the ambiguity of the term "item that supports," which they argued was ambiguous because it is generally understood as part of a system. To this end, commenters advised BIS to define "covered software" as "software, in which there is a foreign interest, executed by the primary processing unit of the Vehicle Connectivity System or Automated Driving System item that directly enables the Vehicle Connectivity System or Automated Driving System function," or similarly. Commenters argued that marrying the definitions of VCS and ADS to the definition of covered software provides clarity to connected vehicle developers and other automotive industry actors while retaining BIS's stated goal of targeting "two integral ICTS systems," of VCS and ADS, and no other vehicle equipment or technologies. Commenters also said this change removes the language "an item that support the function of VCS," which is confusing to industry.

In response to these comments, BIS clarified the definitions of "covered software" and "VCS hardware" to include items that "directly enable" the function of those systems as opposed to "supports" those systems. BIS defined the term "item" in conformity with SAE International's 21434 "Road Vehicles – Cybersecurity Engineering" standard of September 2021, as a term that would be commonly understood by industry. The SAE 21434 standard promotes the delineation of item definitions for different automotive systems and for assessing the cybersecurity of those systems. BIS therefore considered the SAE 21434 terms and practices in drafting its definitions

so that connected vehicle manufacturers can consult existing compliance mechanisms to determine the item definition of different systems and assess what is included within the item definition of a VCS. BIS also retained "covered software" and "VCS hardware" as separate terms and separate prohibitions due to other structural and legal considerations.

Commenters also wanted to better understand the granularity of the ADS software prohibition, seeking clarity as to whether final software is considered "designed" or "developed" by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC when a software module from the PRC is part of the larger ADS suite. If only one software subcomponent of an ADS software suite is designed, developed, manufactured, or supplied by a PRC or Russian entity, then the entire ADS software suite would be considered designed, developed, manufactured, or supplied by a foreign adversary entity. BIS modified the *covered software* definition to make clear that it applies to software components of application, middleware, and system software. BIS acknowledges the burden of determining the provenance of software subcomponents for legacy code bases and therefore added an exclusion for code that was designed, developed, manufactured, or supplied before one year from the effective date of the rule.

One commenter requested clarity about VCS software architecture, specifically regarding whether the regulation's scope includes upstream communication transfer, downstream communications transfer, and communications processing. This commenter thought that upstream communications were within scope of the proposed rule, while the downstream communication transfer and communication processing were out of scope. Some commenters requested specific opinions about specific automotive in-vehicle network architectures. Because of the variety and diversity of automotive network designs, BIS sought to provide definitions that could be applied across the industry and declines to specifically opine on specific architectures. However, BIS intends to work with industry to answer specific questions during the implementation of the rule and through the issuance of advisory opinions.

Commenters commonly sought clarity on the degree and type of remedy necessary for the software to no longer be deemed covered software and therefore not subject to the prohibitions and compliance requirements in this rule. To this end, commenters recommended that BIS consider integrating accepted international regulatory standards to drive its guidance. For example, commenters suggested that BIS adopt the ISO/SAE 21434 Road Vehicles-Cybersecurity Engineering Threat Analysis and Risk Assessment (TARA) to assess the cybersecurity risks in automotive products. Commenters flagged that this standard provides a methodology for the software developer to identify critical assets and privacy concerns and allows for the greatest specificity to address the critical asset(s), such as the specific lines of source code or module at issue, rather than broadly including all software packages. BIS appreciates this recommendation and acknowledges that it previously considered such a framework. BIS ultimately declines to consider compliance with SAE 21434 as a standalone security control sufficient for mitigating the national security risks identified in this rule. BIS determined that a combination of security controls could successfully mitigate the national security risk relating to connected vehicles and intends to use a multi-layered approach when issuing a specific authorization. BIS anticipates that requiring security features controls such as conformity with cybersecurity standards, audits conducted by third parties or BIS, enhanced reporting requirements, and controls on corporate governance may be effective ways to manage risk. However, BIS will consider compliance with cybersecurity standards like SAE 21434, R155, and NHTSA Cybersecurity Best Practices when evaluating applications for specific authorizations.

Many commenters requested that BIS exclude legacy code from the definition to minimize supply chain disruption and ensure warranties can be fulfilled. BIS acknowledges comments regarding the mature code bases that have been built, audited, and refined over time and the significant burden that determining the specific developers that contributed to those libraries over time would create. Based on the comments, BIS incorporated a specific exclusion within the

covered software definition for legacy code. This addition to the covered software definition will exclude all source code that is designed, developed, manufactured, or supplied before a date that is one year from the effective date of the rule. This "legacy" code exclusion will protect products that have already gone to market. Furthermore, excluding legacy code designed, developed, manufactured, or supplied prior to March 17, 2026 will provide regulated entities time to transfer intellectual property rights as well as responsibility for development and maintenance of code to within their organizations in order to come into compliance with the covered software prohibition. BIS believes that this appropriately balances addressing the national security risks posed by software that is actively maintained in the PRC and Russia while lowering potential burdens and disruptions to the market.

Commenters also warned that the regulation does not clearly articulate if ADS added to a completed connected vehicle falls in scope of the prohibition. Commenters advised limiting the scope of the regulation by adding language at the end of the *covered software* definition to ensure that the addition of ADS software that itself is not designed, developed, manufactured, or supplied by PRC or Russian entities to a connected vehicle is not a manufacturing operation for the purposes of this rule. BIS declines to adopt this recommendation. BIS explicitly included the sentence, "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," to make clear that the addition of ADS to a completed connected vehicle falls within scope of this rule as it is a manufacturing operation for a completed connected vehicle. If the addition of covered ADS software to a completed connected vehicle involves software in which there is no foreign interest, then the integrating entity would not be required to submit a Declaration of Conformity. However, if there is a foreign interest in that covered software transaction, then it would require a Declaration of Conformity, or in the case the software is covered by the prohibitions of this rule, a specific authorization. BIS assesses that the addition of covered ADS software to a completed connected vehicle by an aftermarket vendor poses the same national

security threat as the addition of covered ADS software at the initial point of manufacture. BIS believes such a modification or integration of ADS software could introduce the same underlying risk that the connected vehicle can be manipulated, to include unauthorized access to vehicle data.

Commenters also inquired if electronic logging devices (ELDs), insurance-related vehicle tracking devices, and after-market safety technologies are in the scope of covered software. BIS recommends that commenters review the technical specifications of these devices against the updated definition of *covered software* to confirm if they are executed by the primary processing unit or units of an item that directly enables the function of VCS or ADS at the vehicle level to determine if said devices fall within the scope of the definition of covered software. BIS believes the definitions for *covered software* and *VCS hardware* should provide clarity; however, a person may submit a request for an advisory opinion regarding transactions involving specific technologies, along with technical information related to these technologies, so BIS may provide an opinion specific to the technology presented. BIS understands "after-market safety technologies" to be broad and can encompass a range of varying technologies. Such technologies would likely be covered as they relate to ADS software directly; however, uses outside of this scope would likely require BIS to receive additional information within a request for an advisory opinion. While the use of these technologies in the commercial vehicle market is out of scope of this regulation, under certain circumstances these technologies may be subject to this regulation (*e.g.*, if they are used in vehicles weighing less than 10,001 pounds).

Commenters wanted BIS to define "integrated or attached hardware or software" to clarify whether software or hardware attached by a Bluetooth device or USB to a vehicle would be subject to the rule, or if the rule includes only integrated technologies. Per its definitions, this final rule is not limited to integrated technologies.

Commenters advised BIS to reconsider the zero percent threshold for software containing code from prohibited foreign entities, such as a de minimis threshold. BIS chose to not adopt a

de minimis threshold approach due to the risk of circumvention that it would create. For example, entities could add additional code to make their percentage of prohibited content appear to fall below the minimum threshold. This suggestion would not adequately mitigate the risks identified. Additionally, seeking to create an implementable de minimis standard of code, wherein code could be analyzed by various metrics such as per bit, per line, per execution command, per library, etc., would be extremely complex, and the associated difficulty of assessing whether content is de minimis or not would be inefficient and ineffective. Furthermore, BIS added a significant exclusion in the "covered software" definition by excluding all code that had been designed, developed, or supplied prior one year from the effective date of this rule. This legacy code exclusion, paired with the infeasibility and ineffectiveness of a de minimis threshold led BIS to reject this suggestion.

A commenter urged BIS to require companies to implement cybersecurity requirements for edge cloud architecture and to establish domestic or allied sourcing requirements for ADS cloud infrastructure, as well as continuous monitoring of ADS cloud and edge systems. BIS addresses its considerations for cybersecurity requirements in its discussion of Declarations of Conformity, as well as other places in this text. Cloud architecture and infrastructure are out of scope of this current regulation. However, BIS understands the concern and may consider this area for future rulemaking.

Commenters recommend that BIS consider narrowing the *covered software* definition, or the annual reporting requirement, to exclude covered software produced by companies based in trusted or allied nations. Commenters suggest that this change would both streamline connected vehicle manufacturers' reporting obligations and reduce the burden on BIS in reviewing vast quantities of submitted information and allow BIS to focus its resources and efforts on overseeing the use of software-based components in completed connected vehicles that may present actual or heightened risks to U.S. security. One commenter was particularly concerned that not narrowing the foreign interest scope meant that all technology must be sourced from a

U.S. vendor, limiting global supply chains to using only U.S. software. BIS addresses these concerns in its discussion of Declarations of Conformity more in depth. At a high level and as explained in more depth below, BIS will not exclude non-foreign adversary nations from the scope of covered software, because BIS assesses that it is necessary to address the threats posed by interconnected but opaque supply chains writ large, as opposed to finished products imported from non-foreign adversary nations.

Commenters urged BIS to establish a process that would allow an OEM to fully own software purchased from a prohibited supplier so that the purchased software would not be considered prohibited. BIS is willing to discuss such an approach through an advisory opinion request to determine whether such a software purchase may adequately mitigate the identified risk if the transaction is not otherwise excluded by the modified definition of covered software.

In this final rule, BIS has chosen to define *covered software* to mean the software-based components, including application, middleware, and system software, in which there is a foreign interest, executed by the primary processing unit or units of an item that directly enables the function of 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 directly controlling, configuring, and communicating with that hardware device. Covered software also does not include open-source software, which is characterized as software for which the human-readable source code is available in its entirety for use, study, re-use, modification, enhancement, and redistribution by the users of such software, unless that open-source software has been modified for proprietary purposes and not redistributed or shared. Covered software also does not include software subcomponents that were designed, developed, manufactured, or supplied prior to March 17, 2026, as long as those software subcomponents are not maintained, augmented, or otherwise altered by an entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary after March 17, 2026.

With this definition of *covered software*, BIS focused on both the functional characteristics of the software that it intends to regulate as well as the common industry terminology used to refer to that software. For example, BIS acknowledges that there is not a bright line between application-level software, middleware (*e.g.*, device drivers, database management functions), and firmware. However, by combining both industry terminology and a functional definition in its definition of *covered software*, BIS seeks to provide two levels of clarity. In making a reasonable, good faith determination of whether a software subcomponent falls within the *covered software* definition, entities should refer to the architecture of the product to assess whether the software component would be generally considered "application" level software based on industry practice using established methodologies like AUTOSAR software component definitions or ISO 26262 guidelines. When there is uncertainty, entities should consider whether the primary processor (*e.g.*, a central processing unit, a graphics processing unit) processes the executables, or whether the software is executed by a peripheral microcontroller. If the primary processor does not execute the software, and the software would not be classified as application software by an industry standard like AUTOSAR, it is unlikely the software would qualify as application software for the purpose of this definition.

BIS has also provided examples to clarify what constitutes application, middleware, and systems software below. If regulated parties have questions about what constitutes covered software in specific cases, they may request an advisory opinion.

Example 1: A U.S. person licenses automotive software from a vendor who is a foreign person that is owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. The automotive software the U.S. person licenses includes a message processing application that receives a digital message from a peripheral radio device, processes that message, and uses the information within that message to issue a digital control command to a related electronic control unit. This software would be considered application software. Because the licensed software includes application software designed, developed, manufactured, or

supplied by an entity owned by, controlled by or subject to the jurisdiction of a foreign adversary, the licensed software would be prohibited, unless it qualifies for a general or specific authorization granted by BIS.

Example 2: A U.S. person licenses automotive software from a vendor who is a foreign person that is owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. The automotive software the U.S. person licenses includes a software device driver intended for use in the operating system for applications to activate and utilize specific VCS hardware. This driver would be considered middleware. Because the licensed software includes middleware designed, developed, manufactured, or supplied by an entity owned by, controlled by or subject to the jurisdiction of a foreign adversary, the licensed software would be prohibited, unless it qualifies for a general or specific authorization granted by BIS.

Example 3: A U.S. person licenses automotive software from a vendor who is a foreign person that is owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. The automotive software the U.S. person licenses includes a software component in the operating system that coordinates communications between distributed applications and between applications and an internal reference database. This software component would be considered middleware. Because the licensed software includes middleware designed, developed, manufactured, or supplied by an entity owned by, controlled by or subject to the jurisdiction of a foreign adversary, the licensed software would be prohibited, unless it qualifies for a general or specific authorization granted by BIS.

Example 4: A U.S. person licenses automotive system software from a vendor who is a foreign person that is owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. The automotive system software the U.S. person licenses is a proprietary real time operating system that manages system resources as well as task scheduling, prioritization, and synchronization for an automotive system. This software component would be operating system software. Because the licensed software includes operating system software designed,

developed, manufactured, or supplied by an entity owned by, controlled by or subject to the jurisdiction of a foreign adversary, the licensed software would be prohibited, unless it qualifies for a general or specific authorization granted by BIS.

Example 5: A U.S. person purchases a V850 CAN controller from a vendor who is a foreign person. The V850 CAN controller includes a software subcomponent that is embedded into the controller's non-volatile memory and directly enables the transmission and receipt of analog electric signals by interacting with the VCS hardware system's application software. This software component would be considered firmware. Assuming no other facts, this purchase does not involve covered software and would not be affected by the covered software prohibition (but may be affected by the VCS hardware prohibition, depending on other facts and circumstances of the transaction).

BIS determined that it was necessary to exclude firmware because firmware is often shipped with and designed in coordination with the provision of automotive hardware subcomponents. Therefore, while there are similar national security and cybersecurity risks at the firmware level, BIS determined that a firmware prohibition would be tantamount to a hardware prohibition. Finally, BIS made slight modifications to the open-source software definition from the 2019 National Defense Authorization Act when crafting the "covered software" definition. These minor modifications are to make clear that large language models or neural networks that may bill themselves as "open source" but do not openly share their source code or training data in their entirety do not meet the commonly held definition of open-source software. Furthermore, the clause appended to the end of the definition is redundant but meant to emphasize that if an open-source product is modified outside the limits of the open-source license and not shared, the resulting product is definitionally not open source. However, modification would not include integration into an existing code base by engaging with an open-source product's application programming interface, permissible customization within the terms of the open-source license, or selection of modular sections of the open-source product while excluding others.

In light of comments the agency received, BIS emphasizes that regulated entities are not absolved of conducting due diligence on open-source software when that open-source software has been modified outside the scope of its license. Additionally, BIS declines to introduce a static list of approved or excluded open-source software libraries and tools into the text of the rule, as these libraries and tools are dynamic by nature. BIS will maintain and update compliance information on its website and will also be available to work with regulated entities through advisory opinions or compliance education and outreach programs.

BIS included the term "item" within its definition of *covered software* because industry standards define "item" as a scoping boundary when analyzing specific automotive systems for cybersecurity and functional safety requirements to ensure that assessments are targeted and comprehensive. For example, ISO 21434's threat analysis and risk assessment methodology for assessing cybersecurity relies on "item definition" boundaries. Entities seeking additional guidance on the term "item" in this context may find it helpful to refer to its use in ISO 21434 and ISO 26262, and its use by automotive cybersecurity and safety professionals when making a reasonable determination whether a component is part of a covered software system item. Comments about this term are further explained in the "item" subsection of this Definitions section. BIS has incorporated specific language to ensure that legacy parts are not subject to the covered software prohibitions of this regulation. This "legacy" code exclusion in covered software protects products that have already gone to market. By incorporating a one-year timeline, BIS allows regulated entities time to transfer intellectual property rights as well as responsibility for development and maintenance of code within their organizations to come into compliance with the covered software prohibition.

6. Declarant

In this final rule, BIS includes a new definition for "declarant" to mean the U.S. person submitting a Declaration of Conformity to BIS. BIS has included "declarant" in the final rule text to provide more clarity in the regulation since the term is used throughout.

7. FCC ID Number

In the NPRM, BIS proposed defining the term "FCC ID Number" to mean 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. Commenters provided no feedback about this particular definition. BIS retains its definition in the final rule.

While commenters did not provide feedback on the definition of "FCC ID Number," they provided input in how the regulation incorporates them. Commenters pointed out that not all VCS hardware items have FCC Numbers. Taking this point into consideration, BIS will only require an FCC ID Number if known by the submitting party. This change is reflected in 791.305 of the regulation text, which discusses Declarations of Conformity.

8. Foreign Interest

In the NPRM, BIS proposed to define "foreign interest" to mean any interest in property of any nature whatsoever, whether direct or indirect, by a non-U.S. person. Many commenters encouraged BIS to narrow its definition of foreign interest or otherwise provide greater clarity. After consideration of these comments, BIS retains this definition of *foreign interest* in the final rule.

Several commenters, for example, requested that BIS clarify this definition to mean a legally cognizable interest in property. BIS declines to limit this definition to a legally cognizable interest because "legally cognizable" may be overly narrow for purposes of this regulation. Moreover, BIS's approach retains consistency with other IEEPA-based programs, which similarly use a broad definition of "foreign interest." Some commenters suggested that requiring a legally cognizable interest would address the scenario in which the only foreign interest in software is the fact that foreign persons worked on the development of the software. In response, BIS notes that a foreign interest must be an interest in property, and the sole fact a foreign individual worked on a software development team would not meet this requirement unless

additional factors (such as ongoing financial or beneficial interests or contractual rights) are present.

Multiple commenters encouraged BIS to carve out allied persons from the definition of *foreign interest*, defined as citizens of, residents of, or corporations incorporated in nations in "Country Group A" of BIS's own Export Administration Regulations. BIS declines to amend the definition of foreign interest to exclude certain allied nations or to grant preferential status for entities in allied nations as this would inadequately mitigate the national security risk this rule seeks to address. The mere fact that a connected vehicle manufacturer is headquartered in, incorporated in, or otherwise organized under the laws of a non-foreign adversary country does not imply that the manufacturer has appropriate practices in place to address the risks identified by this rule. For example, a connected vehicle manufacturer located in a non-foreign adversary country may actually be controlled by a PRC or Russian entity, or the manufacturer sources design and development of its ADS software or VCS hardware from an entity located in or controlled by the PRC or Russia. However, the fact that a transaction has a foreign interest does not mean that the transaction is prohibited. Rather, the presence of a non-PRC and non-Russian foreign interest in a transaction without the requisite foreign adversary nexus would require the connected vehicle manufacturer or VCS hardware importer to submit a declaration of conformity, a requirement that BIS has substantially streamlined in this rule to facilitate compliance and reduce the burden on regulated entities. BIS is separately working to identify if any security standards or best practices exist, or may be developed, that will sufficiently mitigate this national security risk and allow companies, wherever located, to engage in transactions without need to notify BIS through a Declaration of Conformity.

One commenter also urged BIS to ensure that software developed in the PRC or Russia by wholly owned subsidiaries of U.S. companies would not be considered to contain a foreign interest. BIS declines to create an exemption for software developed by wholly owned subsidiaries of U.S. businesses from the definition of foreign interest. As articulated in this rule,

entities operating in the PRC or Russia are subject to the jurisdiction and control of the PRC or Russian governments, even if wholly owned by a U.S. or allied entity. These types of entities, despite their ownership, are subject to the regulations and laws of the PRC or Russia that could obligate them to comply with information or access requests resulting in undue or unacceptable risks, as discussed in Section IV of this rule.

One commenter stated that BIS's broad definition of *foreign interest* would mean that a publicly traded company with some foreign shareholders would be required to submit a Declaration of Conformity even if the company's covered software itself contained no foreign interest. In response to this comment, BIS has introduced an exemption for the submission of Declarations of Conformity for those transactions where the *only* foreign interest in the product arises from a foreign entity's equity ownership in a U.S. person. This exemption is narrowly tailored intentionally to minimize the compliance burden. BIS continues to understand equity ownership to be a form of foreign interest. However, BIS recognizes that attaching a static percentage foreign interest threshold would be particularly challenging for regulated entities and their compliance teams in practice. For example, shareholders change daily, and while there are some reporting requirements for principal shareholders according to Regulation D of the Securities Exchange Act of 1934, setting a percentage threshold based on equity ownership alone would mean there could be no reporting obligations for a transaction one day and foreign interest that required a Declaration of Conformity. To avoid this outcome, BIS clarifies through this exemption that Declarations of Conformity are not required for transactions where the *only* foreign interest arises from foreign equity ownership of one of the U.S.-based parties to a transaction. If the foreign equity ownership is paired with another foreign interest (*e.g.*, degree of control over the U.S. entity or licensing of intellectual property), a Declaration of Conformity would be required. To provide further clarity regarding transactions involving foreign interest as a result of public shareholder ownership, BIS offers the following examples.

Example 6: Company A develops VCS. Company A is incorporated in the United States and is publicly traded on the New York Stock Exchange. No foreign entity owns more than 5% of Company A's common stock. Assuming no other facts, because no foreign entity shareholder of Company A's common stock can materially affect Company A's operations and corporate management, there is not a foreign interest in Company A's VCS. As such, the sale of completed connected vehicles incorporating Company A's VCS does not require a Declaration of Conformity.

Example 7: Same facts as previous example, except Company A is headquartered in a foreign jurisdiction. The import of completed connected vehicles incorporating Company A's VCS software from a foreign jurisdiction would require a Declaration of Conformity because the import gives rise to a foreign interest independent of equity ownership.

Example 8: Company A develops VCS software, is incorporated in the United States, and is publicly traded on the NASDAQ Stock Exchange. Company A states that one of its shareholders is a foreign person holding 60% of Company A's outstanding shares and is not a person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. Assuming no other facts, because a foreign entity is a shareholder whose holding is such that the foreign entity can materially affect Company A's operations and corporate management, there is a foreign interest in Company A's VCS software other than equity ownership. As such, the sale of completed connected vehicles incorporating VCS software developed by Company A requires submission of a Declaration of Conformity.

Example 9: Company A is incorporated in the United States and is publicly traded on a U.S. stock exchange. In aggregate, foreign shareholders hold 28 percent of Company A's outstanding shares. These shareholders have an informal agreement to act in concert with respect to voting decisions for Company A. The collective 28 percent would allow such foreign shareholders to block resolutions and important decisions regarding Company A's management. The foreign shareholders have an interest in Company A's VCS software independent of their equity

ownership by virtue of their control over the company. As such, the sale of completed connected vehicles incorporating VCS software developed by Company A requires submission of a Declaration of Conformity.

Example 10: Company A, a U.S. person completed connected vehicle manufacturer, purchases ADS software from Company B. Company B is a U.S. person publicly traded company that designs, develops, and manufactures its ADS software solely in the United States. A foreign entity holds 15% of Company B's outstanding public shares. The foreign investor has no board seat and exerts no management or control over Company B. Assuming no other facts, Company A is exempt from the requirement to file a Declaration of Conformity.

Another commenter requested that BIS clarify that foreign IP claims, which may not be recognized under U.S. law, do not constitute a foreign interest. BIS declines to insert language that would require an extensive inquiry into the legal status of IP claims in multiple jurisdictions in order to determine whether a foreign interest is present. BIS notes that there may be situations, such as where a foreign IP claim is frivolous, in which the foreign IP claim would not constitute a valid interest. The commenter suggests revising the definition of *foreign interest* to add that it does not include "legal claims or other allegations, or rights that might be afforded by law even when all other rights have been assigned to another party, such as employee-inventor remuneration obligations and moral rights in works of authorship." BIS believes that many such claims would fall outside of the scope of *foreign interest.* For example, rights that cannot legally be transferred might not meet the definition of "property." BIS does not believe it necessary to amend the definition to specify this point or to provide an exhaustive list of claims that are not included under the definition of foreign interest. If regulated parties have a question about whether a foreign IP interest constitutes a foreign interest in specific cases, they may request an advisory opinion from BIS.

Multiple commenters also requested that BIS amend the provisions on the import of VCS hardware to clarify that a Declaration of Conformity is required only when the VCS hardware

itself contains a foreign interest. Others suggested that BIS remove the foreign interest requirement from the definition of *covered software*. BIS declines to make these changes. As discussed in the NPRM, IEEPA requires a foreign interest in the property that BIS seeks to regulate. BIS has included a foreign interest requirement in the definition of *covered software* because some prohibited covered software transactions are sales that occur within the United States. By requiring a foreign interest in the definition of *covered software*, BIS ensures that this rule only captures those sales covered by IEEPA. By contrast, this rule prohibits imports (not sales within the United States) of VCS hardware. BIS assesses that items crossing into the United States from a foreign jurisdiction will necessarily contain a foreign interest by nature of the transaction, and therefore does not find it necessary to include a foreign interest requirement in the definition. Additionally, the final rule does not require a Declaration of Conformity to be submitted if the only foreign interest related to covered software resides in open-source or legacy code.

After considering all comments, BIS has retained the definition of *foreign interest*, when used with respect to property, to mean 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 of the item itself, intellectual property present in the item, a contractual right to use, update, or otherwise impact the property, (*e.g.*, ongoing maintenance commitments, any license agreement related to the use of intellectual property), profit-sharing or fee arrangement linked to the property, as well as any other cognizable interest. This definition is consistent with the definition of "interest" used in the context of OFAC 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.

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,

this rule regulates the importation of VCS hardware, making VCS hardware importers responsible for compliance.

With respect to covered software, based on feedback from connected vehicle manufacturers, automotive suppliers, and other stakeholders, BIS continues to understand that typically, ADS and VCS software are designed or developed to a connected vehicle manufacturer's specification. ADS and VCS software is frequently designed, developed, or supplied by foreign persons, and those persons frequently retain an 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, have obligations to maintain and update the software, or participate in other ongoing contractual arrangements. Such arrangements are among the types of interests that BIS identifies 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, an obligation to qualify for a general authorization or seek a specific authorization under this final rule. BIS therefore will regulate covered software by regulating the importation or sale of completed connected vehicles, making connected vehicle manufacturers responsible for compliance.

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, this rule additionally regulates 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; data sharing agreements; intellectual property rights transfers from the U.S. subsidiary to the parent company; cooperation in technological development between the parent and U.S. subsidiary; arrangements by which the parent company directly or indirectly appoints the leadership of the U.S. subsidiary; the ability of the parent company to direct some or all corporate decision making by the U.S. subsidiary; and parent company influence over procurement by the U.S. subsidiary. BIS understands many if not all of these arrangements to be standard for the automotive industry. Additionally, because the PRC and Russian legal regimes discussed in Section IV of this rule 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 provides the following examples to assist in interpreting whether a foreign interest is present.

Example 11: Company A is headquartered in a foreign jurisdiction and is the owner of the code, algorithms, and other design elements in a software development kit (SDK) that is used to develop software used in certain payment systems. Company A provides its SDK to Company B, a U.S. person, who uses it to develop software that is installed in connected vehicles in the United States to provide secure communication and payment with transportation infrastructure. Even though Company A has no legal property interest in the software itself, it has an indirect beneficial interest in the use of such software because updates to the software will need to be made using Company A's SDK. Thus, the software Company B develops with Company A's SDK retains a continuing foreign interest.

Example 12: Company A is a wholly owned U.S.-based subsidiary of Company B, a multinational holding corporation incorporated in the British Virgin Islands. Company A imports

products for sale in the United States, which generate revenue. Based on Company B's corporate structure and governance of its subsidiary holding companies including Company A, Company B dictates how Company A's revenue and profits are allocated across Company B's holdings. Because Company B, a foreign person, benefits from each of Company A's domestic transactions and because Company B directs the allocation of revenue generated by those transactions, there is a foreign interest in Company A's domestic United States transactions.

Example 13: Company A is a U.S. based connected vehicle manufacturer. Company B is a parts manufacturer headquartered in a foreign jurisdiction. Company B manufactures systems on chip (SoC) based on customer specifications that are specifically used in VCS. Company A and Company B have entered into a multi-year agreement whereby, among other conditions, Company B will be the exclusive supplier, with rights of first refusal, for replacements and any maintenance and services repairs of SoCs to Company A for the term of the agreement. Because Company B is a foreign entity and because Company A may use no other parts supplier for its VCS SoCs during the term of the agreement, the SoCs that Company B provides to Company A under the agreement retain a continuing foreign interest once those SoCs enter the United States.

Example 14: Company A is a U.S. based connected vehicle manufacturer. Company B is a U.S. subsidiary of a foreign software company, Company C. Company B sells ADS software licenses on behalf of its foreign parent Company C, who holds the intellectual property rights to the software. Company B licenses Company C's ADS software to Company A for system integration and further commercialization within the limits of its licensing agreement. Company C, a foreign entity, will have a continued interest in Company A's use of its software after commercialization.

9. Hardware Bill of Materials

In the NPRM, BIS defined *Hardware Bill of Materials (HBOM)* to mean 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. Public comment provided feedback that led BIS to change the final rule definition of *HBOM*. Commenters provided a variety of opinions on the HBOM requirements of this regulation. Several commenters expressed opposition to the inclusion of HBOMs in Declaration of Conformity submissions on the grounds that they contain highly confidential business information and intellectual property, citing security issues related to storage and transmission. Several commenters noted that the HBOM requirement is overly broad and suggested that they only include "electronic components that execute software." Several commenters recommended that BIS provide a "specific" resource as an example of an HBOM, such as the *HBOM Framework for Supply Chain Risk Management.* Commenters also suggested that BIS remove references to documents and drawings within the HBOM definition to exclude protected intellectual property from compliance submissions. Other commenters requested that BIS provide an HBOM sample model.

After considering the issues raised in these comments, BIS will no longer require the submission of HBOMs as part of Declarations of Conformity. However, BIS will require entities to maintain primary business records related to their certification that due diligence was conducted in analyzing their VCS hardware supply chains, which could include HBOMs. These primary business records must be made available to BIS upon request. BIS has also included a section in the rule dedicated to the submission of CBI, which would cover the submission of HBOMs. BIS will continue to work with industry partners to identify best practices in HBOM development, including templates and advisory documents.

To better align HBOM criteria with industry practices, BIS has modified its definition of *HBOM*. Specifically, BIS has removed documents, drawings, technical information, and descriptive information from the HBOM definition because these elements do not strictly fall under the scope of a bill of materials. This change also addresses industry concerns about the potential exposure of intellectual property and CBI. Additionally, BIS has replaced the term

"comprehensive list" with "formal record" since "record" is a more general term and "comprehensive" is difficult to define precisely.

BIS has chosen to define "Hardware Bill of Materials (HBOM)" as a formal record of the supply chain relationships of parts, assemblies, and components required to create a physical product, including information identifying the manufacturer, and related firmware.

10. Import

In the NPRM, BIS proposed to define the term "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. BIS did not receive comment on its definition of "import" or how the term is used in the regulation text. Therefore, BIS retains the NPRM definition of "import" in the final rule. For clarity, BIS has added a sentence clarifying that the same definition applies to related terms such as "importing" and "imported."

While BIS did not receive any comment on the proposed meaning of "import," one commenter requested that BIS clarify that for the purposes of the regulation, "article" means VCS hardware and covered software as defined in this regulation. BIS is confirming for the purposes of this rule that "article" is referring to VCS hardware and covered software.

11. Item

In the NPRM, BIS proposed to define "item" to mean 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. BIS received a few comments on how this term is used within its regulation text but based on further research chooses to retain this definition of "item" for the final rule. Some commenters urged BIS to replace the term item with "system," both in the context of VCS hardware and covered software to clarify that the terms refer to overall systems. BIS declines this suggestion and maintains the use of the term item. This term is used both in

ISO 26262 and ISO/SAE 21434 to delineate system boundaries. BIS further believes the use of the term item in both covered software and VCS will allow regulated entities to harmonize compliance with this rule with existing cybersecurity and functional security work as dictated by ISO/SAE 21434 and ISO 26262.

12. Knowingly

In the NPRM, BIS proposed to define "knowingly" to mean "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." BIS received no comments requesting changes to this definition and retains this definition for the final rule.

BIS did receive some public comments relating to due diligence and Declaration of Conformity requirements, which are relevant to the context in which the definition of "knowingly" would be applied. Commenters suggested that BIS consider implementing a whitelist of vendors that do not require additional due diligence. According to commenters, a whitelist would provide more clarity on the compliance requirement for regulated entities. One commenter also stated that a whitelist would preclude the need for Declarations of Conformity. BIS declines to create a whitelist at this time. Due to the complexity of connected vehicle supply chains and the multitude of factors involved in each unique transaction undertaken by manufacturers, BIS believes the creation of a whitelist would insufficiently address the national security risks present in the connected vehicle supply chain. However, BIS maintains the flexibility to grant general authorizations for certain types of transactions subject to the prohibitions at a future date.

Several commenters also requested clarity on how far into a supply chain importers are required to maintain visibility. BIS encourages entities to reference the definitions of VCS

hardware and covered software when determining the depth of supply chain due diligence necessary to certify that the VCS hardware or covered software was not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. Based on the definitions provided in this rule, importers would need to conduct due diligence on supply chain components if these components directly enable the function of and are directly connected the VCS systems or are part of an item that directly enable the function of the VCS. Component parts that do not contribute to the communication function of VCS hardware are not considered VCS hardware per the above, and so would not have due diligence requirements.

One commenter suggested that suppliers should be prohibited from importing or selling covered software or VCS hardware linked to the PRC or Russia if they have knowledge that it will be integrated in connected vehicles built for the U.S. market. BIS declines to place the onus of this prohibition on suppliers of VCS hardware and covered software rather than on VCS hardware importers and connected vehicle manufacturers due to the numerous suppliers of the myriad components involved in the VCS hardware and covered software supply chain from which BIS would need to accept specific authorization applications in such circumstances. Instead, through requiring specific authorization applications and Declarations of Conformity from VCS hardware importers and connected vehicle manufacturers, BIS has implemented a more targeted approach, which BIS believes will still create the necessary changes to VCS hardware and covered software supply chains in the interest of national security. However, VCS hardware importers and connected vehicle manufacturers may rely on statements and documentation from suppliers in support of specific authorization applications and Declarations of Conformity so long as all necessary due diligence is documented and made available to BIS (section 791.313, “Reports to be furnished on demand”).

Another commenter asked for clarity that a “regulated entity can wholly and reasonably rely on statements of its tier 1 suppliers that a supplied part or piece of equipment does not contain a

restricted component or subcomponent." As stated above, BIS clarifies that VCS hardware importers and connected vehicle manufacturers may rely on statements and documentation from suppliers in any Declarations of Conformity or specific authorization application. For example, in certifying that regulated entities have conducted due diligence in their covered software and VCS hardware supply chains, entities must also certify that they maintain documentation specifying their due diligence efforts and that they have made arrangements with suppliers to furnish any necessary documentation upon request by BIS (section 791.312, "Recordkeeping"). In making these certifications to BIS, entities may rely on statements from suppliers that a component 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.

13. Model Year

In the NPRM, BIS proposed to define "model year" to mean 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. While many commenters raised issues with the specific model years selected by BIS as the implementation dates for this regulation, none addressed BIS's definition of the term. BIS has addressed concerns over implementation dates further below, under "Exemptions." BIS retains the NPRM definition of "model year" in the final rule.

Several commenters raised the concept of vehicle generations and highlighted that connected vehicle manufacturers do not conduct a major refresh of vehicle technologies every year. Rather, vehicle generation refreshes may only take place every four to six years. As discussed further below, BIS understands that the implementation dates for the rule may fall mid-generation for many connected vehicle manufacturers. In this situation, BIS would consider issuing a time-bound specific authorization in cases where connected vehicle manufacturers are able to demonstrate that they are moving into compliance with the rule for the next vehicle generation refresh. BIS may also contemplate allowing a phased-in implementation of the prohibitions, as

advocated for by some commenters, in a specific authorization for manufacturers mid-generation during the implementation period. Please see the specific authorizations section to learn more about how a phased approach can occur under this regulation.

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

In the NPRM, BIS proposed to define "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" to mean:

> "(1) Any person, wherever located, who acts as an agent, representative, or employee, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign adversary or of a person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary;
>
> (2) Any person, wherever located, who is a citizen or resident of a foreign adversary or a country controlled by a foreign adversary, and is not a 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."

BIS has retained this definition in its final rule. However, it has provided further examples on how to apply this definition below.

Example 15: 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 16: 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 17: 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 18: 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 19: 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 20: 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 10 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 21: 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 "controlled by" and "subject to the direction" of the PRC or Russia.

Example 22: 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 23: 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 24: The PRC or Russian government, through an investment fund, acquires a 1 percent 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 25: 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 26: 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.

Example 27: 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.

Example 28: Company A is an automobile company based in a jurisdiction that is not the PRC or Russia. Company A maintains a supervisory committee established by the company's articles of association that is responsible for supervising the management of the company and is not part of the board of directors. Each member of the committee exercises significant managerial authority over the nature, scope, and attributes of the company's business. An independent member of this committee has known ties to the government of the PRC and

previously served as board director for a PRC state-owned enterprise. Since Company A's supervisory committee contains a member that can affect important matters of the company, has ties to the PRC government, Company A is subject to the direction of the PRC.

For additional clarity for determining what is and what is not designed, developed, manufactured, or supplied by the entities mentioned above, BIS offers the following examples below.

Example 29: Company A is a U.S. person. Company B is headquartered in the PRC and is a fabless semiconductor design company that produces systems on chips for vehicle telematics systems. Through a joint development agreement, Company A collaborates with Company B to design a custom cellular microcontroller for integration into a VCS hardware unit that will be imported into the United States. Assuming no other facts, Company A's VCS hardware unit contains components designed by an entity that is subject to the jurisdiction of the PRC. The import of the VCS hardware unit is a prohibited transaction, unless authorized by a general authorization or specific authorization.

Example 30: Company A is a U.S. person. Person B is a PRC citizen residing in the PRC. Company A contracts with Person B to conduct a cybersecurity review of its operating system software design for a piece of VCS hardware that is imported in the United States. Person B completes that review and recommends improvements and changes to Company A's product, which Company A is free to accept or reject. Person B's review of Company A's software does not mean Company A's covered software product was designed by an entity subject to the jurisdiction of the PRC solely on the basis of Person B being a PRC citizen.

Example 31: Company A is domiciled in the PRC and is a joint venture between Company B and Company C. Company B is headquartered in the United States. Company C is headquartered in the PRC. Company A sources suppliers, including suppliers of VCS hardware and covered software, integrates parts into automotive systems, and conducts prototyping and testing for future model year connected vehicles that Company B will eventually import and sell into the

United States. Assuming no other facts, the connected vehicles that Company A prototypes and tests contain VCS hardware and covered software supplied by an entity subject to the jurisdiction of the PRC. Company B's import or sale of the vehicles is a prohibited transaction, unless a general authorization or specific authorization applies.

Example 32: Company A is a PRC company that is an automotive contract assembler and manufacturer for connected vehicles. Company B is an automotive company headquartered in the United States. Company A assembles and manufactures completed connected vehicles, including installing the VCS hardware and covered software, in another country, that Company B will eventually import into the United States. Company B's connected vehicles contain VCS hardware and covered software supplied by an entity that is subject to the jurisdiction of the PRC. Importing the vehicles into the United States is a prohibited transaction, unless a general authorization or specific authorization applies.

Example 33: Company A is an automotive parts company that is domiciled in the PRC or Russia. Company B is a U.S. person. Company A buys VCS hardware that integrates covered software, then customizes and packages that VCS hardware for sale to and import by Company B into the United States. Assuming no other facts, the VCS hardware supplied by Company A is supplied by an entity subject to the jurisdiction of the PRC or Russia. The import of the VCS hardware into the United States is a prohibited transaction, unless a general authorization or specific authorization applies.

For additional clarity in determining whether a transaction involving VCS hardware or covered software designed, developed, manufactured, or supplied by entities described above is prohibited under the final rule, BIS offers the below examples. In offering these examples, BIS emphasizes, and has further clarified this language in the prohibitions, 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 based solely on the country of citizenship of one or more natural persons who are employed by,

contracted by, or otherwise similarly engaged in such actions through the entity designing, developing, manufacturing, or supplying the VCS hardware or covered software. In particular, BIS confirms that visa holders in the United States would not be considered persons controlled by the PRC or Russia solely based on their citizenship.

Example 34: 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 final 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 final rule, unless it qualifies for a general authorization or a specific authorization from BIS.

Example 35: 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 vehicle would be a prohibited transaction under the final rule unless it qualifies for a general authorization, or a specific authorization granted by BIS.

Example 36: A U.S. person imports a completed connected vehicle, making the U.S. person a connected vehicle manufacturer under the final 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 final rule, the import of the completed connected vehicle would be prohibited unless it was authorized by a general authorization or a specific authorization.

Example 37: 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 final rule unless it qualifies for a general authorization or specific authorization.

Example 38: 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 and contractual and licensing rights 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 and the existence of an ongoing foreign interest (*i.e.*, servicing obligations and contractual and licensing rights), the sale of a completed connected vehicle within the United States that integrates this proprietary covered software would be a prohibited transaction under the final rule, unless it qualifies for a general authorization or specific authorization.

Example 39: 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 the rare circumstance where Company A did not participate in the design or development of the covered software or VCS hardware, Company A would submit a Declaration of Conformity for the import of the completed connected vehicles containing covered software and VCS hardware, identified by make, model, and VIN series. 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 final rule, and a specific authorization from BIS would be required before engaging in such a transaction.

Example 40: 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, Company A's sale of the completed connected vehicles is a prohibited transaction under the final rule, and a specific authorization from BIS would be required before engaging in such a transaction.

Example 41: Company A is a company that, through any of the scenarios detailed above, is deemed to be owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. Company A purchases otherwise completed connected vehicles from Company B, a U.S. company that is not owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. Company A transforms these vehicles into autonomous vehicles by integrating hardware and software, including ADS software, on these vehicles. Company A is thus a connected vehicle manufacturer under this rule. Company A seeks to offer a commercial robotaxi service by which customers are able to use a mobile application to hail one of Company A's vehicles incorporating ADS software. Because Company A is a connected vehicle manufacturer owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia and seeks to offer a commercial service utilizing completed connected vehicles

incorporating ADS, Company A would require a specific authorization from BIS prior to engaging in such a transaction.

Many commenters recommended that BIS further clarify that, under the rule, VCS hardware or covered software would not be considered as designed, developed, manufactured, or supplied by entities with a nexus to the PRC or Russia if individual contributors holding PRC or Russian citizenship work on the hardware or software outside of the PRC or Russia. Commenters expressed similar concerns about visa holders from the PRC or Russia working in the United States. BIS agrees that participation by individual contributors holding PRC or Russian citizenship outside of the PRC or Russia should not alone make VCS hardware or covered software subject to the prohibitions in this rule because this scenario presents a lower national security risk than other situations addressed by this rule. BIS has addressed this point in paragraph (b) of section 791.302 (prohibited VCS hardware transactions) and paragraph (c) of section 791.303 (prohibited covered software transactions). BIS further highlights in the examples below.

Example 42: 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 jurisdiction or direction of a foreign adversary," assuming no other facts, paragraph (c) of the section 791.303 (Prohibited covered software transactions) makes clear that 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 final rule.

Example 43: Company A is a European automotive company. Company B is a supply chain consultancy that is domiciled in Singapore and is majority owned by a PRC citizen. Subject to a non-disclosure agreement, Company B reviews Company A's automotive design specifications and recommends specific hardware and software suppliers to Company A. Company A considers Company B's recommendations and obtains hardware or software from the recommended suppliers directly (not through Company B). Assuming no other facts, Company B's review and recommendation of Company A's covered software and VCS hardware suppliers does not mean those products are developed by an entity subject to the jurisdiction of the PRC. The import or sale of Company A's vehicles in the United States would not be a prohibited transaction, but a VCS hardware importer or connected vehicle manufacturer that imports or sells the vehicles into the United States must comply with any applicable Declaration of Conformity requirements.

To provide further clarification, BIS has added examples to this final rule, such as Example 30, Example 42, and Example 43, to explain that citizenship of natural persons involved in the manufacture or design of a product is not itself determinative of a product being designed, development, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. These examples also help explain the prohibitions described in Section VI subsection (b) *Prohibitions on Certain Transactions Related to Connected Vehicles.*

Numerous commenters urged BIS to provide greater clarity as to the criteria by which regulated entities should deem a person to be owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. Several commenters recommended that BIS adopt the criteria described by the Department of Justice's (DOJ) NPRM, *Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons* (89 FR 86116, October 29, 2024), which uses a fifty percent threshold for ownership as one criteria for an entity to be a "covered person", or adopting a more conservative ownership threshold of 25 percent, as stipulated by the Department of Energy's

(DOE) Foreign Entity of Concern (FEOC) rules. BIS rejects these suggestions and retains the current definition as published in the NPRM because it retains consistency across all ICTS transactions reviewed by BIS under 15 CFR Part 791 Securing the Information and Communications Technology and Services Supply Chain. By contrast, each of the other U.S. government programs identified by commenters differs and addresses national security risks unique to their mandates and missions. For instance, DOE's final guidance applies to the Battery Materials Processing and Manufacturing grant program, authorized by section 40207 of the Bipartisan Infrastructure Law, Public Law No. 117-58, and the 30D Clean Vehicle tax credit created under the Inflation Reduction Act, Public Law No. 117-169, which imposes limits on when an entity's battery supply chain includes FEOC. DOE's final guidance was issued to aid stakeholders in identifying FEOCs in their battery supply chains rather than those entities involved in supply chains related to VCS and ADS. DOJ's NPRM on *Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons* also differs in that it prohibits and restricts certain transactions that could allow persons from countries of concern access to bulk sensitive personal data or to U.S. government-related data. Additionally, BIS rejects the recommendation to define ownership thresholds. While BIS recognizes that thresholds may provide a bright line for industry, BIS maintains that connected vehicle supply chains are complex and opaque, with varying ownership structures of OEMs and connected vehicle suppliers. Bright-line thresholds alone can be limited when dealing with an entity with a PRC or Russia nexus and one who may circumvent the prohibitions by adjusting its ownership structure, while still retaining corporate control or executive management that may be subject to the direction of the PRC or Russia. Retaining the current definition of *owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia*, will allow BIS to address the evolving and unique national security risks across a variety of supply chains for distinct industries, as articulated in Section IV of this rule. Additionally, one commenter requested that BIS further clarify the meaning of *subject to the*

direction in this definition. This commenter expressed concern that "direction" diverges from common industry understandings of ownership and control, and that it could be interpreted to include a one-time event. BIS retains the definition of *person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary*, which is consistent with the scope of E.O. 13873 and reflects the possibility that a person may act at the direction of a foreign adversary in situations in which typical corporate ownership or control may not be present. BIS considers "subject to the direction" to typically entail a continuous and ongoing relationship between a regulated person and the PRC or Russian government or entities subject to the jurisdiction of the PRC or Russian government.

One commenter maintained that the ultimate ownership structure of an entity should not subject that entity to the prohibitions of the rule, and the location of covered software and VCS hardware design should instead be determinative. BIS reiterates the threat outlined in the NPRM and in this final rule that entities owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia may be compelled to provide logical access to their VCS hardware or covered software resulting in the exfiltration of sensitive data or remote manipulation of the vehicle. While the location of covered software and VCS hardware design and development, as well as corporate structure and security practices, will play an important factor in BIS's decision to issue specific authorizations, BIS declines to amend the rule in response to this comment.

15. Prohibited Transactions

In the NPRM, BIS proposed *prohibited transactions* to mean collectively, the transactions described in section 791.302 (Prohibited VCS hardware transactions), section 791.303 (Prohibited covered software transactions), or section 791.304 (Related prohibited transactions) of this subpart. BIS did not receive any comments directly about this definition. Feedback on prohibited transactions focused on the transactions described in the body of the regulation text. To review the comments and responses on the prohibited transactions in this rule, please review

Section VI subsection (b) *Prohibitions on Certain Transactions Related to Connected Vehicles* below.

16. Sale

In the NPRM, BIS proposed *sale* to mean 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*. Some commenters recommended that BIS clarify and revise the definition of sale. Commenters highlighted differences between the commercial vehicle market and the passenger vehicle market and emphasized that the NPRM *sale* definition is inadequately scoped for the commercial vehicle market. BIS, after taking all comments into consideration, retained this definition in the final rule but made a related change to the definition of *connected vehicle* to focus on the passenger market by limiting the scope of this final rule to vehicles under 10,001 pounds.

One commenter recommended that BIS clarify that contracting with a third party to manufacture one's own completed connected vehicles with one's own VCS or ADS does not constitute a sale. In response, BIS believes that such a transaction could, but would not necessarily always, constitute a sale, and such a determination would depend on the specifics of the arrangement, including the chain of custody or legal rights over the vehicle while with a third-party manufacturer. BIS generally believes that it is not in the national security interest of the United States to categorically exempt third-party manufacturing from the prohibitions of this rule. For example, the rule would prohibit the sale of completed connected vehicles manufactured by an entity that is owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, even if that manufacturing is on behalf of a U.S. connected vehicle manufacturer. In this scenario, BIS believes the integration of VCS hardware or covered software by that manufacturer constitutes the "supply" of such ICTS by a prohibited entity.

Whether or not the actual transfer of the vehicles from the third-party manufacturer to the U.S. connected vehicle manufacturer occurred would depend on the specifics of the transaction, but if there is a foreign interest in the software (*e.g.*, ongoing contractual arrangements or IP rights), the ultimate sale of those vehicles in the United States would be prohibited. However, if, for example, the third-party manufacturer incorporates prohibited ADS software that is designed, developed, manufactured, or supplied by a PRC or Russian entity, the subsequent transfer of those vehicles to any entity for commercial operations would be prohibited.

One commenter claimed that the definition as written could be interpreted to impose compliance duties on dealers who sell but do not manufacture or import connected vehicles. As written, the prohibitions of the rule apply only to the sale of a completed connected vehicle by a connected vehicle manufacturer. Given that dealers do not perform manufacturing operations on vehicles to transform an incomplete connected vehicle into a completed connected vehicle (nor do they integrate ADS onto an otherwise completed connected vehicle), the sale of vehicles from a dealer to a consumer would not be captured by any of the prohibitions of this rule. BIS emphasizes that instead, given both the definition of *sale* and the prohibitions contained in this rule, it is the sale by the connected vehicle manufacturer to the dealer that would be prohibited if the VCS hardware or covered software is designed, developed, manufactured, or supplied by an entity owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, or if the connected vehicle manufacturer itself is such an entity. In this case, it is the connected vehicle manufacturer that is subject to the prohibition, and it is the connected vehicle manufacturer that would be subject to civil or criminal penalties should they knowingly violate these prohibitions. As such, BIS stresses that this rule places no additional compliance responsibilities on dealers.

17. Software Bill of Materials

In the NPRM, BIS proposed to define *software bills of materials (SBOM)* to mean 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. Based on public comment, BIS has altered its definition of *SBOM* and modified its compliance requirements with respect to SBOMs.

Commenters provided feedback on what BIS should include in the criteria for an SBOM, suggesting how its definition should be changed in the final rule. Multiple commenters recommended that BIS align its *SBOM* definition to the National Telecommunication and Information Administration's (NTIA) "The Minimum Elements for a Software Bill of Materials" (Minimum Elements for an SBOM), a report written in collaboration with the Department of Commerce and authorized under President Biden's E.O. 14028, "Improving the Nation's Cybersecurity," 86 FR 26633 (May 12, 2021), which identifies the prevention, detection, assessment, and remediation of cyber incidents. Many commenters recommended referencing NTIA's Minimum Elements for an SBOM in BIS's SBOM definition. Another commenter specifically advised removing the "component hash" requirement in BIS's SBOM definition to match the NTIA's Minimum Elements for an SBOM. Commenters also recommended revising the definition to only require the detailed elements "if available."

Based on the numerous comments received, BIS opted to align the SBOM definition with the NTIA Minimum Elements for an SBOM requirements rather than reference them directly to avoid any confusion should the NTIA definitions change. In addition, BIS has removed several SBOM elements (*e.g.*, version string, component hash, package URL, and unique identifier) from the minimum documentation requirements necessary to apply for a Declaration of Conformity or specific authorization. BIS declines to add "if available" to the SBOM requirements included in the final rule with the understanding that this regulation is prospective, allowing industry the opportunity to ensure these minimum requirements are met for any covered

software transaction. These changes also reflect comments arguing that the NPRM definition requires information that may be beyond the detail provided by automated scanning tools and would create burdens for manufacturers, and cautioning BIS that industry did not have sufficient time to gather SBOMs as defined in the NPRM by model year 2027. By reducing the minimum documentation requirements for an SBOM, as described above, and removing the requirement to submit an SBOM with Declarations of Conformity (*see* Section VI.c.1), BIS has significantly reduced the compliance burden for industry, including for small entities. BIS has significantly reduced the compliance burden for industry, including for small entities.

One auto manufacturer recommended that BIS replace "supplier's name" and "author's name" with "person's name" in the definition. While BIS has removed the required baseline software attributes from the definition of SBOM, including the requirements for author's name and supplier name, it declines to replace the term "supplier" and "author" with "person" in the context of SBOMs throughout the remaining regulatory text based on the understanding that a "supplier" or "author" may be either an entity or person. Additionally, this language is inconsistent with E.O. 14028 and NTIA's Minimum Elements for an SBOM, on which BIS bases its SBOM definition. Another commenter stated that if BIS intends for SBOM requirements to include open-source software within covered software, that this be specified in the definition by adding "including open-source software used in covered software, even if the open-source software is outside the definition of covered software." In alignment with the removal of the SBOM submission requirement, BIS will only require retention of minimal documentation related to products for which a Declaration of Conformity is submitted, including documentation or third-party assessments sufficient to identify, at minimum, the author name, timestamp, component name, and supplier name of all proprietary additions to the development of the covered software.

Commenters provided other feedback about how to use and process SBOMs. A commenter highlighted how SBOMs could be useful to BIS in variety of ways, including: verifying if known

vulnerabilities exist using the CPE (Common Platform Enumeration) in the unique identifier against the NVD (National Vulnerability Database); ensuring the supplier names listed in the SBOMs do not match any entity under foreign adversary control, as defined by the proposed rule; confirming that component hashes match those generated from package URLs to verify source code integrity; and using dependency relationships to provide specific guidance to entities on scope to address for achieving conformity when issues arise with identified components. This commenter also recommended that BIS allow a flexible SBOM update method that can be integrated into the frequent software update typical for VCS and ADS without disrupting development cycle. BIS appreciates this feedback; however, given its decision to not require SBOMs at this time, BIS will not take action on these recommendations. NBIS has chosen to define "Software Bill of Materials" or SBOM as a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open-source and commercial software components. The SBOM enumerates these components in a product.

18. United States

In the NPRM, BIS proposed *United States* to mean 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. Commenters did not provide feedback on this definition. BIS retains this definition for its final rule.

19. Vehicle Connectivity System

In the NPRM, BIS proposed *Vehicle Connectivity System (VCS)* to mean 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. Public comments informed BIS's modification of *VCS* definition for the final rule, which includes explicit hardware and software exclusions.

Numerous commenters provided feedback on BIS's proposed definition for *Vehicle Connectivity System*. Many commenters urged BIS to narrow the definition to exclude specific radio frequency bands, functions, or devices. Comments regarding specific VCS hardware devices are discussed in the next section, "VCS Hardware."

Multiple commenters took issue with the proposed rule's threshold of 450 MHz and argued that this cutoff is overly broad. For example, some commenters recommended that BIS include an upper limit for the radio frequency band in order to scope out certain ultra-wideband automotive applications, such as some key fobs. Other commenters encouraged BIS to scope out certain convenience functions such as garage door opening or rear seat entertainment. Several commenters also encouraged BIS to explicitly scope out systems that connect internally within the vehicle, supply power to the VCS, exchange data with the VCS, authenticate a user to access or drive a vehicle, or localize a device intended to control vehicle functions.

In response to these comments, BIS has amended the definition of *VCS* to include a variety of function-based exclusions to exclude certain low-risk use cases and provide industry with greater flexibility. BIS declines to implement an upper bound for the radio frequency as this would unnecessarily constrain the definition of *VCS* as automotive technology evolves. BIS has accepted the majority of recommendations to exclude certain functions, including automotive sensing (which includes LiDAR, radar, cameras, and ultrawideband); global navigation satellite system (GNSS); and satellite, AM, and FM radio. BIS declines to exclude convenience functions given the difficulty in adequately defining this exemption to address only convenience functions rather than communications functions that present undue risk. Further, many of the "convenience" functions referenced by the commenters are simply systems that use VCS to accomplish a non-driving task, often by communicating non-expressive data with an external device. BIS added a number of VCS exclusions that may exclude certain "convenience" functions, but declines to categorically exclude them all, as the term is broad and eludes concise definition. BIS further believes that the amended definition of *VCS hardware*, particularly the

replacement of "supports" to "directly enables," renders unnecessary the exclusion of internal vehicle communications or an exemption for systems that simply exchange data with the VCS. While BIS believes that this amended definition excludes features that enable vehicle access and user authentication, BIS declines to exclude the hardware and software that enable the localization of a device intended to control vehicle functions, as the vehicle-side hardware and software of that function presents a possible threat vector that could enable the national security risks spelled out in this rule.

A commenter recommended that the definition of *VCS* be restricted to the electronic control unit or part of an item that supports the VCS external communications capability. Restricting the definition of *VCS*, and therefore *VCS hardware*, to solely the electronic control unit or "telematics control unit" would be overly narrow and would leave many other components that also support wireless communications that could enable long-range cybersecurity exploits. For example, if an infotainment module or a battery management system included a cellular module for its own wireless communication, those modules could be considered VCS but would not be covered by a regulation that only focused on an "ECU." Furthermore, major subcomponents of ECUs that are software programmable often retain connectivity with their OEMs and continue to receive software updates throughout their lifecycle. Therefore, BIS determined that addressing connectivity systems at the ECU level only would be insufficient.

Commenters urged BIS to clarify the definition of *VCS* by clarifying that (1) a system that may convert or process radio frequency communications at a frequency over 450 megahertz, but that does not both receive and transmit data either to or from the vehicle, is outside the scope and (2) a system that does not both receive data from external sources and transmit data to an external source is outside the scope. In response to this comment and others that raised similar issues, BIS modified the definition of *VCS* to add a number of functional exclusions, one of which excludes unidirectional communication systems. However, a subcomponent within an item that directly enables the function of transmission, receipt, conversion, or processing of a

connectivity item would nonetheless be defined as *VCS* even if that subcomponent has only an internal, unidirectional communication purpose. One commenter urged BIS to modify the *VCS* definition to clarify that: "Items that are either for wired frequency communications (*e.g.*, USB port, OBD port) or for the purpose of distance positioning or imaging only are exempted (*e.g.*, Ultra-Wide Band (UWB), cameras, and sensors including LiDAR and radar)." BIS understands that wired-frequency communications-related hardware may also pose risks, but they are not as significant as those defined in the final rule's definition of *VCS*. BIS accepts this recommendation in part and has modified the *VCS* definition to define specific function-based exclusions, including on that explicitly excludes sensor hardware.

Commenters recommended that the *VCS* definition align with the Federal Communication Commission (FCC) equipment authorization regulations. BIS attempted, wherever able, to conform and harmonize with preexisting standards in both the automotive and telecommunications industries. In this case, aligning the VCS definition with the scope of the FCC's equipment authorization definition would be overly broad, as the FCC requires declarations of conformity or certification for products that BIS did not intend to be VCS, including unintentional radiators, as defined by 47 CFR § 15.3. To keep the definition as narrow as possible to address only those items and components necessary to mitigate the identified national security risks, BIS decided not to rely on the FCC equipment authorization program's scope.

One commenter suggested that BIS amend this term to "Vehicle Communication Device," believing that the term would provide industry with greater clarity on covered items. BIS has decided to retain the original Vehicle Connectivity System term and believes that "Vehicle Communication Device" would unnecessarily constrain covered components, including unintentionally excluding major VCS subcomponents that could directly pose a national security risk as outlined in this rule. However, BIS believes that other changes to the definitions of *Vehicle Connectivity System* and *VCS hardware* substantially address the intent behind this

comment. BIS also rejects commenters recommendation to define system. Another commenter urged BIS to reconsider its prohibitions on vehicle connectivity given the U.S Department of Transportation's efforts to deploy Vehicle-to-Everything (V2X) technology. This commenter argued that the proposed rule unnecessarily risks delaying V2X deployments and undermines local, state, and federal investments into V2X infrastructure deployment. BIS appreciates this comment and has been in contact with the Department of Transportation in drafting this regulation. BIS understands that the requirements of this regulation may create new compliance burdens. However, those requirements seek to ensure automotive supply chain security, which will help secure the future of V2X technology implementation.

BIS has chosen to define *Vehicle Connectivity System* or *VCS* as a hardware or software item installed in or on a completed connected vehicle that directly enables the function of transmission, receipt, conversion, or processing of radio frequency communications at a frequency over 450 megahertz. VCS does not include a hardware or software item that exclusively:

(1) enables the transmission, receipt, conversion, or processing of automotive sensing (*e.g.*, LiDAR, radar, video, ultrawideband);

(2) enables the transmission, receipt, conversion, or processing of ultrawideband communications to directly enable physical vehicle access (*e.g.*, key fobs);

(3) enables the receipt, conversion or processing of unidirectional radio frequency bands (*e.g.*, global navigation satellite systems (GNSS), satellite radio, AM/FM radio); or

(4) supplies or manages power for the VCS.

20. VCS Hardware

In the NPRM, BIS proposed *VCS hardware* to mean the following software-enabled or programmable components and subcomponents that support the function of VCS or are part of an item that supports the function of VCS: microcontroller, microcomputers or modules, systems on a chip, networking or telematics units, cellular modem/modules, Wi-Fi microcontrollers or

modules, Bluetooth microcontrollers or modules, satellite navigation systems, satellite communication systems, other wireless communication microcontrollers or modules, and external antennas. VCS hardware does not include component parts that do not contribute to the communication function of VCS hardware. BIS received a variety of comments on VCS hardware that informed the final rule definition.

One commenter encouraged BIS to adopt an entity-based approach, rather than target specific VCS hardware devices, or to introduce an exhaustive list of covered components. BIS declines these suggestions. BIS has determined that an entity-based approach would not adequately mitigate the national security risks outlined in this rule, given the ability of prohibited entities to restructure and ingrain themselves in the connected vehicle supply chain before being subject to an enforcement action by BIS. Rather, a technology-based approach more broadly covers entities of concern and would not require individual enforcement actions against all PRC or Russian suppliers of covered software or VCS hardware. Some commenters requested that BIS clarify that the list of VCS hardware components is exhaustive, meaning any component not included in the definition would not be captured by the prohibition. BIS declines this recommendation as it believes the modifications to the definition of VCS and VCS hardware will allow industry to appropriately identify covered components, and further believes that limiting the definition to a set list of components would not adequately address the potential for changes in nomenclature in the future or address technological developments in which components that are not listed might directly enable VCS functions.

Commenters requested several changes to the *VCS hardware* definition. As with covered software, numerous commenters requested that BIS refine the definition of *VCS hardware* and replace the phrase "support the function of." Most commenters making this point suggested that BIS replace this language with "directly enable the function of" or similar language. BIS accepts this recommendation and believes it will allow industry to more easily identify components that are captured by the *VCS hardware* definition. One commenter requested that BIS remove the

word “subcomponent” from the definition. BIS rejects this recommendation because VCS hardware subcomponents with a nexus to foreign adversaries facilitate the same risk identified in this regulation.

Many commenters encouraged BIS either to explicitly exclude certain VCS hardware devices from the definition, or, in some cases, to explicitly include a set of devices not originally present in the proposed rule’s definition. As referenced above, commenters encouraged BIS to exclude automotive radar from the definition of *VCS hardware* given its safety-critical nature and its inability to communicate independently of the vehicle. As noted, BIS accepts this recommendation and has amended the definition of *Vehicle Connectivity System* accordingly where it has noted this exclusion. Radar hardware is also excluded in the definition of VCS hardware because its primary function is for sensing rather than communications.

Other commenters urged BIS to include LiDAR as a separate category of VCS hardware, contesting BIS’s decision to exclude the technology from the proposed rule. One commenter pointed to outside research assessing that certain PRC manufacturers of LiDAR could insert vulnerabilities into the technology and that the reliance of U.S. connected vehicle manufacturers on PRC LiDAR could pose an unacceptable supply chain risk. In response, BIS reaffirms its decision to exclude LiDAR from the definition of *VCS hardware*. While recognizing that foreign adversary-sourced LiDAR may present certain cyber or supply chain risks, BIS continues to assess that the ADS software is the most appropriate avenue through which to address the potential remote manipulation of a connected vehicle at this time. In general, ADS software is responsible for overseeing the autonomous behavior of the car, processing data from sensors in the car, and executing operations based on that data. In contrast, LiDAR software is merely responsible for analyzing and processing the data collected by LiDAR. BIS recognizes that the scope of both data and control over the vehicle is greater for ADS software than LiDAR software, which is why BIS has prioritized ADS software in this regulation. However, BIS

emphasizes that it may consider LiDAR separately as part of a separate rulemaking effort or investigation under 15 CFR 791.

Commenters specifically asked that components and subcomponents that do not have the ability to process or modify data be removed from the scope of VCS hardware, such as antennas and tuners. In response to these comments, BIS notes that if a tuner is a passive electronic part that is not software programmable, it may not be covered by this regulation. However, if the tuner is a software-enabled and programmable component that directly enables the function of a VCS item then it would likely be defined as *VCS hardware* and thus regulated by this rule. This also applies to one commenter, who requested that BIS clarify that RF switches and passive oscillation components not be included in the definition of VCS hardware. BIS believes that the clarification that VCS hardware must "directly enable" vehicle communication addresses this comment. Other outstanding questions may be answered on BIS's FAQ website page or via an advisory opinion.

Commenters requested that BIS define the terms system and modules. BIS accepts this recommendation in part, as it has defined "system" to the extent it has defined Vehicle Connectivity *System* and Automated Driving *System*. Further, the definition of *item* reflects BIS's stance on the term "system," insofar as a system can be considered an *item* if that system performs a function. Given this portion of the *item* definition, a subsequent definition of "system" would be redundant. With regard to the term "module," BIS again determines that the definition of *item* is sufficient to provide a known industry benchmark that regulated entities may use to delimit the types of components that fall within the regulated systems. Multiple commenters, particularly in the commercial vehicle sector, urged BIS to reconsider the inclusion of aftermarket VCS devices. BIS believes that certain aftermarket devices, specifically those that fulfill VCS functions, pose a significant national security risk when designed, developed, manufactured, or supplied by PRC or Russian entities. BIS does recognize that the inclusion of aftermarket devices poses particular concerns for the commercial sector, and consequently may

consider a separate rulemaking on commercial connected vehicles to address this significant threat in a tailored manner. For the passenger connected vehicle market, BIS emphasizes that aftermarket devices that directly fulfill VCS functions are captured by the VCS hardware prohibition.

Some commenters raised that under the proposed rule, a cellphone that paired with a connected vehicle could be considered aftermarket VCS hardware. BIS believes that the updated definition of *VCS hardware*, particularly the stipulation that the hardware "directly enable the function of" and be "directly connected to" VCS sufficiently clarifies BIS's intent that cellphones not be captured by this rule. VCS hardware includes aftermarket devices not contained in a completed connected vehicle at sale but that are later integrated into the vehicle to perform VCS functions. Conversely, VCS hardware does not include aftermarket devices whose primary function is not to enable vehicle connectivity. For example, mobile phones that are paired with a connected vehicle are not considered aftermarket VCS hardware as vehicle connectivity is not the primary intended function of the device.

Additionally, just as commenters requested legacy software to be excluded from the definition of covered software, other commenters requested BIS exclude legacy hardware, or "as produced" repairs, from the scope of the regulation. BIS rejects adding a legacy hardware exclusion because of the longevity of hardware and completed connected vehicles in general. As such, excluding hardware designed prior to the effective date of the prohibition but imported after the effective date from the scope of this regulation could result in national security risks emanating from such hardware for decades. BIS believes that setting the date in the prohibition for January 1, 2029, or model year 2030 and allowing the import of parts meant for vehicles with a model year prior to 2030 provides a reasonable middle ground. Additionally, BIS assesses that inspecting hardware for embedded vulnerabilities is more burdensome than inspecting software for the same. Legacy hardware could contain persistent undetected vulnerabilities that would continue to enable potential access to or exploitation of vehicles or vehicle data that would be

difficult or impossible to mitigate if scaled across a generation of vehicles. Conversely, regulated entities are more likely to discover such vulnerabilities in software during the continuous cycle of software development and testing, and have the means to patch those vulnerabilities across their fleets. BIS emphasizes that VCS hardware importers may engage in otherwise prohibited transactions so long as (1) the import of VCS hardware not associated with a vehicle model year prior to January 1, 2029, or (2) the import of VCS hardware is associated with a vehicle model year prior to 2030, the VCS hardware is imported as part of a connected vehicle with a model year prior to 2030, or the VCS hardware is imported for purposes of repair or warranty for a connected vehicle with a model year prior to 2030. BIS believes this is sufficient time to adjust VCS hardware supply chains, including for legacy VCS hardware.

BIS defines *VCS hardware* to mean software-enabled or programmable components if they directly enable the function of VCS, or are part of an item that directly enables the function of VCS, including but not limited to: 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 communication systems, other wireless communication microcontrollers or modules, external antennas, digital signal processors, and field-programmable gate arrays. 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, diodes, field-effect transistors, and bipolar junction transistors).

The representative list of VCS hardware included in its definition is not exhaustive but provides a bright line for certain examples where BIS would consider a component to be VCS hardware. 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.

21. VCS Hardware Importer

In the NPRM, BIS proposed *VCS hardware importer* to mean 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. Commenters' feedback led BIS to provide a more specific definition in the final rule.

Some commenters highlighted that the proposed rule's broad definition of both *VCS hardware* and *VCS hardware importer* would capture the import of components whose primary use is not automotive and thus cause severe ancillary effects on other industries. In response, BIS has clarified the definition of *VCS hardware importer* to include only those entities who are importing VCS hardware components that are for use in completed connected vehicles, or that are already incorporated in a connected vehicle (incomplete or completed). BIS further believes that the changes to the definition of *VCS hardware* provide additional clarity on this point.

Other commenters requested that BIS codify its expectation that this definition would capture OEMs and tier one and tier two suppliers. While BIS anticipates that these will be the primary entities who are engaging in the import of VCS hardware components covered by this rule, BIS has opted not to specify this expectation in the rule text given the possibility that other entities may become involved in the import of VCS hardware. BIS emphasizes that parties may submit a request for an advisory opinion on a specific transaction if they are unsure if they qualify as a VCS hardware importer under the terms of this rule.

BIS defines *VCS hardware importer* as a U.S. person who imports:

(1) VCS hardware for further manufacturing, incorporation, or integration into a completed connected vehicle that is intended to be sold or operated in the United States; or

(2) VCS hardware that has already been installed, incorporated, or integrated into a connected vehicle, or a subassembly thereof, that is intended to be sold as part of a completed connected vehicle in the United States.

BIS anticipates that this definition will primarily capture OEMs, tier one, and tier two suppliers importing VCS hardware into the United States. This definition also delineates that only entities importing VCS hardware with an intention of incorporating it into the U.S. automotive supply chain are subject to this regulation, rather than VCS hardware importers providing products to markets beside the auto industry.

b. *Prohibitions on Certain Transactions Related to Connected Vehicles.*

The NPRM proposed to prohibit three categories of transactions: prohibited VCS hardware transactions, prohibited covered software transactions, and related prohibited transactions (collectively described as *prohibited transactions*). In this section, BIS summarizes the prohibitions proposed in the NPRM and examines public comments on them. This final rule largely retains these same prohibitions, but in response to comments, BIS has added additional examples to provide more clarity for the scope of transactions that fall under this regulation. Many commenters also requested that BIS provide greater clarity regarding the definitions of *VCS hardware*, *covered software*, and *foreign interest* so that auto manufacturers can better understand what constitutes a prohibited transaction. Comments on these definitions as well as BIS's efforts to clarify these definitions are discussed above and should be considered in tandem with this discussion.

In the NPRM, BIS proposed the following language identifying prohibited transactions. First, under prohibited VCS hardware transactions, the NPRM stated:

(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."

Second, under prohibited covered software transactions, BIS proposed the following language:

(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 [c]overed [s]oftware."

Finally, BIS proposed the following language addressing 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."

Multiple commenters requested that BIS provide clearer guidance on what constitutes a prohibited transaction, notably (1) to demonstrate the difference between "design" and "develop" (relevant to both the VCS hardware and the covered software prohibitions) and (2) to narrow the

scope of the entity responsible for the "design" or "development" of the item when multiple entities are involved in its creation. BIS acknowledges the need for clear guidance on what constitutes a prohibited transaction and has therefore in response to commenters included new examples in explaining the definitions above to clarify the scope of "design and develop" and the entities responsible.

Several commenters voiced that BIS should narrow the scope of the prohibited transactions. For example, one commenter recommended that the covered software prohibition only apply prospectively and not to software developed prior to the effective date of the rule. Another commenter stated that BIS should exclude embedded software similar to firmware, while another commenter stated that BIS should amend its prohibitions to only prohibit the import of VCS hardware if it is integrated into a VCS or a completed connected vehicle. BIS appreciates these recommendations and has addressed them by clarifying the definitions of ADS, VCS, VCS hardware, and covered software, as described above.

One commenter proposed narrowing the scope of prohibited transactions by adding an exemption to the prohibited transactions for OEMs physically manufacturing connected vehicles in the PRC and Russia if those OEMs met certain security standards such as the independent design of covered software and VCS hardware, verifiable hardware and software integrity, secure key and certificate management, and ongoing monitoring. BIS appreciates this recommendation and may utilize this suggestion when issuing specific authorizations, which are discussed in Section VI.c.3 below. However, BIS believes that such mitigations are more appropriately implemented and monitored on a case-by-case basis and therefore declines the suggestion for a blanket exemption.

Other commenters recommended that BIS expand the scope of prohibited transactions to include BMS, vehicle charging equipment, connectivity apps, edge cloud architecture, and core ADS components to better protect national security. BIS regulates VCS and ADS based on feedback from the ANPRM that eliminates these other areas. For example, ANPRM comments

emphasized that BMS do not have their own connectivity and require communication through a VCS, thereby making VCS a better system for mitigating the identified risks in this rule. BIS also recognizes that the traditional BMS does not have its own external wireless data link, which is why it rejects commenters' recommendation to include BMS at this time. An additional commenter stated that BIS should avoid "politicization" of technical issues and cancel all prohibitions against the PRC in the rule. BIS declines to make this change due to the national security risks discussed in Section IV above.

One commenter requested that BIS clarify with regard to the preamble's "potential regulatory statement" that the prohibition on the sale of completed connected vehicles by connected vehicle manufacturers who are themselves owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia (related prohibited transactions) applies only when the VCS hardware or covered software within the vehicle 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 has amended the rule to clarify that this prohibition applies to all vehicles (with VCS hardware or covered software) sold by these connected vehicle manufacturers given the substantial national security risk posed by the provision of these completed connected vehicles by these entities.

Some commenters asked whether ownership alone, regardless of the location of manufacturing or development, falls under this prohibition. Given the legal authorities laid out in Section IV and the threats stemming from those authorities, BIS assesses that a connected vehicle manufacturer that is owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia creates an unacceptable risk. The risk applies even if manufacturing or design operations are located in the United States or other non-foreign adversary countries, and BIS assesses that the costs of reducing the risk are justified by the reduced risk to national security.

One commenter suggested that ADS hardware should also be prohibited. This commenter suggested that the supply chain disruptions can be reduced by incorporating a phased

implementation, where the prohibitions relating to ADS hardware could be modeled after the VCS hardware exemption. This commenter also emphasized that if ADS hardware is not included in the final rule, industry will have little incentive to develop and manufacture hardware in the United States, leaving the national security risk unmitigated. BIS declines to expand this regulation to prohibit ADS hardware at this time. Much of the hardware that supports or directly enables the ADS function, or that falls within the ADS item definition, are end point sensing devices or internal wired communication devices that often do not have external connectivity. For that reason, BIS maintains that regulating VCS hardware and ADS software is an appropriate means to mitigate the national security concerns at this time. BIS's decision not to include ADS hardware in this rule's prohibitions does not preclude BIS from addressing it in a subsequent rulemaking.

BIS agrees with commenters' focus on the potential impacts of foreign adversary involvement in developing technology for autonomous vehicles and the degree to which PRC and Russian legal and regulatory environments inhibit the transparency that would be necessary to adequately ensure both public safety and U.S. national security. One commenter noted that the lack of data transparency required of PRC autonomous vehicle developers makes it particularly difficult for the public to assess their safety. BIS appreciates this feedback and notes its alignment with its own risk assessment.

After reviewing and considering all of the comments, in this final rule, BIS has adopted prohibitions consistent with the NPRM: (1) VCS hardware importers are 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; (2) connected vehicle manufacturers are prohibited from knowingly selling within the United States, or importing into the United States, completed connected vehicles that incorporate 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; and (3) connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia are also prohibited from knowingly selling in the United States completed connected vehicles that incorporate covered software or VCS hardware, regardless of whether such VCS hardware or covered software is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or control of the PRC or Russia. These connected vehicle manufacturers are also prohibited from offering commercial services in the United States that utilize completed connected vehicles that incorporate ADS.

Because of the role connected vehicle manufacturers play in the design and development of the key components in connected vehicles, which are generally built to the manufacturers' specifications, the third prohibition will often be duplicative of the other prohibitions in this final rule. However, as BIS intended in the NPRM and has clarified in this final rule, the third 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. Additionally, in the NPRM, BIS intended to prohibit persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia from integrating ADS onto otherwise completed connected vehicles and offering them for commercial services, to include rideshare or robotaxi services. For this reason, BIS included in the NPRM's definition of sale that "distributing for…other commercial operations" qualifies as a sale (even if it is not for purchase or lease). In order to provide greater clarity to regulated parties, BIS has chosen to explicitly state in the related prohibited transactions provision in section 791.304, that this rule prohibits connected vehicle manufacturers who are themselves owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia from offering commercial services that utilize completed connected vehicles that incorporate ADS. BIS anticipates that this will

include both robotaxi and rideshare services. BIS has added Example 41 above to provide further clarity.

As noted above, for the purposes of the final 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 are prohibited, BIS has offered examples of persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC and Russia in Section VI subsection (a) above. BIS incorporates the examples provided in the NPRM and has added several new examples to provide further illustration.

c. *Compliance*

1. Declaration of Conformity

Declarations of Conformity will be a critical tool for advancing the goals of this final rule, and addressing the emergency declared in E.O. 13873 (section 791.306, "General authorizations"). 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. Given the complexity, the vast number of parts, and the supply-chain opacity, BIS assesses there is a significant risk that 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 will be incorporated into connected vehicles if connected vehicle manufacturers do not conduct adequate supply chain due diligence or fail to prioritize and prevent the risks BIS has assessed. BIS considered whether to remove the Declarations of Conformity requirement and only require the submission of specific authorization applications for connected vehicles incorporating VCS hardware and covered software imported from PRC and Russia. However, BIS does not believe that this alternative adequately mitigates the risks identified in this rule. Foreign adversaries are not limited to operations within their geographical area and may obtain access to VCS and ADS supply chains through investment and participation in operations in a variety of foreign locations. Current customs and other supply chain reporting, which is focused on country of origin, creates a layer of opacity that can be exploited by adversaries to compromise connected vehicle components that can later be used to threaten United States persons and infrastructure. In other words, current practices for reporting supply chain due diligence do not prioritize the same national security focus required by this regulation.

As BIS stated in the NPRM and as discussed in further detail below, based on extensive engagement with connected vehicle manufacturers and automotive suppliers, BIS assesses that

connected vehicle supply chains often have significant numbers of suppliers for a single connected vehicle in a given model year. Connected vehicle manufacturers typically have strong relationships with their immediate suppliers, including the development of years-long supply contracts that span entire vehicle generations; however, their understanding of the deeper supply chain, such as who is supplying their suppliers (*e.g.*, tier two, tier three) is substantially weaker. Additionally, BIS understands through industry engagement that although the COVID-19 pandemic and associated supply chain crisis forced connected vehicle manufacturers to critically evaluate their hardware supply chains, detailed knowledge of software supply chains remains largely unachieved. Even where it may exist, BIS cannot actively identify a specific supply chain compliance framework for the auto industry that requires due diligence on the national security risks in the auto market's supply chain. Such complexity and opacity, without a requirement to conduct the necessary due diligence, could result in the incorporation 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, into connected vehicles without the full knowledge of the connected vehicle manufacturer.

Consequently, BIS believes that the requirement to submit annual Declarations of Conformity will serve as an important mechanism that will substantially reduce the risk of the current supply chain opacity by requiring enhanced due diligence into the auto market's supply chain through a specific national security lens. BIS requires VCS hardware importers and connected vehicle manufacturers to submit Declarations of Conformity to certify their compliance with this regulation, including their completion of due diligence requirements. BIS has considered whether, as an alternative, a recordkeeping approach could adequately address the national security risk posed by connected vehicle technology with a nexus to the PRC and Russia, but recordkeeping is a retroactive activity. It does not create an adequate incentive to change supply chain business practices to achieve the goals of this rule.

If Declarations of Conformity were entirely replaced by a recordkeeping requirement, manufacturers may have to undergo recalls on parts that have already entered the supply chain. Automotive recalls are difficult to execute, with automakers traditionally struggling to reach a 100 percent completion rate on recalls due to various complications, including customer communication failures and the preowned vehicle market. If a recall fails to remove all of the vulnerable vehicles from the road, the national security threat will continue to persist. As such, the undue risks to national security would not be sufficiently mitigated without proactive due diligence requirements that deter the threat before it enters the U.S. supply chain, rather than reactive measures such as recordkeeping, reporting requirements, or unsatisfactory recalls by VCS hardware importers and covered vehicle manufacturers to secure their supply chains. At the same time, recalls would represent a source of unpredictability for automakers and suppliers, and this cost would likely be passed on to consumers. By contrast, requiring companies to submit Declarations of Conformity to the government will motivate them to conduct supply chain due diligence in order to make the required certifications. Because companies are conducting proactive due diligence, they will be able to detect prohibited components and mitigate risks before they enter the larger connected vehicle ecosystem.

Given the national security risks posed by the ADS and VCS supply chains, BIS requires that industry actively participate in securing the supply chain. By requiring certifications in the Declaration of Conformity, BIS creates an incentive for industry to invest in supply chain review and assessment and to accelerate necessary changes to ensure each regulated entity achieves compliance. The act of requiring affirmative certification encourages the adoption of enhanced supply chain due diligence and begins the process of standardizing how industry will be required to respond to foreign adversary ICTS in the automotive supply chain. Public comments to the ANPRM and the NPRM and information conveyed in BIS's external engagements indicate that much of the industry does not factor national security issues into their supply chain operations. Ultimately, by requiring connected vehicle manufacturers and VCS hardware importers to

submit Declarations of Conformity, BIS ensures that parties subject to this final rule implement necessary procedures to fully understand their VCS hardware and covered software supply chains. Declarations of Conformity are an important tool in ensuring that parties subject to this final rule comply with the 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.

Apart from encouraging suppliers to re-examine their supply chains, the certification process will also help the U.S Government execute its responsibility to maintain the national security interests of the American people. Through requirements for recordkeeping and due diligence on the part of declarants, BIS will be able to obtain data which may not otherwise exist in a useable format without such requirements to verify Declarations of Conformity, such as documentation of the tiers of ICTS suppliers (section 791.312, "Recordkeeping") (section 791.313, "Reports to be furnished on demand"). BIS will further use such information to better inform and identify risks as they evolve within ADS and VCS supply chains. For example, if, through the verification process, BIS determines that a supplier has a nexus to foreign adversary, BIS can highlight to other companies that the supplier is prohibited by using an "Is-Informed" notice. Additionally, if a company previously acting under a Declaration of Conformity must, due to their own discovery of a change in circumstance, cease acting under a Declaration of Conformity, and instead submit an application for a specific authorization, BIS may, upon receipt of said specific authorization, be able to identify supply chain issues impacting other companies acting under a Declaration of Conformity. Receipt of Declarations of Conformity will also help BIS to spot trends in the importation of covered software and VCS hardware with a foreign interest into the U.S., which will allow BIS to appropriately analyze the hardware and software with the largest risk of evasion by prohibited companies. In sum, through receipt of Declarations of Conformity, BIS will be more capable of monitoring the pervasiveness of the

risk and gain insight into any additional mitigation measures which may be required to secure the continuously evolving ICTS supply chain, as authorized by E.O. 13873.

The information collected through Declarations of Conformity will be essential for BIS to effectively protect U.S. national security from the risks identified in this rule. BIS has generally found that research using publicly available data is often incapable of revealing whether a supplier has ties to the PRC or Russia. As BIS has detailed extensively in this rule, there are myriad ways in which an entity may be owned by, controlled by, or subject to the jurisdiction of a foreign adversary, and not all of these circumstances will be publicly disclosed. Additionally, regulated entities working directly in the sector will have a far more intimate understanding of the parties with whom they transact, another form of information which is often otherwise undisclosed. BIS will need access to both types of information in order to execute on the goals of this rule. As such, to ensure industry-wide compliance with this rule and maintain the understanding of the connected vehicle sector necessary to conduct enforcement, BIS will require companies to maintain such information, and submit said information in the case that it is otherwise unavailable. Without the Declaration of Conformity certifications, BIS will be unable to receive a fulsome picture of the regulated supply chain and relevant technologies, and it will be left with a needle-in-a-haystack approach when assessing companies' compliance with this rule. Ultimately, the certification process will bring transparency to an opaque supply chain.

In the proposed rule, BIS proposed including several reporting requirements for connected vehicle manufacturers, connected vehicle importers, and VCS hardware importers that submit Declarations of Conformity. These reporting requirements included, but were not limited to, submitting SBOMs and HBOMs and a list of third-party external endpoints to which the VCS hardware connects, including the country where each endpoint is located and the identity and location of the service provider, as applicable.

After considering public comments, BIS has restructured the Declarations of Conformity requirement to clarify the certification, narrow the reporting requirements, and add

recordkeeping elements. The final rule requires that Declarations of Conformity would be submitted in two instances by persons not engaged in prohibited transactions: (1) Declarations by entities engaged in VCS hardware transactions; and (2) Declarations by entities engaged in covered software transactions.

Persons required to submit a Declaration of Conformity need to do so once per model year for units associated with a vehicle model year, or once per 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. Several commenters voiced confusion and requested clarification on the timeline for Declarations of Conformity. BIS has extended the timeline for submitting updates to a Declaration of Conformity from 30 to 60 days.

BIS further clarifies the certification statement that connected vehicle manufacturers and VCS hardware importers must make. BIS agrees that the use of terms like "knowingly engaged," which is past tense, made the timing for submission of a Declaration of Conformity confusing. Therefore, BIS has adjusted the language to require a more straightforward certification: that the VCS hardware or covered software triggering the need for, and described in, the Declaration of Conformity was not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

In the final rule, entities must submit to BIS the name and contact information of the VCS hardware importer or connected vehicle manufacturer, as well as additional information outlined in section 791.305, based on whether the entity is engaging in a covered software or VCS hardware transaction. Entities must also certify to BIS that they have conducted due diligence into their supply chain and that their VCS hardware or covered software was not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. Primary business records documenting these due diligence efforts, which may include the optional use of independent or hired third-party research (section 791.315, "Third-party verification and assessments"), must be maintained by the

declarant or a third-party and made available to BIS upon request. HBOMs and SBOMs are no longer required to be submitted as part of a Declaration of Conformity but can function as a method of recordkeeping.

Several commenters expressed fundamental disagreement with BIS's proposed regulatory approach for connected vehicle supply chains. One commenter suggested that BIS adopt a framework like the NHTSA Federal Motor Vehicle Safety Standards (FMVSS), which allows companies to import restricted components provided they conduct their own due diligence and risk analysis. NHTSA FMVSS establishes minimum performance requirements for manufacturers and the equipment used to make vehicles, prioritizing safety standards for drivers and passengers. BIS's concern with ADS and VCS technology is broader than that of public safety of drivers and passengers, but also addresses additional concerns, including national security risks posed by adversary countries, such as data exfiltration and remote access control that may compromise critical infrastructure. BIS does not believe that the NHTSA FMVSS provides a framework that is designed to address national security concerns, however, BIS has adopted some similar characteristics of this framework. For example, BIS may allow companies to import restricted components through specific authorizations if those companies show a certain degree of due diligence, risk analysis, and risk mitigation to minimize the threat present in otherwise prohibited ICTS.

One commenter requested withdrawal of the use of the Declaration of Conformity in favor of a presumption of conformance, claiming that a presumption of conformance would reduce regulatory burden, address the national security risk, and remove potential hurdles to innovation posed by the NPRM. BIS rejects utilizing a presumption of conformance. The risks identified in this rulemaking are too great to rely solely on a presumption of conformance by commercial companies, which is only exacerbated by the opacity of the supply chain as discussed above. A presumption of conformance would also allow hardware and software to linger and remain in the U.S. ecosystem for a longer period of time as BIS would not have insight or confirmation of the

existence of such hardware or software. Through receipt of declarants' certification regarding VCS hardware or covered software, that they have conducted due diligence to inform this certification, and that they, or a designated third party, maintain documentation related to this certification as part of their Declarations of Conformity, BIS will be able to more accurately and efficiently confirm and verify that no VCS hardware or covered software designed, developed, manufactured, or supplied by persons with a sufficient nexus to the PRC or Russia continues to operate in the United States.

In the final rule, BIS has largely adopted a certification and recordkeeping approach in Declarations of Conformity that significantly lessens the burden on regulated entities. Entities can now certify to BIS that they have conducted due diligence into their covered software and VCS hardware supply chains without needing to submit such documentation to BIS. A recordkeeping requirement alone would not be sufficient to mitigate the identified risk because it would not create the incentive to change business processes to identify and address risks in their supply chains. Requiring certifications in Declarations of Conformity, on top of a recordkeeping requirement, creates an enforceable incentive for industry to invest in supply chain review and assessment thereby furthering mitigation of the risks identified in this rule.

Commenters also requested that software traceability be included in the compliance requirements of this regulation. BIS believes that in order to determine compliance, entities regulated under this rule will be required to conduct the necessary software traceability as part of their supply chain due diligence. For example, in submitting a Declaration of Conformity, declarants are required to certify both that the covered software was not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia and that the declarant has conducted due diligence to inform its certification. If such due diligence determines that certain VCS hardware or covered software was designed, developed, manufactured, or supplied by a foreign adversary, such use of ICTS would be prohibited and the entity would need to apply for a specific authorization. Furthermore,

an applicant for a specific authorization may be required to furnish additional information to BIS prior to the granting of a specific authorization, which may require applicants to conduct further due diligence into their software supply chain.

Some commenters criticized the NPRM for being developed in isolation from other automobile trade actions taken by the U.S. government, suggesting that this lack of coordination prevents the streamlining of existing governmental processes related to the automotive industry. BIS emphasizes that the statement in the NPRM that one commenter referenced, which stated that the proposed rule was issued irrespective of other trade policies, does not mean to imply that this action was undertaken without coordination with other government agencies regulating vehicle safety or the trade of vehicles. Rather, BIS emphasizes that this regulation is being promulgated strictly on national security grounds that exist irrespective of specific trade policy surrounding connected vehicles, which do not adequately (or at all) address the national security risks articulated in this rule. BIS emphasizes that the ANPRM, the NPRM, and this final rule all underwent extensive interagency review and incorporated views of all other relevant Federal agencies. In addition, BIS met weekly with an interagency technical working group as part of its drafting process.

Existing trade actions do not sufficiently address the national security risks identified by BIS in the connected vehicle supply chain. In response to commenters requesting that BIS clarify the role of coordinating agencies or other regulations, such as the FCC Covered List, BIS anticipates that it will continue closely collaborating with relevant government agencies including when adjudicating applications for specific authorizations or determining if and when updates to this rule are necessary. BIS emphasizes that regulated entities will be responsible for verifying compliance with all laws and regulations applicable to the transactions in which they seek to engage but may request an advisory opinion from BIS if unsure that a specific transaction is subject to the prohibitions of this rule.

Commenters raised a series of concerns with the SBOM and HBOM requirements in the Declarations of Conformity requirement. Most of these concerns involved the ambiguity of the SBOM and HBOM requirements described in the NPRM and what should be included in these documents. Commenters argued that the NPRM's HBOM and SBOM requirements are overly burdensome, demanding both regulated entities and BIS to devote substantial resources to meet compliance. Commenters also wanted clarity on when companies would be required to submit an HBOM or SBOM, and for BIS to specify whether they would be required to do so every time an SBOM or HBOM changes. In response to comments, BIS is no longer requiring the submission of SBOMs and HBOMs in Declarations of Conformity. Entities will instead be required to certify to BIS that they have conducted due diligence in analyzing their VCS hardware and covered software supply chains and maintain documentation in support of this certification. The documentation may take the form of an SBOM or HBOM or another appropriate format. Entities must also certify that this documentation can be made available to BIS upon request.

Commenters wanted BIS to describe how it will receive, store, protect, and use SBOMs and HBOMs. Commenters repeatedly raised concerns about the protections of sensitive proprietary information in Declarations of Conformity. Commenters argued that BIS is creating a heightened risk that hostile actors may attempt to exfiltrate sensitive technical specifications, software components, or system designs, leading to significant economic damage and undermining the global competitiveness of U.S. companies if BIS fails to adopt protective measures. Commenters often sought BIS assurance that their data will be protected and secured. Commenters recommended that BIS adopt strict access controls for submitted Declarations of Conformity, particularly those containing classified or sensitive proprietary information. These controls could include encryption of submissions, limiting access to authorized personnel only, and ensuring that proprietary information is not unnecessarily shared during any public disclosure or regulatory review processes. One commenter also requested that BIS delete CBI provided in support of a submission after a period of time.

BIS acknowledges commenters' concerns related to the submission of sensitive information in the Declarations of Conformity. In response, BIS has limited the amount of sensitive information required as part of the submission by eliminating the requirement to submit SBOMs and HBOMs. BIS has also included a section in the rule (section 791.314, "Confidential Business Information") dedicated to the submission of CBI, which would cover the submission of SBOMs or HBOMs if they were ever required for third-party verification purposes. Section 791.314 outlines the confidentiality of information the same as in BIS regulation 15 CFR 791.102 including that information or documentary materials, not otherwise publicly or commercially available, submitted or filed with the Secretary under this part will not be released publicly except to the extent required by law. BIS declines the suggestion to delete CBI after a period of time, as such information may need to be referenced in future investigations due to evolving national security concerns.

Tier one and tier two suppliers often explained that providing SBOMs and HBOMs to customers, such as OEMs, can potentially undermine their business value because it is equivalent to giving their proprietary information to their client. These suppliers would rather submit this information directly to BIS. In response to these comments, and apart from removing the mandatory submission of SBOMs and HBOMs as part of the Declaration of Conformity process, BIS has allowed connected vehicle manufacturers and VCS hardware importers to rely on third parties as part of their due diligence efforts. If BIS requires the submission of additional documentation in the verification of a Declaration of Conformity, suppliers would be allowed to submit the required documentation directly to BIS.

Commenters offered ideas on how BIS could enact different models to limit the burdens imposed on both BIS and regulated entities, as well as ensure the protection of IP. A handful of commenters suggested implementing the NHTSA self-certification model requiring VCS hardware importers and connected vehicle manufacturers to produce and retain their Declarations of Conformity and provide them to BIS on an as-needed basis. Commenters also

suggested implementing other attestation or self-certification programs, including those that could be modeled by Federal agencies, such as U.S. Customs and Border Protection's Certifications of Origin template or the Food and Drug Administration's Importation of Electronic Products declarations. One commenter in particular emphasized that the adoption of these methods would create a streamlined self-certification compliance process that eases production burdens on regulated entities and allows BIS to focus on monitoring for prohibited transactions, rather than processing and maintaining a substantial amount of information through Declarations of Conformity that may not provide meaningful data. As described above, BIS determined that relying entirely on a self-certification system for Declarations of Conformity would be insufficient given the nature of the national security risk and these self-certification models. Self-certification would not give BIS the visibility that Declarations of Conformity provide to track and monitor the connected vehicle supply chain industry, specifically as it relates to the timeliness of identifying potential violations of this rule and the actions BIS would need to take to remedy a national security issue stemming from prohibited covered software or VCS hardware that has entered the U.S. supply chain.

Commenters suggested other ways of narrowing the scope of the Declaration to be less burdensome on regulated entities. For instance, some commenters recommended that BIS change the requirement to submit a Declaration of Conformity for every model year. While it has not removed the requirement to submit a Declaration of Conformity every model year, BIS has updated the Declaration of Conformity submission requirements to be less burdensome on regulated entities by allowing declarants to submit a confirmation that a prior Declaration of Conformity remains accurate in lieu of submitting a new Declaration of Conformity. Some commenters also requested BIS allow regulated entities to rely on statements, attestations, or affirmations from suppliers regarding the origins of components and software so as to limit reporting requirements and ensure that tiered suppliers did not have to share their intellectual property with their customers. Based on comments, BIS will allow connected vehicle

manufacturers to rely on their suppliers' submissions of supply chain information to BIS, if an agreement between the connected vehicle manufacturer and supplier permits such sharing of information. Commenters suggested that entities should be able to simply provide a comprehensive list of all imported VCS and ADS fleet-wide for a given model year. BIS accepts this suggestion as the Declaration of Conformity procedures would allow for connected vehicle manufacturers or VCS hardware importers to submit a single comprehensive submission. Other commenters strongly recommended that BIS abandon the universal submissions requirements of SBOM and HBOM and instead require them only in the event of an investigation or audit. BIS acknowledges commenters' feedback, and in response has adjusted SBOM and HBOM submission requirements. BIS accommodates the requests to forego the submissions of HBOMs, SBOMs, and other proprietary information, and rely more on a certification-based model as commenters suggested.

As such, for the purposes of submitting a Declaration of Conformity, BIS has clarified that a certification is a written statement or attestation, made in relation to section 791.305(a) of this rule, to the U.S. Government, signed by a duly authorized designee, certifying under the penalties provided in 18 U.S.C. 1001, that the information provided is accurate and complete in all material respects to the best knowledge of the designee on behalf of the entity filing the Declaration of Conformity. BIS further clarified that for the purposes of a Declaration of Conformity, a duly authorized designee is:

(i) In the case of a partnership, any general partner thereof;

(ii) In the case of a corporation, the chief executive officer, or any officer with the authority to bind the corporation;

(iii) An employee with authority to make certifications on behalf of the company as designated by a person in (i) or (ii); and

(iv) In the case of an entity lacking partners and officers, any individual manager, or designated agent who has been explicitly authorized by the board of directors or equivalent to sign contracts and make legally binding agreements on behalf of the entity.

BIS concluded that this approach provides the declarant with clear instructions as to who may make certifications as part of Declarations of Conformity. While the requirements for a certification have certain guidelines, BIS has still provided companies with flexibility to internally determine who may make these statements. BIS acknowledges that adopting a more certification-based model for Declarations of Conformity, as commenters suggested, requires an increased level of trust in such certifications on the part of BIS. BIS's guidelines as to who can make a certification ensures that only duly authorized individuals can attest to an entity's compliance and that supply chain security is a priority within the connected vehicle industry.

BIS has additionally allowed for connected vehicle manufacturers and VCS hardware importers to rely on third parties as part of their due diligence requirements for a Declaration of Conformity. This could include a VCS hardware importer or connected vehicle manufacturer relying on assessments from suppliers, provided that they have arranged for suppliers to furnish documentation and third-party assessments (as applicable) to BIS upon request. Further, BIS confirms that the Declaration of Conformity requirement will be satisfied by VCS hardware importers and connected vehicle manufacturers who submit a compiled Declaration of Conformity that covers the covered entity's entire fleet for the given model year, so long as it appropriately identifies the minimum required information (including, without limitation, the FCC ID Number of the hardware, if known, and the makes, models, and trims of vehicles covered by the Declaration of Conformity).

Commenters raised concerns about the efficiency of the compliance process and provided solutions to promote processing in a timely manner. Commenters suggested that Declarations of Conformity be replaced with dialogue between BIS and entities subject to regulation. Another commenter urged BIS to consider clarifying the applicability of the Declaration of Conformity

requirement for import purposes in order to avoid a huge surge in advisory opinion requests, particularly for importers. To help with expediency, one commenter recommended that BIS use best-in-class documentation and verification standards to ensure that submission of compliance materials does not hinder the pace of commerce. This commenter also suggested that BIS allow companies to digitally present import and compliance documentation proactively via their due diligence processes. BIS took these comments under consideration when re-assessing the requirements in the Declarations of Conformity. While BIS did not accept all of the commenter's suggestions, BIS believes that the updated Declaration of Conformity provisions and clarifications in the final rule will increase the rule's efficiency. BIS believes that the Declaration of Conformity requirement will be integral to the expedient administration of this rule because it will incentivize industry compliance and help BIS administer this rule when reviewing industry compliance.

Commenters advised BIS to reconsider the timeline submission requirements of Declarations of Conformity. Many commenters advised increasing the Declaration of Conformity submission deadline from 30 days to 60 days to provide manufacturers and importers adequate time to prepare, verify, and submit updates. Another commenter requested more details on the timeline required for regulated entities to submit their initial Declarations of Conformity, urging BIS to provide more time for entities to initially review their supply chains. Commenters also recommended that BIS clarify that manufacturers or importers must submit amended Declarations of Conformity within 30 days if they discover errors, omissions, or other issues in previously submitted documents. BIS acknowledges commenters' concerns and has increased the submission deadline for Declarations of Conformity to 60 days in all instances. Connected vehicle manufacturers and VCS hardware importers must submit digital documentation of their compliance at least 60 days prior to the first import or first sale of each model year of a completed connected vehicle that incorporates covered software and the first import of VCS hardware for each model year or calendar year, as applicable.

Commenters provided feedback on the "material" change requirements of Declarations of Conformity. Comments included conflicting opinions on when industry should be responsible for providing an updated Declaration of Conformity. One commenter requested that material changes be limited to the first submission because hardware can be used for several different makes, models, and trims. Another commenter suggested that a material change submission should require an updated Declaration of Conformity within 60 days. Several commenters suggested that BIS remove the requirement for annual certification and instead only require recertification if there is a material change to the model year. Separate from this, another commenter identified that the NPRM placed no limit on how far into the future automakers will have to declare material changes, suggesting that material changes be limited to 10 years to align with the document retention limit. One commenter also advised that BIS clarify when the material change clock starts, specifying it to be when the declarant first knows of the material change. More broadly, commenters urged BIS to define "material" change and provide examples.

BIS has clarified the scope of a "material" change, which is limited to the "discovery, by the declarant, of an omission, inaccuracy, or error in the information provided to the Department in a prior Declaration of Conformity that could reasonably mislead as to the true source of VCS hardware or covered software in question." BIS accepts the suggestion that connected vehicle manufacturers and VCS hardware importers must notify BIS of any material change to the information conveyed in a previously submitted Declaration of Conformity by submitting a revised Declaration of Conformity within 60 days following the discovery of such change. BIS clarifies that covered software updates alone do not constitute a material change. BIS declines to remove the annual certification requirements for Declarations of Conformity as the information certified in an annual certification is more robust than that considered to be a "material" change. However, BIS confirms that connected vehicle manufacturers and VCS hardware importers may submit a confirmation that a prior Declaration of Conformity remains accurate by associating the

relevant new model year of vehicles (if known) to an existing Declaration of Conformity. In addition, BIS confirms that the declarant's obligation to inform BIS of material changes to the information on which a Declaration of Conformity depends ceases 10 years after submission of the original Declaration of Conformity for that model year or calendar year.

Commenters also respectfully questioned whether a 10-year retention requirement for Declarations of Conformity is reasonable, appropriate, or practicable for the connected vehicle industry given that rate of technological advancement, ultimately recommending a shorter retention period. One commenter suggested to require only keeping records that would be retained in a normal course of the business. BIS declines to adjust the 10-year recordkeeping requirement so as to maintain consistency with the statute of limitations clause of IEEPA. Additionally, BIS understands that the connected vehicle industry generally maintains a minimum standard of 10-year spare parts availability. As such, BIS believes the 10-year recordkeeping requirement contained in this rule represents a relatively small additional burden to the industry. BIS agrees with the commenter's request to narrow the scope of recordkeeping to primary business records and has modified the final rule accordingly.

Commenters shed light on a handful of other areas of improvement for the Declarations of Conformity. For example, one commenter requested that an incorrectly submitted Declaration of Conformity in good faith should not be considered a "violation" and should be excluded from the penalties listed in the BIS proposed rule. BIS acknowledges commenters' concerns and would advise commenters to review section 791.305(k) which subjects any person who submits false information in a Declaration of Conformity, with knowledge that such information is false, and engages in a prohibited transaction, to potential penalties. Furthermore, in response to commenters, BIS has provided an opportunity for connected vehicle manufacturers and VCS hardware importers who incorrectly submit a Declaration of Conformity in good faith to submit an updated Declaration of Conformity to BIS within 60 days of discovery of an error or omission in a previously submitted Declaration of Conformity.

Other commenters highlighted a contradiction between the NPRM's discussion text and its regulation text about third-party research requirements. Commenters provided several examples of text to update this language. BIS appreciates this notification and has adjusted the discussion and regulation text to indicate that the use of third-party research is not required but may be used by declarants to fulfill due diligence requirements as part of the submission of a Declaration of Conformity.

Commenters also pointed out that requiring importers and manufacturers to record all third-party external endpoints that VCS hardware connects is not possible because these connection points are inherently in the control of third parties, such as app providers. Further, to limit third-party external endpoints in order to create a complete list, VCS hardware manufacturers would need to develop and operate completely closed ecosystems, which is inconsistent with consumer demand. Ultimately, commenters recommend that BIS delete the requirement to record all third-party external endpoints or narrow the information requested to that which is in the possession and control of the VCS hardware manufacturer or importer. BIS agrees with these commenters and has removed reporting requirements related to external endpoints from the final rule.

Commenters urged BIS to consider how it could streamline the approach for tier one, tier two, tier three, and below suppliers. One commenter recommended that BIS provide guidance on establishing a shared responsibility framework, making tier one and tier two suppliers equally accountable for compliance of their components in order to accelerate due diligence efforts. Another commenter advised that BIS form a volunteer certification process for VCS hardware suppliers to help streamline the process of compliance at the OEM level. Another commenter suggested that BIS provide additional clarity on how OEMs should interface with tier three suppliers and below, which was not contemplated in the NPRM. In an effort to create a semi-shared responsibility framework, BIS has allowed connected vehicle manufacturers and VCS hardware importers to rely on third-party assessments (including assessments from suppliers) as a part of the due diligence requirements for the submission of a Declaration of Conformity. If

declarants rely on assessments from suppliers, declarants must certify that they have taken all possible measures, either contractually or otherwise, to ensure any necessary documentation and assessments from suppliers will be furnished to BIS upon request either by the declarant, or, in cases including CBI, directly by the supplier. BIS declines to create a volunteer certification process for VCS hardware suppliers at this time but may consider issuing a general authorization at a later date if applicable. With regard to interfacing with tier three suppliers and below, BIS declines to prescribe the nature by which OEMs conduct the required due diligence to allow each regulated entity the flexibility to align with their unique business model.

As noted above, one commenter argued that BIS's broad definition of foreign interest would mean that a publicly traded company with some foreign shareholders would be required to submit a Declaration of Conformity. As explained above, BIS does not intend for every publicly traded company with minority foreign shareholders who do not affect management or control over the company to submit Declarations of Conformity if no other foreign interest exists. Therefore, BIS has created an exemption to the Declarations of Conformity requirement in section 791.305(l) for circumstances where the only foreign interest arises when a foreign person owns equity of a public company but does not affect the company's management or control.

One commenter sought clarification on whether the NPRM requires that all OEMs must prepare and submit a Declaration of Conformity even when no foreign interest is involved. BIS clarifies that if VCS hardware or the addition of covered software to a completed connected vehicle involves components in which there is no foreign interest, then it would not fall within the scope of this rule. However, if there is a foreign interest in that VCS hardware or covered software transaction, then it would require a Declaration of Conformity or specific authorization.

1. The sections below explain in greater detail the types of Declaration of Conformity that are required under the final rule.

i. VCS Hardware

The Declarations of Conformity described in section 791.305(a)(1) 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. 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. The FCC ID is used to identify and certify that the device meets the necessary regulatory standards for wireless communication. BIS will require the Declaration of Conformity to contain the FCC ID number(s) of the VCS hardware if known. BIS will also require the Declaration of Conformity to list any subcomponents in the VCS hardware that also have an FCC ID number if applicable. The final rule additionally requires VCS hardware importers to provide the make and model of the connected vehicle(s) for which the VCS hardware is intended or already integrated, if known. The VCS hardware importer submitting a Declaration of Conformity must certify that the VCS hardware was not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, has conducted due diligence (with or without the use of third-party assessments), and maintains any supporting documentation (either through an HBOM or otherwise) and third-party assessments (as applicable). Declarants must also specify who maintains the supporting documentation or assessments and certify that the declarant has arranged for suppliers to furnish any documentation or third-party assessments upon request by BIS.

ii. Covered Software

The Declarations of Conformity described in section 791.305(a)(2) applies to connected vehicle manufacturers that import or sell completed connected vehicles in the United States that incorporate covered software, including U.S.-based OEMs and foreign-headquartered OEMs with operations in the United States. Section 791.305(a)(2) requires covered entities to provide information to BIS on the make, model, trim, and Vehicle Identification Number (VIN) series applicable to the completed connected vehicles that incorporate covered software. Persons

submitting a Declaration of Conformity for covered software must certify that the covered software was not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, has conducted due diligence (with or without the use of third-party assessments), and maintains any supporting documentation (either through an SBOM or otherwise) and third-party assessments (as applicable). Declarants must also specify who maintains the supporting documentation or assessments and certify that the declarant has authorized suppliers to furnish any documentation or third-party assessments upon request by BIS.

iii. Procedures to Submit Declarations of Conformity

The NPRM contemplated that VCS hardware importers and connected vehicle manufacturers submitting a Declaration of Conformity would be required to submit the Declaration of Conformity to BIS annually, 60 days prior to the first sale or first import of a 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. The NPRM also provided that 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. Additionally, the NPRM stipulated that 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.

The final rule provides that connected vehicle manufacturers shall submit a Declaration of Conformity at least 60 days prior to the first import or first sale of each model year of completed connected vehicle that incorporates covered software. VCS hardware importers shall submit a

Declaration of Conformity at least 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. BIS has chosen not to stipulate combined versus individual Declaration of Conformity submissions if an entity engages in both covered software and VCS hardware transactions at this time, but entities may do so if they choose for submission efficiency. The final rule also clarifies that connected vehicle manufacturers and VCS hardware importers must notify BIS of any material change to the information conveyed in a previously submitted Declaration of Conformity by submitting a revised Declaration of Conformity within 60 days following the discovery of such change. A declarant's obligation to inform BIS of material changes to a Declaration of Conformity ceases 10 years after the original submission. The final rule defines "material changes" as any omissions, inaccuracies, or errors in the information provided to BIS in a prior Declaration of Conformity that could reasonably mislead as the true source of VCS hardware or connected software in question. Additionally, the final rule stipulates that, in lieu of submitting a new Declaration of Conformity, a declarant may, if applicable, submit a confirmation that an existing Declaration of Conformity remains accurate and encompasses relevant new model year of vehicles (if known). Declarants shall follow the electronic filing instructions on BIS's website.

2. General Authorizations

In the NPRM, BIS provided for four general authorizations, which would have allowed VCS hardware importers and connected vehicle manufacturers to engage in otherwise prohibited transactions in certain low risk use cases without need to notify BIS. These general authorizations would have applied if (1) the connected vehicle manufacturer or VCS hardware importer produced fewer than 1,000 connected vehicles or VCS hardware units; (2) the completed connected vehicle was used on public roadways for fewer than 30 calendar days in a year; (3) the completed connected vehicle or VCS hardware was used solely for purposes of display, testing, or research; or (4) the completed connected vehicle was imported solely for

repair, alteration, or competition off public roads and would have been exported within one year of import. Persons availing themselves of a general authorization, while not required to notify BIS, would have been required to monitor their usage of the authorization for any change in use and would have been subject to audit and inspection by BIS. VCS hardware importers and connected vehicle manufacturers who were themselves owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia would have been ineligible for a general authorization.

Commenters nearly universally supported BIS's decision to include a provision for general authorizations while raising a variety of concerns or suggestions related to general authorizations, which are discussed below. However, it is important to note that in this final rule, BIS has amended the provision to allow BIS to issue general authorizations on its website and in the *Federal Register*, rather than provide for predetermined general authorizations in this rule. Several commenters encouraged BIS to consider issuing more general authorizations, including to consider issuing general authorizations for connected vehicle manufacturers who meet a certain set of robust security standards to mitigate the national security risks described in this notice. BIS's decision to provide for the issuance of general authorizations as and when it determines, rather than enumerate four specifying categories of general authorizations in this rule, will enable BIS to more nimbly and quickly issue general authorizations as appropriate, without the need for a lengthy rulemaking process to issue or amend such general authorizations. BIS anticipates that it will issue a set of general authorizations shortly after publication of this rule that align with the general authorizations outlined in the NPRM. This will include general authorizations for small businesses; for connected vehicles used infrequently on public roads; for display, testing, or research purposes; and for repair, alteration, or competition.

The following is a summary of public comments received regarding the general authorizations provisions and BIS's response.

Commenters urged BIS to raise the cap for the small business general authorization from 1,000 vehicles or units to 5,000 vehicles or units in order to align with other regulatory authorities. BIS acknowledges that differing standards exist across regulation and legislation that define small manufacturers. BIS is continuing to consider this threshold but anticipates that it will retain the 1,000-vehicle threshold because this aligns with the high-volume manufacturer definition found in Vehicle Identification Number (VIN) requirements in 49 CFR 565. BIS emphasizes that this general authorization threshold will apply to U.S. production, not global production. BIS anticipates that it will limit this general authorization to all entities under common control so as to prevent the misuse of this general authorization by numerous subsidiaries of a single entity that are purpose-built to circumvent the prohibitions of this rule. Some commenters urged BIS to clarify that vehicles assembled in the United States for export to foreign markets qualify for a general authorization. BIS does not intend for this rule to capture vehicles manufactured exclusively for export outside of the United States and anticipates that it will issue a general authorization to this effect shortly after publication of this rule. One commenter recommended that BIS implement a general authorization for re-imported hardware. The commenter highlighted that the prohibitions could capture hardware that is manufactured in the United States, exported abroad to locations other than the PRC or Russia for integration, and then imported back into the United States. BIS does not anticipate that it will institute a general authorization to this effect as it believes that such a transaction is already permitted under the terms of the rule. In this scenario, the supply chains in question "do not involve the PRC or Russia," as the commenter noted. In this scenario, products are not designed, developed, manufactured or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, and thus are permitted. Further, this final rule substantially reduces the burden of submitting Declarations of Conformity for imported VCS hardware, so BIS believes that BIS's decision to decline to add this general authorization will not negatively affect the manufacture of VCS hardware in the United States that is later reimported. Another

commenter requested BIS add a general authorization exempting hardware "for general communications purposes" that is "not integrated into a VCS." BIS believes that modifications of the terms VCS and VCS hardware eliminate the need for this general authorization, as the revisions clarify that hardware that does not "directly enable" VCS, is not destined for VCS, or is not already incorporated in VCS is not captured by the rule.

Commenters identified challenges with the software prohibition timeline (discussed below). To remedy this challenge, commenters recommend that BIS provide time-limited general authorization for its software prohibition. Given that BIS has amended the definition of covered software to exclude software developed prior to one year following the effective date of this rule, BIS believes such a general authorization to be unnecessary at this time.

General authorizations 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. When issuing a general authorization, BIS will publish this decision on its website (https://www.bis.gov/OICTS) and will also publish the decision in the *Federal Register*. Notices regarding individual general authorizations may contain specific instructions that persons must follow if they wish to avail themselves of a general authorization, which could include filing regular reports with BIS regarding their use of the general authorization. However, BIS anticipates that most general authorizations will not require reports to BIS. Under the amended provisions for general authorizations, VCS hardware importers and connected vehicle manufacturers availing themselves of general authorizations must monitor their use of such authorizations, and, within 30 days of discovering a change in circumstance, conduct an inquiry as to if the general authorization still applies. Should the importer or manufacturer determine the general authorization no longer applies, it must, within an additional 30 days, cease all prohibited conduct and submit a report to BIS detailing the incident and proposing remediation.

BIS may, at its discretion, contact VCS hardware importers or connected vehicle manufacturers to determine if the party is availing itself of a general authorization. If the party confirms that it is indeed availing itself of one or more general authorizations, BIS reserves the right to request documentation to verify compliance with these provisions. Such documents would include the primary documentation upon which the VCS hardware importer or connected vehicle manufacturer has relied to determine that it is eligible (and has remained eligible) for the general authorization(s). For more information, see "Reports to be furnished on demand."

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 is required to apply for a specific authorization before engaging in an otherwise prohibited transaction.

3. Specific Authorizations

In the NPRM, BIS proposed a specific authorization process by which VCS hardware importers and connected vehicle manufacturers could apply to engage in an otherwise prohibited transaction. Commenters provided a variety of feedback on the specific authorization criteria. One commenter suggested that BIS specify requirements for conducting proof of concept testing in the United States with Chinese network access device technologies only available from the PRC. Multiple commenters recommended that BIS consider utilizing industry or government standards and frameworks when granting specific authorizations. These recommended standards include NIST standards, the ISO/SAE 21434 Standard, UNR155, the "Proposal for Recommendations on Uniform Provisions Concerning Cyber Security and Software Updates" by the World Forum for Harmonization of Vehicle Regulations in April 2026, and the Multiple Independent Levels of Security (MILS) standards. Although not within the scope of the NPRM, one commenter recommended that BIS develop standards with NIST for vehicle to cloud interfaces and incorporate this as part of the specific authorizations process. BIS agrees with commenters that standards and assessments should be considered when reviewing specific

authorization applications. In the final rule, BIS lists several examples of documentation that could be used to support the information contained in a specific authorization application, including the ISO/SAE 21434 Threat Analysis and Risk Assessments. However, BIS intends to leave the documentation that can be used to support the information contained in a specific authorization application broad to give applicants flexibility in how they wish to support their application.

Commenters recommended different forms of preclearance procedure to ensure auto manufacturers and suppliers have advance approval for the use of certain covered software. One commenter recommended that BIS establish a process for companies to obtain preclearance for certain covered software items, such as base code that is not specifically designed or developed for automotive applications. In addition to allowing preclearance with respect to certain covered software, BIS could require companies seeking preclearance to meet specified cybersecurity standards and risk mitigation measures specific to ensuring the integrity of the relevant code, including third-party vulnerability testing as applicable. Another commenter suggested that this preclearance could replace specific authorizations for companies that demonstrate that they meet the provided preclearance requirements. BIS appreciates these recommendations but finds conducting a case-by-case review to be a more effective method of risk management. BIS notes, however, that VCS hardware importer or connected vehicle manufacturers may request an advisory opinion that may inform a specific authorization at any time in accordance with section 791.310 and may apply for a specific authorization as early as sufficient information is known to fulfill the requirements of section 791.307. BIS also retains the right to issue a general authorization at a later date.

Multiple commenters urged BIS to establish with more clarity as to how frequently specific authorizations must be submitted. In response, specific authorizations will generally be approved for a duration of no less than one (1) model year or calendar year. At the time of issuance, BIS will advise specific authorization applicants the duration of any approved specific authorizations.

BIS clarifies that in situations in which BIS may make an exception to approve a specific authorization for less than one (1) model or calendar year such as for model years that are actively being sold or imported as of the effective date of the rule, for situations in which supply chains are affected by force majeure events, or due to an unexpected change in the supply chain during model year production. BIS believes these exceptions will allow companies to continue to operate while a long-term solution is pursued. BIS anticipates that each specific authorization granted under an exception will be superseded by a more permanent and long-term specific authorization.

Commenters asked that BIS be more transparent about its specific authorization procedures, such as its approach to public disclosure and preferential status. In response to these comments BIS has indicated that it will not publicly disclose any approved specific authorizations. With regards to commenters' request for preferential status to auto manufacturers headquartered in, incorporated in, or otherwise organized under the laws of an allied country, BIS believes that granting this preferential status will not limit the risk posed by foreign adversaries that are intertwined within supply chains. Therefore, BIS will not provide preferential treatment to companies on the sole basis of being headquartered in, incorporated in, or otherwise organized under the laws of a non-foreign adversary.

Another commenter argued that BIS should also include a mechanism for an emergency authorization such as in cases of supply chain disruption, natural disaster, or other temporary emergencies. BIS has accepted this feedback and incorporated it into the regulation text, allowing for the ability to grant exceptions to the default minimum one-year specific authorization and for durations of less than one year in response to force majeure events. BIS believes this change will allow companies to continue to operate while a long-term solution is pursued. BIS anticipates that each specific authorization granted under an exception will be superseded by a more permanent and long-term specific authorization. In addition to force majeure events, BIS recognizes that other potential exigencies may arise causing supply chain

challenges for companies, thus requiring a specific authorization to mitigate national security risk while BIS collaborates with companies to integrate them into the standard specific authorization process. BIS has included these additional scenarios which it believes cover a wide scope of exceptions so as to be flexible with companies regulated under this rule: 2027 Model Years that include covered software and are actively being sold or imported as of the effective date of this rule; as a result of a corporate merger, investment, acquisition, joint venture, or conversion of equity (such as from debt) that occurs during model year production; as a result of the closure or relocation of facilities involved in the production of covered software or VCS hardware; and other instances as determined by BIS. BIS envisions that specific authorizations granted under an exception with be shorter than one year in length and include proactive measures such as more frequent reporting requirements while BIS works with companies that are actively implementing or modifying corporate security policies or control measures for a more permanent solution and for which BIS would be more comfortable in granting a standard specific authorization.

Commenters additionally recommended that BIS adopt a portfolio phased approach for both software and hardware compliance. One commenter in particular highlighted that BIS could require OEMs to need only a portion of their portfolio to be compliant in the first year and then increasing each year after (*e.g.,* 33 percent the first year, 66 percent the second year, 100 percent the third year). BIS appreciates this as a recommendation and will consider it as a compliance approach when issuing specific authorizations.

Based upon this review of commenters' feedback and further consideration, BIS has modified the specific authorization process to provide more clarity to industry. VCS hardware importers and connected vehicle manufacturers wishing to engage in an otherwise prohibited transaction who are ineligible for an exemption or general authorization will 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 this final rule. Specific authorization requests will be reviewed on a case-by-case basis, and a decision regarding the application will be provided within 90 days unless BIS determines and notifies the applicant within the 90-day period that additional time is required. Applications for a specific authorization must contain detailed information on the proposed transaction, including each party to the transaction, 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, information on the connected vehicles in which the VCS hardware of covered software will be integrated, 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 will submit an application according to instructions 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 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: ISO/SAE 21434 Threat Analysis and Risk Assessments; 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 actual 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. As a default, specific authorizations will be approved for a duration of no less than one (1) calendar year, except on a case-by-case basis under certain exceptions including model years that are actively being sold or imported as of the effective date of the rule, for situations in which supply chains are affected by force majeure events, or due to an unexpected change in the supply chain during model year production.

Applicants with denied authorizations would not be precluded from submitting new applications for specific authorizations for 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

In the NPRM, BIS delineated several exemptions to the proposed rule. First, VCS hardware importers could engage in prohibited transactions described in section 791.302 without a general or specific authorization, and would be exempt from submitting Declarations of Conformity with respect to all other transactions, as described in section 791.305, provided that (1) the import of the VCS hardware occurred prior to January 1, 2029 for VCS hardware units not associated with a vehicle model year, or (2) the VCS hardware was associated with a vehicle model year prior to 2030 or the VCS hardware was imported as part of a connected vehicle with a model year prior to 2030. Second, connected vehicle manufacturers could engage in prohibited covered software transactions described in section 791.303 without a general or specific authorization and would be exempt from submitting Declarations of Conformity with respect to all other transactions described in section 791.305, provided that the completed connected vehicle that incorporates covered software described in section 791.303(a)(1) was manufactured prior to model year 2027. Third, it was contemplated in the NPRM that connected vehicle manufacturers who are owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia could engage in prohibited transactions without a general or specific authorization, and would be exempt from submitting Declarations of Conformity for all other transactions, provided that the completed connected vehicle that incorporated VCS hardware and/or covered software was manufactured prior to model year 2027. The final rule has maintained this existing list of exemptions while adding a specific exemption for parts that are imported for purposes of warranty or repair of a completed connected vehicle with a model year prior to 2030.

Many commenters requested that BIS extend the software and hardware prohibition timelines in the rule so that industry has sufficient time to adjust their supply chains. For example, one commenter claimed that the proposed timelines do not account for existing contracts between manufacturers and suppliers. Commenters requested compliance timeline extensions ranging from one to five years for the software prohibition to go into effect, and one to six additional years for the hardware prohibition to go into effect. Alternatively, multiple commenters recommended incorporating a phased-in approach for both the software and hardware prohibitions. In contrast, two commenters recommend that BIS shorten the implementation timeline due to the national security, privacy, and safety risks posed by the software and hardware transactions. Due to the national security risk being addressed by this regulation as discussed in Section IV, BIS has declined to extend the proposed software and hardware implementation timelines. For situations in which connected vehicle manufacturers or VCS hardware importers anticipate this regulation will impact connected vehicles or VCS hardware currently under production, those connected vehicle manufacturers or VCS hardware importers may apply for a specific authorization. Furthermore, with the exclusion of legacy software from the definition of covered software, BIS anticipates the regulatory burden to be lessened for industry, allowing regulated entities to more easily comply with the timeline.

Regarding exemptions, commenters recommended that BIS clarify whether systems which include their own communication but are only operational during parking are covered by the regulation. BIS declines to confirm whether systems which include their own communication but are only operational during parking are covered by the regulations, as this would require a case-by-case analysis. BIS advises industry to reference the definition of Vehicle Connectivity System.

Lastly, multiple commenters urged BIS to clarify that spare, replacement, or warranty parts imported after January 1, 2029, but for integration into a vehicle with a model year prior to 2030 which are exempted from the rule. BIS understands that connected vehicle manufacturers may

have warranty or repair obligations that extend years past the date of manufacture of the vehicle. BIS does not intend for this rule to interfere with those obligations, and BIS believes the rule as written adequately allows for the import of otherwise prohibited VCS hardware if it is for a vehicle with a model year prior to 2030. Some commenters envisioned a scenario in which a VCS hardware importer may wish to import a specific component after January 1, 2029, but the component is not yet "associated" with a model year and would thus be prohibited. In response, BIS has amended the exemptions to clarify that VCS hardware components imported for repair or warranty purposes for a vehicle model year prior to 2030 are exempt.

5. Appeals

In the NPRM, BIS proposed a process 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. Commenters suggested that BIS expand the appeals section and create a detailed framework for navigating the process, including procedures for a software supplier to participate in a connected vehicle manufacturer's appeal. Commenters also suggested that BIS be specific in defining a "reasonable time" for appealing decisions. In response to comments, BIS has included a provision that allows third parties to submit amicus filings in support of parties undergoing an informal appeals hearing if, for example, their technology is the subject of the appeal. BIS also specified that 45 days is the reasonable amount of time to file an appeal and is consistent with 15 CFR 756.2(c).

Based on commenters' feedback, BIS has further clarified the appeals process. In the final rule, the appeals process remains 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 BIS's action should be reversed or otherwise modified. The Under Secretary, at his or her discretion, may delegate to the Deputy Under Secretary of Commerce for Industry and Security or another BIS official responsibility to review and decide appeals, including arranging, at the official's discretion, informal hearings with relevant parties regarding the appeal.

On their own accord or at the request of the Under Secretary or designated reviewing official, appellants may submit supplementary information in support of their appeal. However, the Under Secretary or designated reviewing official generally will not consider additional information submitted on an appellant's own accord more than 30 days after submission of the original appeal. 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 sole discretion, grant or deny a request for an informal hearing. Parties not subject to the administrative action under appeal may submit an amicus filing in support of an appellant as part of a granted informal hearing.

6. Advisory Opinions

In the NPRM, BIS proposed the inclusion of an advisory opinion provision in order to provide interested parties greater clarity about how to comply with the proposed rule on an as-needed basis. Commenters supported BIS's inclusion of an advisory opinion mechanism in the rule. Some commenters urged BIS to set a deadline by which BIS must respond to a request for an advisory opinion. In response, BIS has implemented a 60-day deadline for advisory opinion requests unless BIS determines that additional time is needed. BIS also emphasizes the timely issuance of an advisory opinion will depend upon prompt responses by the requester in the event that BIS requests additional documents or information to inform the advisory opinion. BIS may publish on its website an advisory opinion that may be of broad interest to the public, with redactions where necessary to protect CBI. To solicit an advisory opinion from BIS, persons will

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.

In response to the NPRM's stipulation that advisory opinion requests be only for real and not hypothetical transactions, some commenters suggested that BIS allow an initial period after the rule comes into effect during which BIS will allow advisory opinion requests for hypothetical transactions. One commenter also recommended that BIS use the advisory opinion mechanism to create a trusted supplier program for connected vehicle manufacturers and VCS hardware importers. Another commenter urged BIS to issue advisory opinions for hypothetical transactions to avoid compliance challenges and high costs. BIS declines these suggestions, as such reviews for hypothetical transactions could burden the department for transactions that may never materialize and for which the binding opinion risks being made on incomplete facts. The intent of limiting advisory opinion requests to actual transactions is to allow BIS to provide thorough responses to each request that would ultimately bind the Department with regard to that transaction. Permitting entities to submit requests for vague, unspecified transactions would likely result in an untenable influx of requests and therefore undermine BIS's ability to provide comprehensive responses to each request. BIS emphasizes that a transaction need not have been initiated or executed in order to qualify for an advisory opinion request. Indeed, where a regulated entity believes that the transaction may be prohibited, the entity should request an advisory opinion before initiating or executing the transaction. BIS stresses that an advisory opinion request must contain real, specified parties to the transaction and real, specified VCS hardware or covered software in order for BIS to issue the opinion.

One commenter requested that BIS allow suppliers or other relevant parties to submit information in support of an advisory opinion request in order to avoid the forced transfer of IP from the supplier to the customer who is seeking the advisory opinion. In response, BIS has

clarified that interested parties may submit information directly to BIS in support of an advisory opinion request.

Another commenter recommended that BIS hold compliance forums to assist regulated persons in implementing the provisions of this rule. BIS will take this suggestion under advisement and will consider holding such forums after the publication of this rule. BIS further anticipates posting guidance and responses to frequently asked questions on its website (https://www.bis.gov/OICTS) to assist the public in complying with the rule.

Multiple commenters addressed the concept of preclearance and urged BIS to consider implementing such a process in parallel to the advisory opinion program. While BIS declines to institute a preclearance program given the need to adequately address the national security concerns posed by otherwise prohibited transactions, BIS has emphasized in the advisory opinion stipulations that a regulated entity may rely upon an advisory opinion issued by BIS in seeking a specific authorization or submitting an appeal to BIS to the extent that the facts and assertions made in the request remain truthful and accurate. BIS also believes that the exclusion of legacy software and refinement of the open-source software exclusion further address this commenter's point. Finally, BIS reiterates that it may publish certain advisory opinions, in accordance with the CBI section of this rule, in the case that it may be of general interest to regulated entities or relating to a supplier with which many entities wish to transact.

7. "Is-Informed" Notices

BIS received no comments on the proposed "Is-Informed" notice provision and retains the same "Is-Informed" notice provision for the final rule (section 791.311, "Is-Informed notices").

BIS may 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 final 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 official designated by the Under Secretary.

8. Recordkeeping, Reporting Requirements, and Confidential Business Information

BIS made a few notable changes from the NPRM to the final rule. First, BIS no longer requires submission of SBOMs and HBOMs, mitigating concerns about the retention of CBI and complexity of reporting requirements. Additionally, BIS has reworked the estimates of compliance costs in response with comments. As described below in more detail, BIS estimates that the initial cost of compliance will increase, but the annual cost to conduct ongoing due diligence and resubmit Declarations of Conformity will be less due to the decreased reporting requirements. BIS declined, however, to change the timeline for the retention of business records, as it is in line with IEEPA authority.

Commenters urged BIS to provide explicit assurance for protecting CBI and limit the scope of recordkeeping requirements. Some commenters provided suggestions that delineated how BIS should protect CBI and limited recordkeeping requirements. Other commenters advised that BIS establish robust protections for CBI and sought that BIS provide more information on how the agency will identify and redact CBI in published advisory opinions. Several commenters also expressed that recordkeeping requirements of the regulation were unduly burdensome and requested that BIS restructure the requirements. One commenter suggested narrowing the scope to "primary business records, such as contracts, import records, bills of sale, essential correspondence, and other key documents specified for compliance assessment." BIS understands the concerns surrounding CBI and burden posed by recordkeeping requirements. Accordingly, BIS has determined that the final rule will not require the submission of SBOMs and HBOMs. BIS notes that CBI still may be submitted pursuant to other provisions of the final rule, but not to the extent proposed in the NPRM.

A commenter urged BIS to adopt robust CBI protections given that requests for an advisory opinion will almost certainly contain proprietary information. BIS believes this comment is addressed by its addition of a new section of the rule detailing the submission of CBI. Furthermore, entities submitting CBI should refer to 15 CFR 791.102, which outlines the circumstances under which the Secretary of Commerce may authorize the disclosure of CBI materials submitted to BIS. BIS emphasizes that any information submitted as confidential will be handled in compliance with applicable laws and regulations, to ensure proper handling and to prevent unauthorized disclosure. The CBI will be used exclusively for investigative, enforcement, or regulatory purposes.

One commenter requested that BIS provide guidance on how suppliers should mark CBI in their submissions and implement a secure CBI portal. In response, BIS encourages the commenter to refer to section 791.314, which captures the CBI submission and procedures, including how the CBI files should be marked "CONFIDENTIAL BUSINESS INFORMATION" at the top of the page. Submission will occur as indicated on the BIS website, initially via email, and eventually through a submission portal which will be described in more detail on the BIS website once available.

Another commenter asked if all reports to be furnished on demand are covered in the 10-year recordkeeping requirement. BIS requires that primary business records be retained for 10 years and furnished to BIS upon request. Based on this feedback, BIS confirms that all reports to be furnished on demand are covered by the 10-year requirement.

Commenters provided conflicting feedback on the time requirements of recordkeeping. One commenter suggested that recordkeeping requirements be lowered to five years. Another commenter suggested increasing it to fifteen years. Another commenter noted 10-year recordkeeping requirements but said the information collected should be limited. BIS agrees that recordkeeping should be limited solely to primary business records related to the execution of a

transaction. However, BIS declines to adjust the 10-year recordkeeping requirement so as to maintain consistency with IEEPA.

One commenter suggested that suppliers should be responsible for recordkeeping. BIS underscores that the primary compliance responsibility is on the connected vehicle manufacturer and VCS hardware importer. However, when submitting a Declaration of Conformity, entities must certify that they have arranged for suppliers to furnish any documentation and third-party assessments (as applicable) upon request by BIS.

One commenter requested information on "permissible locations for data centers." BIS declines to explicitly name permissible locations for data centers for vehicle-external data storage but may consider the location of a data center as it relates to the design, development, manufacturing, and supplying of covered software or VCS hardware for applicants of specific authorizations.

Several commenters expressed that BIS's recordkeeping cost estimates are inaccurate. A few commenters argued that the initial range of "$30,964 and $38,554 per regulated entity, followed by estimated yearly costs of $16,133 to $80,667" to comply with the rule was underestimated. One commenter noted that two staff members managing this regulation compliance would prevent BIS from sufficiently processing all Declarations of Conformity and relevant materials. After reviewing the comments and re-analyzing the cost to entities to read the rule, understand the rule, and conduct initial due diligence, BIS re-estimates that this initial cost is between $56,671 and $77,055. Additionally, BIS re-estimates that the estimated yearly costs to re-conduct due diligence and potentially re-submit a Declaration of Conformity is between $24,200 and $48,400. While BIS agrees that its initial estimate of conducting due diligence with the rule was understated due to the complexity of automotive supply chains, BIS estimates that the annual cost to re-conduct due diligence and potentially re-submit Declarations of Conformity is reduced due to the decreased reporting requirements. Additional information on these new estimates can

be found in the *Paperwork Reduction Act* section of this final rule, and the accompanying Final Regulatory Impact Analysis.

A few commenters also noted that the estimates do not reflect BIS's own suggestion that regulated entities provide evidence of due diligence "to include independent or hired third-party research." BIS clarifies that third-party research and assessments is optional when submitting a Declaration of Conformity. However, BIS notes that third-party verification may be required as a condition for the approval of a specific authorization.

Commenters suggested implementing lists of trusted countries or suppliers in order to reduce the due diligence burden on connected vehicle manufacturers and VCS hardware importers. The publication of a list of trusted countries or suppliers would complicate compliance for BIS. The broad application of trusted countries or suppliers undercuts BIS's ability to address each transaction on a case-by-case basis with proportionate mitigation measures, as may be necessary. Creating a preapproved list of countries and suppliers would also lead to a more uncertain regulatory environment as BIS may be required to update such a list from time to time as the threat environment evolves.

BIS has chosen 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 10 years. This recordkeeping requirement applies regardless of whether the transaction is subject to a general authorization or specific authorization, or whether the connected vehicle manufacturer or VCS hardware importer has not yet sought an authorization. Records subject to the recordkeeping requirement include all information pertinent to transactions completed pursuant 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 are 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 may request business records, before, during, or after the transaction in question has taken place.

In response to numerous public comments requesting deeper commitments by BIS to protect CBI as well as greater clarity regarding how BIS will protect CBI, BIS has included a new section in this final rule detailing relevant measures BIS will take. Under these new provisions, entities submitting information that they wish to receive CBI protections should clearly mark any pages containing such CBI in their submission. Additionally, the entity requesting CBI handling should submit a statement to BIS that justifies non-disclosure by citing the specific legal authority on which the entity believes BIS should rely, such as Exemption 4 of the Freedom of Information Act (FOIA) as codified at 5 U.S.C. 552(b)(4), or other relevant authorities. As stated above, BIS will maintain confidential information in accordance with 15 CFR 791.102.

9. Third Party Verification and Assessments

In response to numerous public comments, BIS decided to further clarify the voluntary use of third-party assessments. Several comments indicated that for many of the rule's regulated entities, companies would need to outsource to third parties to maintain compliance and assist in preparing documentation for recordkeeping and submission of Declarations of Conformity. BIS emphasized that the use of third parties to maintain compliance with this rule is generally voluntary but may be required by BIS as a condition for granting a specific authorization. While regulated entities may use a third party to assist with compliance checks, the final rule does stipulate that such third parties may not be a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia. Additionally, any reports produced by these third parties would be subject to the final rule's recordkeeping requirements.

d. *Enforcement*

BIS notes as a threshold matter that it has reordered the enforcement sections of this rule to flow more naturally and to provide readers with a better sense of the chronology and sequencing of enforcement actions as compared to the structure in the NPRM. The reorder of these sections in the regulatory text has no bearing on the substance of the sections nor the rule as a whole. BIS's consideration of comments related to the enforcement provisions is discussed in the sections that follow.

1. Penalties

One commenter requested that BIS provide greater clarity on how it will determine whether a civil or criminal penalty will be assessed, as well as provide means by which an entity may rectify an error before a penalty is assessed. In response, BIS emphasizes, as detailed below, that the penalties in this rule are derived from IEEPA, and the individual nature of the violation will determine both the type of penalty and the amount to be assessed. Additionally, this rule contains multiple paths through which VCS hardware importers and connected vehicle manufacturers may rectify errors. For example, BIS may issue an "Is-Informed" notice to a party informing them that a specific authorization is needed to continue with a certain transaction. As provided below, BIS may also issue a pre-penalty notice outlining BIS's intention to issue a penalty and providing the party with the opportunity to respond and present any potentially mitigating or exculpatory evidence or remediation proposals. Lastly, in response to a request from a commenter, BIS has included in this rule a clarification that it will take into account voluntary self-disclosures of potential violations when deciding to issue a penalty.

IEEPA provides the authority for this rulemaking. Thus, persons who violate, attempt to violate, conspire to violate, or knowingly cause a violation of this rule will 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 final rule that would be subject to penalties include, but are not limited to, 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 exemption, authorization, order, regulation, directive, instruction, or prohibition issued under IEEPA and this rule.

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 final 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 final 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 mail 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 violation alleged in 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, as it 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 the Treasury for administrative collection or to the Department of Justice for collection via civil suit in U.S. District Court.

2. Finding a Violation

BIS did not receive any feedback on this in the NPRM and retains its approach for "finding a violation" in its final rule.

Under the final 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 final 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 did not receive any feedback on this in the NPRM and retains its approach to "Severability" in its final rule.

This rule implements, and is fully consistent with, governing law. However, in the event of legal challenge. BIS intends for the provisions of the final rule to be severable from each other. If a court holds that any provision in the final 15 CFR 791, subpart D, is invalid or unenforceable, BIS intends that the remaining provisions of the final 15 CFR 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 (such as the recordkeeping or Declarations of Conformity requirements), BIS intends that the provision would remain in effect as to any other person or circumstance. Each provision of the final rule and application thereof serves an important, related, but distinct purpose; provides a distinct benefit separate from, and in addition to, the benefit provided by other provisions and applications; is supported by evidence and findings that stand independent of each other; and is capable of operating independently such that the invalidity of any particular provision or application would not undermine the operability or usefulness of other aspects of the final rule. Depending on the circumstances and the scope of the court's order, BIS believes that the remaining provisions of the 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 final 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. *Other Commentary*

1. Coordination with Interagency and Industry

Commenters urged BIS to consider its overlap with other government agencies in a variety of ways. One commenter suggested that BIS conduct a conflict-of-laws analysis to ensure there is no overlap with the Committee on Foreign Investment in the United States (CFIUS) authorities. In response, BIS clarifies that its authorities are different from CFIUS authorities, the latter of which apply to certain foreign investments in the United States and are coordinated by the Department of the Treasury.

One commenter urged BIS to coordinate more closely with the NHTSA, the Federal Motor Carrier Safety Administration (FMCSA), and industry when finalizing the rule. Additional commenters advised BIS to evaluate its overlapping authorities with other government bodies. Another commenter claimed that the telecommunications supply chain is subject to overlapping authorities and regulations and therefore BIS should ensure the rule is narrowly tailored to connected vehicles. BIS acknowledges these suggestions and notes for commenters that it has robustly engaged with its interagency partners to deconflict any overlap in authorities. As noted previously, BIS's ICTS authorities are explicitly focused on addressing unique national security risks from foreign adversary involvement in the ICTS supply chain such as those articulated in Section IV of this rule and differ from other programs in the U.S. government. BIS has coordinated with interagency partners and industry to inform the development of this final rule and has worked with them to ensure this rule does not conflict with but complements other governmental efforts.

2. Global Standards/Regulations for Consideration

Multiple commenters stated that BIS should consider adopting the United Nations regulations concerning cybersecurity and software update management, such as UN Regulation 155 and UN Regulation 156. Other commenters proposed utilizing standards and frameworks including ISO/SAE 21434, ISO 26262, CISA's Autonomous Ground Vehicle Security (TISAX), Auto-ISAC Cybersecurity Best Practices, NHTSA's Cybersecurity Best Practices for the Safety of Modern Vehicles, 2024 Technical Requirements for Vehicle Overall Information Security

(GB44495), and the United Nations World Forum for Harmonization of Vehicle Regulations (WP.29). In response, BIS wants to voice its appreciation for the commenters' input and thoughts on incorporating these standards into its regulation format. However, after consideration, BIS does not assess these standards as sufficient methods to mitigate the identified risk within the connected vehicle supply chain. These standards and frameworks all have different scopes that do not accurately match BIS's goal of mitigating national security risk posed by the connected vehicle technology supply chain when containing a nexus with adversary countries.

However, some of these standards and frameworks may offer support for the compliance process. For example, when processing specific authorizations, BIS will take into consideration existing cybersecurity measures employed by the entity, such as the implementation of UN Regulation 156, which involves software update and software update management systems, or SAE Standard 21434, as they relate to the unique ICTS transaction. BIS's review for specific authorizations will be conducted on a case-by-case basis, and BIS therefore does not see it beneficial to provide blanket clearance for any one cybersecurity standard at this time. In addition to advocating for BIS to consider international standards, one commenter asked BIS to reconsider the impact of its regulation, arguing that it will hinder the United States' ability to meet its 2030 goal under the Paris Agreement. This commenter urged BIS to prepare an environmental assessment of the rule. Given that the focus of BIS's authority is limited to national security threats from adversary countries, an environmental evaluation is neither pertinent nor required.

Commenters also sought clarification on how BIS would consider international standards to which adversary countries had input. One commenter asked BIS to clarify that vehicle technologies would not be prohibited simply because they had been developed according to international standards in which the PRC had been a party. A separate commenter stated that BIS should clarify that the participation of Chinese or Russian citizens in international technical

standards-setting would not deem the VCS hardware subject to that standard as captured by the rule. BIS appreciates these comments but notes that PRC or Russia support in an international standard development process does not fall within the scope of this regulation.

3. Stakeholder Meetings

Between September 24 and December 13, 2024, BIS conducted 35 meetings with industry stakeholders to gather information, follow up on ambiguous comments, and better understand current business practices in the U.S. connected vehicle supply chain.[2]

In each meeting, BIS encouraged the participant(s) to submit written comments to the public docket. For the most part, commenters in these meetings offered views that they previously or subsequently submitted in written comments. BIS summarizes below additional points not addressed in written comments. In many of the meetings, participants provided BIS with confidential business information relating to their design and manufacturing of completed connected vehicles and/or components to provide context for points made in written submissions.

Across all meetings, stakeholders generally reiterated information submitted in written comments regarding specific authorizations; advisory opinions; Declarations of Conformity; definitions of terms such as *person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary* and *foreign interest*; a whitelist for approved components; unconventional ownership structures; and commercial trucking. As stated above, BIS has addressed each of these issues in the final rule by: clarifying the process for specific authorizations (Section VI.c.3) and advisory opinion requests (Section VI.c.6); greatly reducing the burden for Declarations of Conformity (Section VI.c.1), including exclusion of SBOMs and HBOMs; updating the definition of *covered software* (Section VI.a.5); and providing more examples regarding the definition of a *person owned by, controlled by, or subject to the*

[2] These meetings included 20 meetings held after the close of the comment period. BIS met with all stakeholders who requested meetings until the draft final rule was submitted to OMB for coordinated interagency review under Executive Order 12866.

jurisdiction or direction of a foreign adversary (Section VI.a.14) and *foreign interest* (Section VI.a.8); providing more examples on unconventional ownership structures (Section VI.a.14); and scoping the rule to address only those vehicles under 10,001 pounds (Section VI.a.3). For the reasons stated above, BIS declines to implement a whitelist (Section VI.a.12).

Finally, a stakeholder expressed interest in whether like-minded countries would be encouraged to adopt similar provisions to this regulation. BIS notes that throughout the rulemaking process it has been working closely with international allies and partners and has experienced high interest. BIS also participated in a meeting with interested foreign governments convened by the Department of State and the White House on July 31, 2024, to jointly address the national security risks associated with connected vehicles.

f. *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, and distributed impacts and equity). This final 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 final 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 final 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 final rule does not contain policies that have takings implications.

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

The Department has analyzed this final 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 final rule would not have a significant impact on the quality of the human environment.

7. Paperwork Reduction Act

There are several changes between the NPRM and the final rule regarding information collection requirements. First, BIS has significantly decreased the reporting requirements in the Declaration of Conformity provision, including eliminating the need to submit SBOMs/HBOMs or a list of third-party external endpoints to which the VCS hardware connects. These provisions have been replaced with certification and recordkeeping requirements, with specific documentation and assessments on due diligence only needing to be submitted to BIS upon request. Additionally, BIS has removed the submission of an SBOM/HBOM for advisory opinion requests. Lastly, BIS has specified in the final rule that only primary business records relating to VCS hardware and covered software need to be maintained. These changes have significantly reduced the recurring annual cost and burden hour estimates.

Several commenters noted that the initial estimation to read the rule, understand the rule, and conduct initial due diligence in preparation to comply with the rule was significantly underestimated. One commenter noted that the approximately $39,000 per entity estimate to

initially read and understand the rule and comply with its requirements is under-representative of the scope of activity required by the new proposed restrictions, compliance activities, and certification requirements. It was also noted that one of the main compliance tasks for OEMs would be the supply chain due diligence, which is time consuming and resource intensive. After internal deliberation, BIS agrees with commenters that the initial estimations to read the rule, understand the rule, and conduct initial due diligence in preparation to comply with the rule were likely underestimated, most significantly is the initial time burden for entities.

The initial time burden hour estimate for operations managers in the Preliminary Regulatory Impact Analysis was between 50 to 70 hours. BIS now estimates that the burden hour estimate for operations managers is between 100 to 160 hours. BIS evaluates that the burden hours for operations managers is essentially doubled compared to the estimation in the proposed rule due to improved insight into the complexities surrounding mapping supply chains and the initial efforts that will need to be invested in preparing to comply with the rule. BIS assesses that this updated hour estimate more accurately reflects these activities.

The initial burden hour estimate for lawyers in the Preliminary Regulatory Impact Analysis was between 80 and 100 hours. BIS now estimates that the burden hour estimate for lawyers is between 160 and 200 hours. Similarly to operations managers, BIS evaluates that the burden hours for lawyers is doubled compared to the estimation in the proposed rule due to improved insight into the legal efforts needed to (1) ensure that complex supply chains are compliant with the requirements outlined in the rule, and to (2) establish the reporting and recordkeeping practices as prescribed in the rule. The increase in lawyer burden hours also accounts for potential outside counsel engagement if a company does not have the proper in-house legal support or expertise.

Lastly, the initial burden hour estimates in the Preliminary Regulatory Impact Analysis assumed a time burden of 50 to 70 hours for engineers. This estimation remains the same in this

final rule. After internal deliberation, BIS estimates that the burden to read the rule, understand the rule, and conduct initial due diligence in preparation to comply with the rule will largely fall on operations managers and lawyers. Therefore, BIS did not increase the engineer burden hour estimate.

In the NPRM and Preliminary Regulatory Impact Analysis, BIS estimated that the cumulative initial burden (in hours) placed on applicable entities would be 180 to 240 hours and that the initial cost burden for these entities would be between $30,964 and $38,554. This estimate took 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 estimated that the total annual cost burden (in hours) for applicable entities to implement the rule would be 100 to 500 hours and that the total annual cost burden for applicable entities to implement the rule would be $16,133 to $80,667 a year. In the final rule and final Regulatory Impact Analysis, BIS re-estimates that the cumulative initial burden (in hours) placed on applicable entities is between 310 and 430 hours to initially read the rule, understand the rule, and conduct initial due diligence in preparation to comply. The re-estimated cost burden for these entities to read the rule, understand the rule, and conduct initial due diligence is between $56,671 and $77,055. Every subsequent year after the publication of the final rule, the Department anticipates that the total annual burden (in hours) for connected vehicle manufacturers and VCS hardware importers to re-conduct due diligence into their VCS hardware or covered software supply chains and potentially re-submit a Declaration of Conformity will be 150 to 300 hours. BIS estimates that the total annual cost burden for a connected vehicle manufacturer or VCS hardware importer to re-conduct due diligence into their VCS hardware or covered software supply chains and potentially re-submit a Declaration of Conformity will be $24,200 to $48,400 per year.

BIS has also re-calculated the expected cost to the U.S. Government. Consistent with the proposed rule, BIS estimates that it will take staff an average of 20 hours to review and, if applicable, respond to each Declaration of Conformity, specific authorization application, or

advisory opinion request. However, BIS has corrected the calculation by removing the 20 percent overhead addition, as overhead is already captured in staff wages. For this final rule, BIS has increased the expected legal support personnel from one to two employees in response to comments related to staffing needs in managing compliance with the rule. The re-estimated annual cost to the U.S. Government in the final rule is $1,299,728, a slight decrease from the $1,437,982 estimate in the NPRM.

Some commenters to the NPRM expressed that BIS did not provide adequate time to review the costs of the rule. BIS acknowledges the short publication timeline of this rule, but also recognizes that the national security risks the rule addresses are severe. BIS also aims to address national security risks in a way that does not unduly burden the industry, as reflected by changes in the final rule. In its efforts to reduce associated costs and compliance burden, BIS has revised the final rule to reduce information submission requirements and expand on provisions that are designed to help the industry comply with the rule. For example, BIS has dramatically reduced the information submission requirements by removing the HBOM and SBOM submission requirements, which not only meets the industry where they are but also reduces the cost of this regulation. BIS has also established a process for issuing advisory opinions to assist parties who are unsure how the requirements in this rule affect them, and a process for requesting specific authorizations if a party believes that certain transactions prohibited by this rule should be permitted to go forward. BIS also notes that the delayed implementation of this rule will provide additional time for the industry to come into compliance with its requirements and seek specific authorizations or advisory opinions, as applicable. Also, BIS emphasizes that it will continue to engage with industry following publication of this rule to educate and facilitate compliance.

One commenter also indicated concerns about “the costs of hardware compliance, particularly regarding aftermarket suppliers in the trucking industry.” BIS has since chosen to exclude commercial vehicles from this regulation and intends to propose a subsequent rule to address specific national security risks tailored towards this sector.

Commenters urged BIS to re-evaluate the broader impact of the regulation and noted the potential impact the rule would have on the automotive supply chain. BIS has been working to carefully scope the rule so that it does not place an undue burden on industry or the broader automotive supply chain. One commenter expressed concern about similar actions potentially being taken by other governments. BIS notes that this rule is focused on the domestic market within the United States.

As described above, BIS agrees with commenters who indicated the initial compliance cost estimates described in the NPRM were understated. However, BIS believes that subsequent annual costs will be lower due to the decreased reporting requirements in this final rule. BIS has revised this PRA section to account for compliance costs new to the final rule, the initial cost to comply with the rule, and lower annual cost to comply with the rule due to decreased reporting requirements.

One commenter wanted to ensure that the rule does not impair the ability for American consumers to access the data from their own vehicles. BIS notes that this concern is not implicated by this final rule. Relatedly, a few commenters shared the view that the rule will limit consumer choice and innovation, is a form of economic protectionism, and is overly broad. BIS has worked to carefully scope this rule and notes that there are numerous firms both in the United States and abroad who are leading the development of innovative products. Moreover, BIS believes that it has narrowed the scope of this rule to the extent possible by solely focusing on VCS hardware and connected software designed, developed, manufactured, or supplied by entities with a sufficient nexus to the PRC and Russia. This rule leaves the remainder of the global market out of scope.

The collections of information contained in this final rule have been submitted to the Office of Management and Budget (OMB) for review in accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501, *et seq.*) (PRA) under control number 0694-0145. This final rule will

create new information collection requirements, which are subject to review and approval by OMB under the PRA.

For regulated entities whose covered software or VCS hardware 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, the entity would be responsible for attesting to BIS that due diligence has been conducted through the submission of a Declaration of Conformity. Entities must submit to BIS the name and contact information of the VCS hardware importer or connected vehicle manufacturer, and additional pieces of information, if known, based on the type of declaring entity. Entities must also certify to BIS that they have conducted due diligence into their supply chain and can attest that their covered software and VCS hardware 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. A Declaration of Conformity will need to be submitted to BIS each calendar year or for every new connected vehicle model year.

Regulated entities whose covered software or VCS hardware is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia can apply for a specific authorization to engage in an otherwise prohibited transaction. In the application, an entity must submit information substantial enough to demonstrate to BIS that the otherwise prohibited transaction does not pose undue and unacceptable risk to U.S. national security. For example, entities may submit ISO/SAE 21434 Threat Analysis and Risk Assessments, including 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; and/or other actions or proposals such as technical controls (*e.g.*, software validation) or operational controls (*e.g.*, physical and logical access monitoring procedures) the applicant intends to take to mitigate undue or unacceptable risk. Because specific authorization applications can vary in the level of specificity and volume

of submitted materials, BIS cannot accurately estimate the costs and burden hours associated with an entity applying for a specific authorization.

Specific authorizations are reviewed and approved by BIS on a case-by-case basis. The final rule specifies that BIS may stipulate a variety of measures as conditions for the issuance of a specific authorization based on the level of risk that needs to be mitigated. For example, BIS may require the submission of annual third-party assessments as a condition. This condition would incur annual costs for an entity that seeks to engage in an otherwise prohibited transaction. Due to the variety of mitigating factors that BIS may impose when issuing specific authorizations, BIS cannot accurately estimate the costs and burden hours associated with an entity adhering to the conditions in a specific authorization.

There are several other compliance costs that regulated entities may incur from the rule, including the submission of advisory opinion requests and recordkeeping. Advisory opinions are voluntary requests that VCS hardware importers and connected vehicle manufacturers may submit to BIS to seek guidance on whether a prospective transaction is subject to a prohibition of the rule. BIS sought comments on the potential number of advisory opinions that regulated entities may submit and did not receive any. Additionally, all regulated entities are required to retain primary business records under the recordkeeping requirements in the rule. For instance, entities subject to a Declaration of Conformity will need to maintain primary business records related to their covered transactions, while entities subject to approved specific authorizations may need to record keep additional documentation based on the conditions of a specific authorization. Due to these varying circumstances, BIS cannot accurately estimate the costs and burden hours associated with recordkeeping or submitting voluntary advisory opinion requests.

As noted above, BIS estimates that it will take regulated entities between 310 and 430 hours to initially read the rule, understand the rule, and conduct initial due diligence in preparation to comply. Every subsequent year after the publication of the final rule, the Department anticipates that the total annual burden (in hours) for connected vehicle manufacturers and VCS hardware

importers to re-conduct due diligence into their VCS hardware or covered software supply chains and potentially re-submit a Declaration of Conformity will be 150 to 300 hours.

Based on analysis conducted in the accompanying final Regulatory Impact Analysis, BIS assesses that there are 27 to 215 entities potentially impacted by the rule. This range has been updated since the proposed rule to account for the removal of the commercial market from this regulation (narrowing the scope from NAICS: 3361 Motor Vehicle Manufacturing to NAICS: 33611 Automobile and Light Duty Motor Vehicle Manufacturing). The estimated cost burden for these entities to read the rule, understand the rule, and conduct initial due diligence is between $56,671 and $77,055. Every subsequent year, BIS estimates that the total annual cost burden for a connected vehicle manufacturer or VCS hardware importer to re-conduct due diligence into their VCS hardware or covered software supply chains and potentially re-submit a Declaration of Conformity will be $24,200 to $48,400 per year (average of operations manager, engineer, and lawyer hourly salaries [$484/hour / 3 = $161.33] * [150 and 300 hours]). This broad range accounts for the varying levels of information that entities need to update in a Declaration of Conformity per model year. For example, a material change in the covered software or VCS hardware could lead to the entity conducting more due diligence and then submitting a new Declaration of Conformity. Alternatively, where there are no material changes to the covered software or VCS hardware for a subsequent model year or calendar year, the connected vehicle manufacturer or VCS hardware importer can submit a confirmation that the previously submitted information remains accurate.

The estimated annual Federal salary cost to the U.S. Government to review and, if applicable, respond to Declarations of Conformity, specific authorization applications, and advisory opinion requests after the rule is fully implemented is $971,800 [an estimated total of 430 Declarations of Conformity, specific authorization applications, and advisory opinion requests per year * hourly GS-13 staff rate of $113/hour * average of 20 hours to review each Declaration of Conformity, specific authorization application, or advisory opinion request]. 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. While BIS expects the time to review and, if applicable, respond to Declarations of Conformity, specific authorization applications, and advisory opinion requests to vary, 20 hours is our best estimate of this average.

The total estimated annual cost to the U.S. Government is $1,299,728. The calculation is as follows: Annual Federal Salary Cost [$971,800] + Legal Support (two GS-15 Step 1 employees (multiplied by 2 to include the cost of benefits and overhead) @50% of their time) [$327,928] = $1,299,728.

Under the PRA, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the agency displays a valid control number assigned by OMB. Approved information collection requests may be viewed at https://www.reginfo.gov/public/do/PRAMain.

8. Regulatory Flexibility Act

In compliance with Section 604 of the Regulatory Flexibility Act (RFA), 5 U.S.C. 601–612, the Department has prepared a final regulatory flexibility analysis (FRFA) for this final rule. The FRFA describes the economic impacts the action may have on small entities. Public comments to the initial regulatory flexibility analysis (IRFA) and BIS's response is captured in subsection 2 below.

1. *A statement of the need for, and objectives of, the rule.* 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 and foreign adversaries may exploit vulnerabilities to gain access to vehicles. 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. The PRC and Russia are able to leverage legal and regulatory regimes to compel private companies subject to their jurisdiction, including carmakers and vehicle importers, to cooperate with state security and intelligence services. Cooperation could include providing data, logical access, encryption keys, and other vital technical information, as well as 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 allows remote manipulation for vehicles driven by U.S. persons.

2. *A statement of the significant issues raised by the public comments in response to the IRFA, a statement of the assessment of the agency of such issues, and a statement of any changes made in the final rule as a result of such comments.* BIS received minimal comments on the IRFA. One commenter noted that BIS should allow flexibility in the rulemaking approach where minimal or negligible risk is present, citing the IRFA. BIS agrees that there should be flexibility where minimal or negligible risk is present. To accomplish this, the rule's general and specific authorization mechanisms allow VCS hardware importers and connected vehicle manufacturers to engage in otherwise prohibited transactions if they meet certain requirements or conditions as will be identified by BIS. Another commenter noted that the NPRM, Preliminary Regulatory Impact Analysis, and IRFA did not adequately take into account the disruption the rule could cause to the availability of relevant hardware and software. BIS acknowledges this commenter's concern, and notes that although the market for component systems this rule targets has very limited publicly available data, BIS has presented its best estimates for the regulatory impact of this rule and updated its assumptions and calculations in the Regulatory Impact Analysis based on publicly available information and comments to the NPRM.

3. *The response of the agency to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration in response to the proposed rule, and a detailed statement of any change made to the final rule as a result of the comments.* BIS did not receive comments from the Chief Counsel for Advocacy of the Small Business Association in response to the proposed rule.

4. *A description of and an estimate of the number of small entities to which the rule will apply or an explanation of why no such estimate is available.* 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 supplier network is dominated by a small set of manufacturers, likely none of which would qualify as small entities. Additionally, BIS received no comments on the number of firms that engage in covered software and VCS hardware transactions in the United States. Based on information available, BIS currently estimates that there will be 27 to 215 connected vehicle manufacturers and VCS hardware importers potentially affected by this rule. This range is the U.S. Census Bureau Statistics of U.S. Businesses' estimate for the number of firms operating at least one establishment in NAICS 33611: Automobile and Light Duty Motor Vehicle Manufacturing, with the low estimate being the number of firms with 500 or more employees in total nationwide and the high estimate being all firms (this therefore includes an estimate of 188 firms with fewer than 500 employees). In comparison, the Small Business Administration's (SBA) small business size standard for NAICS 336110: Automobile and Light Duty Motor Vehicle Manufacturing (covering both manufacturer and supplier activities) uses 1,500 employees or fewer. Despite having this small entity estimate of 188, BIS does not have knowledge of which of these entities engage, or have the potential to engage, in covered software and VCS hardware transactions. Therefore, BIS is unable to estimate how many entities captured in the 27 to 215 range are small entities and engage in covered software

and VCS hardware transactions, and cannot estimate the percentage of connected vehicle manufacturers and VCS hardware importers that qualify as small entities.

We also note that it is possible that an affected entity may be considered a small entity using SBA's size standard based on employee counts for the automobile manufacturing industry, but could nevertheless have large sales or import volumes, which is BIS's primary concern because the national security risks are due to the number of connected vehicles on public roads rather than the size of the entities supplying them. For example, it is possible that a VCS hardware importer with fewer than 1,500 employees could be importing tens of thousands of VCS hardware units in a calendar year.

5. *A description of the projected reporting, recordkeeping, and other compliance requirements of the rule, including an estimate of the classes of small entities which 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 final rule's compliance costs. However, BIS maintains the flexibility to grant general authorizations to small entities that produce or import connected vehicles or VCS hardware units below a certain threshold each calendar year. The maintenance of records in support of the general authorization would be a compliance requirement for these small entities.

This rule requires regulated entities that cannot avail themselves of a general authorization to examine their automotive supply chain and ensure that their covered software and VCS hardware 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. Entities that do not have supply chains that contain covered software and VCS hardware designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia must attest to BIS that this due diligence has been conducted through the submission of a Declaration of Conformity. A Declaration of Conformity entails both reporting and recordkeeping elements. Entities must submit to BIS the name and contact information of

the VCS hardware importer or connected vehicle manufacturer, and additional information, if known, based on the type of declaring entity. Entities must also certify to BIS that they have conducted due diligence into their supply chain and can attest that their covered software and VCS hardware 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. Primary business records documenting these due diligence efforts, including the optional use of independent or hired third-party research, must be maintained by the declarant and made available to BIS upon request.

Entities that do manufacture or import covered software and VCS hardware designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia have the option of applying for a specific authorization. Specific authorizations will be reviewed by BIS on a case-by-case basis and, if granted, may require greater reporting requirements depending on BIS's assessment of the national security risks posed by the transaction. For example, BIS could require annual third-party verification as a condition for the issuance of a specific authorization.

BIS is requiring the maintenance of primary business records related to any transaction subject to a specific authorization, Declaration of Conformity, or general authorization for a period of 10 years, consistent with IEEPA's statute of limitations. Primary business records include contracts, import records, commercial invoices, bills of sale, essential correspondence, and any other records requested by BIS to assess compliance with this rule.

6. *A description of the steps the agency has taken to minimize the significant economic impact on small entities consistent with the stated objectives of applicable statutes, including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected.* In the NPRM, BIS listed specific circumstances that would qualify for a general authorization, which would allow regulated

entities to engage in otherwise prohibited transactions in certain lower-risk cases. Commenters suggested a variety of additional circumstances that BIS should consider qualifying for a general authorization. In the final rule, rather than provide predetermined general authorizations in the rule itself, BIS will instead separately issue general authorizations under any circumstances that it feels presents lower risk, allowing BIS to maintain the flexibility to grant as many general authorizations as possible and appropriate. For example, BIS may issue a general authorization to further minimize the impact of this rule on small entities that produce or import connected vehicles or VCS hardware units below a certain threshold each calendar year. If small entities do not qualify for a general authorization but feel they have been adversely affected by the rule, they can apply for a specific authorization related to their specific circumstances. Additionally, the requirements associated with submitting a Declaration of Conformity have been significantly reduced from those proposed in the NPRM, minimizing the economic impact on all submitting entities. Finally, based on public comments to the NPRM, many of the reporting requirements have been converted to recordkeeping and certification provisions. These changes will make Declarations of Conformity less burdensome for all regulated entities.

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 791, is amended as follows:

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 31.

2. Amend part 791 by adding subpart D, consisting of § 791.300 through § 791.321, to read as follows:

Subpart D—ICTS Supply Chain: Connected Vehicles

§ 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 directly enable connected vehicle Automated Driving Systems (ADS) or Vehicle Connectivity Systems (VCS), as defined in this subpart;

(b) Implement Declarations of Conformity to provide a mechanism for connected vehicle manufacturers and VCS hardware importers to communicate to BIS that they have conducted supply chain due diligence, and to confirm that no prohibited transactions, as defined in this subpart, have knowingly occurred;

(c) Provide for the issuance of general authorizations for certain transactions that would otherwise be prohibited by this subpart, but where certain factors described in the authorizations reduce the risk to an acceptable level;

(d) Provide a mechanism to apply for specific authorizations for certain transactions that would otherwise be prohibited by this subpart, where the undue or unacceptable risks can be reasonably mitigated, based on criteria and conditions that are specifically constructed for each applicant; and

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

§ 791.301 Definitions.

The following definitions apply only to this subpart. 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. A vehicle operated only on a rail line is not included in this definition. For the purposes of this subpart, a connected vehicle with a gross vehicle weight rating of more than 4,536 kilograms (10,000 pounds) is not included in this definition.

Connected vehicle manufacturer means a U.S. person who:

(1) Manufactures or assembles completed connected vehicles in the United States for sale in the United States;

(2) Imports completed connected vehicles for sale in the United States; and/or

(3) Integrates ADS software on a completed connected vehicle for sale in the United States. A connected vehicle manufacturer may also be a VCS hardware importer, as defined herein, if VCS hardware has already been installed in a connected vehicle when the connected vehicle manufacturer imports it.

Covered software means the software-based components, including application, middleware, and system software, in which there is a foreign interest, executed by the primary processing unit or units of an item that directly enables the function of 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 directly controlling, configuring, and communicating with that hardware device. Covered software also does not include open-source software, which is characterized as software for which the human-readable source code is available in its entirety for use, study, re-

use, modification, enhancement, and redistribution by the users of such software, unless that open-source software has been modified for proprietary purposes and not redistributed or shared.

Covered software also does not include software subcomponents that were designed, developed, manufactured, or supplied prior to March 17, 2026, as long as those software subcomponents are not maintained, augmented, or otherwise altered by an entity owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary after March 17, 2026.

Declarant means the U.S. person submitting a Declaration of Conformity to BIS.

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 formal record the supply chain relationships of parts, assemblies, and components required to create a physical product, including information identifying the manufacturer, and related firmware.

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. This definition also applies to related terms such as *importing* or *imported*.

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.

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 (1) through (3) of this definition 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.

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.

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 record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product.

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.

Vehicle Connectivity System (VCS) means a hardware or software item installed in or on a completed connected vehicle that directly enables the function of transmission, receipt, conversion, or processing of radio frequency communications at a frequency over 450 megahertz. VCS does not include a hardware or software item that exclusively:

(1) enables the transmission, receipt, conversion, or processing of automotive sensing (*e.g.*, LiDAR, radar, video, ultrawideband);

(2) enables the transmission, receipt, conversion, or processing of ultrawideband communications to directly enable physical vehicle access (*e.g.*, key fobs);

(3) enables the receipt, conversion or processing of unidirectional radio frequency bands (*e.g.*, global navigation satellite systems (GNSS), satellite radio, AM/FM radio); or

(4) supplies or manages power for the VCS.

VCS hardware means software-enabled or programmable components if they directly enable the function of and are directly connected to Vehicle Connectivity Systems, or are part of an item that directly enables the function of Vehicle Connectivity Systems, including but not limited to: 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 communication systems, other wireless communication microcontrollers or modules, external antennas, digital signal processors, and field-programmable gate arrays. 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, diodes, field-effect transistors, and bipolar junction transistors).

VCS hardware importer means a U.S. person who imports:

(1) VCS hardware for further manufacturing, incorporation, or integration into a completed connected vehicle that is intended to be sold or operated in the United States; or

(2) VCS hardware that has already been installed, incorporated, or integrated into a connected vehicle, or a subassembly thereof, that is intended to be sold as part of a completed connected vehicle in the United States.

§ 791.302 Prohibited VCS hardware transactions.

(a) VCS hardware importers are prohibited from knowingly importing into the United States VCS hardware that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of 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, based solely on the country of citizenship of one or more natural persons who are employed by, contracted by, or otherwise similarly engaged in such actions through the entity designing, developing, manufacturing, or supplying the hardware.

§ 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 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) Connected vehicle manufacturers are prohibited from knowingly selling within the United States completed connected vehicles that incorporate 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.

(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, based solely on the country of citizenship of one or more natural persons who are employed by, contracted by, or otherwise similarly engaged in such actions through the entity designing, developing, manufacturing, or supplying the software.

§ 791.304 Related prohibited transactions.

Connected vehicle manufacturers who are 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, regardless of whether 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. These connected vehicle manufacturers are also prohibited from offering commercial services in the United States that utilize completed connected vehicles that incorporate ADS.

§ 791.305 Declaration of Conformity.

(a) *Requirements*—(1) *VCS hardware*: A VCS hardware importer must submit a Declaration of Conformity to BIS prior to importing VCS hardware, unless otherwise specified by this subpart. The Declaration of Conformity for VCS hardware shall include:

(i) The name and address of the VCS hardware importer, to include identifying information for an individual point of contact (including name, email address, and phone number);

(ii) If known, the FCC ID Number associated with the VCS hardware and, if applicable, of the subcomponents contained therein;

(iii) If known, the make and model of the connected vehicle(s) for which the VCS hardware is intended, or already integrated;

(iv) A certification that the VCS hardware described in the Declaration of Conformity was not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia;

(v) A certification that the declarant has conducted due diligence (with or without the use of third-party assessments) to inform the above certification, and the declarant or a delegated third party maintains documentation (either through an HBOM or otherwise) and third-party assessments (as applicable) in support of the above certification, which can be made available upon request by BIS;

(vi) Identification as to who maintains the documentation and third-party assessments (as applicable) as certified above;

(vii) A certification that the declarant has taken all possible measures, either contractually or otherwise, to ensure any necessary documentation and assessments from suppliers will be furnished to BIS upon request either by the declarant, or, in cases including confidential business information, directly by the supplier; and

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

(2) *Covered software*: A connected vehicle manufacturer must submit a Declaration of Conformity to BIS prior to importing or selling in the United States completed connected vehicles that incorporate covered software, unless otherwise specified by this subpart. The Declaration of Conformity for covered software shall include:

(i) The name and address of the connected vehicle manufacturer, to include information identifying an individual point of contact (including name, email address, and phone number);

(ii) The make, model, trim, and Vehicle Identification Number (VIN) series applicable to the completed connected vehicles that incorporate the covered software;

(iii) A certification that the covered software described in the Declaration of Conformity was not designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia;

(iv) A certification that the declarant has conducted due diligence (with or without the use of third-party assessments) to inform the above certification, and the declarant or a delegated third party maintains documentation (either through an SBOM or otherwise) and third-party assessments (as applicable) that are sufficient to identify, at minimum, the author name, timestamp, component name, and supplier name of all proprietary additions to the development of the covered software, which can be made available upon request by BIS;

(v) Identification as to who maintains the documentation and third-party assessments (as applicable) as certified above;

(vi) A certification that the declarant has taken all possible measures, either contractually or otherwise, to ensure any necessary documentation and assessments from suppliers will be furnished to BIS upon request either by the declarant, or, in cases including confidential business information, directly by the supplier; and

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

(b) *Certification*. A certification is a written statement or attestation within a Declaration of Conformity in § 791.305(a) above to the U.S. Government, signed by a duly authorized designee, certifying under the penalties provided in 18 U.S.C. 1001, that the information provided is accurate and complete in all material respects to the best knowledge of the designee on behalf of the entity filing the Declaration of Conformity.

(1) For purposes of this section, a duly authorized designee is:

(i) In the case of a partnership, any general partner thereof;

(ii) In the case of a corporation, the chief executive officer, or any officer with the authority to bind the corporation;

(iii) An employee with authority to make certifications on behalf of the company as designated by a person in (i) or (ii); and

(iv) In the case of an entity lacking partners and officers, any individual manager, or designated agent who has been explicitly authorized by the board of directors or equivalent to sign contracts and make legally binding agreements on behalf of the entity.

(c) *Additional Information.* BIS may request additional information after receipt of a Declaration of Conformity.

(d) *Reliance on Third-Party Assessments*. Declarants are permitted to utilize assessments produced by third parties to assist and prepare a Declaration of Conformity, in addition to ensuring ongoing compliance with this rule, as long as such entities conform to § 791.315 of this subpart.

(e) *Material Changes*. The following events will require an update to a previously submitted Declaration of Conformity:

(1) The discovery, by the declarant, of an omission, inaccuracy, or error in the information provided to BIS in a prior Declaration of Conformity that could reasonably mislead as to the true source of VCS hardware or covered software in question.

(2) Covered software updates alone do not constitute a material change unless an additional condition above is true.

(f) *Change in circumstance.* If the connected vehicle manufacturer or VCS hardware importer determines that articles subject to a Declaration of Conformity are no longer eligible, it must, within 30 days, cease any prohibited conduct and submit a specific authorization application, pursuant to § 791.307(m).

(g) *Deadline to Submit Declarations of Conformity.* Connected vehicle manufacturers and VCS hardware importers shall submit Declarations of Conformity prior to the first sale of the subject connected vehicle in the United States, prior to the import of VCS hardware as specified in this section, and following discovery of a material change that makes a prior Declaration of Conformity no longer accurate.

(1) Connected vehicle manufacturers shall submit a Declaration of Conformity at least 60 days prior to the first import or first sale of each model year of completed connected vehicle that incorporates covered software. Declarants may submit a single Declaration of Conformity for all connected vehicles that use the same covered software, grouped by make, model, and VIN series.

(2) VCS hardware importers shall submit a Declaration of Conformity at least 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) Connected vehicle manufacturers and VCS hardware importers must notify BIS of any material change to the information conveyed in a previously submitted Declaration of Conformity by submitting a revised Declaration of Conformity within 60 days following the discovery of such change. A declarant’s obligation to inform BIS of material changes to the information ceases 10 years after submission of the original Declaration of Conformity for that model year or calendar year.

(h) *Annual updates to Declarations of Conformity.* If applicable, connected vehicle manufacturers and VCS hardware importers may, in lieu of submitting a new Declaration of Conformity, submit a confirmation that the prior Declaration of Conformity remains accurate and that associates the relevant new model year of vehicles (if known) in lieu of submitting a new Declaration of Conformity.

(1) Where there are no material changes to the covered software for a subsequent model year of completed connected vehicles, the connected vehicle manufacturer may submit a confirmation no later than one year after the previous submission, certifying that the prior information remains accurate, and that associates the new relevant model year of vehicles to an existing Declaration of Conformity.

(2) Where there are no material changes to the VCS hardware for a subsequent model year of completed connected vehicles (if known) or calendar year, the VCS hardware importer may submit a confirmation no later than one year after the previous submission, certifying that the prior information remains accurate, and that associates the new relevant model year of vehicles (if known) to an existing Declaration of Conformity.

(i) *Submission Instructions*. The declarant shall follow the electronic filing instructions on BIS's website, https://www.bis.gov/OICTS.

(j) *Verification.* BIS, in its sole discretion, may choose to verify Declarations of Conformity that have been submitted by VCS hardware importers and connected vehicle manufacturers.

(k) *Connected vehicle introduced by means of false information in the Declaration of Conformity.* Any person who submits false information in a Declaration of Conformity, with knowledge that such information is false, and engages in one or more prohibited transactions, may incur penalties as defined in § 791.318.

(l) *Exemptions*. No Declaration of Conformity is required if the only foreign interest in a transaction arises from a foreign person's equity ownership of a U.S. person, whether through ownership of public shares or otherwise. This exemption has no effect on transactions where a

foreign interest arises from a foreign entity's design, development, manufacture, or supply of VCS hardware or covered software for a U.S. person or where equity ownership allows a foreign person to exercise control over the U.S. person. Further, this exemption has no effect on the analysis of whether or not an entity is owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

§ 791.306 General authorizations.

(a) *Overview*. VCS hardware importers and connected vehicle manufacturers may rely on a general authorization to engage in an otherwise prohibited transaction if they meet the stated requirements or conditions identified in the general authorization and are not subject to the restrictions identified in this section. Records demonstrating compliance with the terms of general authorizations must be retained for a period of 10 years, as specified in § 791.312, and be made available to BIS upon request.

(b) *General course of procedure.* BIS may issue general authorizations for certain types of transactions subject to the prohibitions contained in this subpart. In determining whether to issue a general authorization, BIS may consider any information or material BIS deems relevant and appropriate, classified or unclassified, from any Federal department or agency, or from any other source. BIS will publish general authorizations it issues under this subpart on its website (https://www.bis.gov/OICTS), and will also publish them in the *Federal Register*.

(c) *Relationship with specific authorizations*. BIS will not grant specific authorizations for transactions in which a general authorization is applicable.

(d) *Instructions*. Persons availing themselves of certain general authorizations may be required to file reports and statements in accordance with the instructions specified by BIS in each general authorization. Failure to fulfill instructions provided in a general authorization may nullify the authorization and result in a violation of the applicable prohibitions that may be subject to BIS enforcement action.

(e) *Change in circumstance.* Unless otherwise prescribed by BIS, within 30 days of discovering a change in circumstance, the VCS hardware importer or connected vehicle manufacturer must assess if it still qualifies for the general authorization.

(1) If the connected vehicle manufacturer or VCS hardware importer determines that articles subject to a general authorization have been used outside the conditions of the general authorization, it must, within 30 days of such a determination, cease any prohibited conduct, conduct an internal inquiry, and submit to BIS a report identifying any prohibited transactions, the number of connected vehicles or VCS hardware units implicated, and proposed remedial measures.

(f) *Verification.* BIS may, at its discretion, seek verification from VCS hardware importers and connected vehicle manufacturers as to whether they are relying on a general authorization, and if so, may request documentation to verify compliance with this subpart.

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

(1) BIS has notified, either directly or through an advisory opinion, the VCS hardware importer or connected vehicle manufacturer is not eligible for a general authorization; or

(2) The VCS hardware importer or connected vehicle manufacturer is owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

§ 791.307 Specific authorizations.

(a) *Prohibited transactions authorized*. Upon receipt of a valid and complete application, BIS may grant specific authorizations to permit a VCS hardware importer or connected vehicle manufacturer to engage in an otherwise prohibited transaction.

(b) *Policy.* It is the policy of BIS not to review applications for specific authorizations for transactions that are otherwise 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, including persons responsible for assembling and packaging VCS hardware or covered software;

(3) If known, the make, model, and trim of the connected vehicle(s) 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, such as any ISO/SAE 21434 Threat Analysis and Risk Assessments (if available);

(6) An assessment of 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;

(7) Security standards used by the applicant with respect to the VCS hardware or covered software; and

(8) Other actions and proposals such as technical controls (*e.g.*, software validation) or operational controls (*e.g.*, physical and logical access monitoring procedures) the applicant intends to take to mitigate undue or unacceptable risk, if applicable.

(d) *Application submission procedures and timing.* VCS hardware importers or connected vehicle manufacturers who seeks to engage in an otherwise prohibited transaction must submit an application for a specific authorization in writing prior to engaging in the transaction, and await a

decision from BIS prior to engaging in the transaction. Specific authorization submissions must be delivered to BIS as specified on its website, https://www.bis.gov/OICTS.

(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. BIS may request an oral briefing by the applicant and any other relevant parties. The applicant may present additional information concerning an application for a specific authorization at any time before BIS issues its decision regarding the application.

(g) *Review and decisions.* Applications for specific authorizations will be reviewed on a case-by-case basis, and conditions to be applied to each specific authorization may vary as needed to mitigate any risk that arises as a result of the otherwise prohibited transaction. Such review will include an evaluation of the risks and potential mitigation measures proposed by the applicant for the particular transaction. The risks that BIS may consider include, but are not limited to, risks of data exfiltration from, and remote manipulation or operation of, the connected vehicle and the extent and nature of foreign adversary involvement in the design, development, manufacture, or supply of the VCS hardware or covered software. Mitigation may 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 intends to take to mitigate undue or unacceptable risk. BIS will advise each applicant in writing of the decision respecting the filed application. Decisions regarding specific authorizations will not be made publicly available.

(h) *Processing period.* BIS will provide a decision regarding an application for a specific authorization within 90 days unless BIS determines, in its sole discretion, and notifies the applicant

within that 90-day period, that additional time is required. Failure or delays by the applicant in submitting additional information requested by BIS may delay or prevent BIS's ability to issue a specific authorization.

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

(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) As a condition for the issuance of any specific authorization, BIS may require the applicant to submit third-party assessments or SBOMs/HBOMs 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.

(3) Any materially false or misleading representation in or otherwise associated with the application, or in any document submitted in connection with the application under this section, shall cause the specific authorization to be deemed void as of the date of issuance, and the applicant may incur penalties as specified in § 791.318.

(j) *Verification.* BIS may establish, in its sole discretion as conditions for receiving a specific authorization, any compliance, auditing, or verification requirements.

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

(l) *Effect of specific authorization.* (1) No specific authorization issued under this subpart, or otherwise issued by BIS, permits or validates any prohibited transaction effectuated 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.

(4) Specific authorizations will be approved for a duration of no less than one (1) model year or calendar year except as provided in § 791.307(m).

(m) *Exceptions.* BIS may approve specific authorizations for a period of less than one (1) calendar year on a case-by-case basis under the following circumstances:

(1) 2027 model years that include covered software and are actively being sold or imported as of the effective date of this rule;

(2) Covered software and VCS hardware supply chains that are affected by force majeure events;

(3) As a result of a corporate merger, investment, acquisition, joint venture, or conversion of equity (such as from debt) that occurs during model year production;

(4) As a result of the closure or relocation of facilities involved in the production of covered software or VCS hardware; and

(5) Other instances as determined by BIS.

(n) *Records.* Persons receiving a specific authorization are required to maintain records for a period of 10 years, as required in § 791.312, as well as to submit reports and statements in accordance with the instructions specified in each specific authorization.

(o) *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, the VCS hardware is imported as part of a connected vehicle with a model year prior to 2030, or the VCS hardware is imported for purposes of repair or warranty for 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 §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 claiming to be 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 a 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. The responsibilities of an appeals coordinator may include presiding over informal hearings.

(c) *Appeals procedures*—(1) *Filing*. 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 NW, Washington,

DC 20230 no later than 45 days after the date appearing on the written notice of administrative action.

(2) *Content of appeal*. 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 from the appellant. The Under Secretary or the designated official will not ordinarily accept any submission filed voluntarily more than 30 days after the filing of the appeal.

(3) *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.

(d) *Informal hearing procedures*—(1) *Presentations*. 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 BIS. 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.

(2) *Evidence*. 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.

(3) *Procedural questions.* 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.

(4) *Transcript*. 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 if 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.

(5) *Report*. 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.

(e) *Amicus filings.* At the request of the appellant, parties not subject to the administrative action under appeal may submit amicus filings in support of the appellant prior to any informal hearing.

(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 to determine whether a prospective transaction is subject to a prohibition, or requirement under this subpart. The requestor must have a direct financial interest in the substance of the question(s) presented, and the submission must include the name of the parties to the transaction.

(b) Requests for advisory opinions must be delivered to BIS as specified on its website, https://www.bis.gov/OICTS.

(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, telephone, and email address of the submitter;

(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) 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 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; and

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

(d) BIS may consider third-party materials on a case-by-case basis as part of its review of an advisory opinion request. Each person that submits an advisory opinion request or information in support of another party's advisory opinion request shall provide any additional information or documents that BIS may thereafter request in its review of the matter.

(e) BIS shall issue an advisory opinion within 60 days of the request unless it notifies the requester within that 60-day period that more time is required. Failure or delays by the applicant in submitting additional information requested by BIS may delay or prevent BIS's ability to issue an advisory opinion.

(f) 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 to reflect circumstances accurately and completely 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.

(g) 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.

(h) BIS may, at its sole discretion, decline to issue an advisory opinion within 60 days after receipt of the request.

§ 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.

(a) Except as otherwise provided herein, or through subsequent communication with BIS, VCS hardware importers, connected vehicle manufacturers, and/or third-party assessors (if applicable) shall keep all primary business records related to the execution of each transaction for which a Declaration of Conformity, general authorization, or specific authorization would be required under §§ 791.305, 791.306, or 791.307. Primary business records include contracts, import records, commercial invoices, bills of sale, corporate policy documentation, and reports produced by third parties created for the purposes of compliance with this rule. Regardless of whether these transactions are effectuated pursuant to a general authorization, specific authorization, or otherwise, such records shall be available for examination for at least 10 years after the date of such transactions.

(b) Third-party assessors are required to maintain all records relating to third-party verification or assessment of a U.S. person's compliance with this rule.

§ 791.313 Reports to be furnished on demand.

(a) VCS hardware importers and connected vehicle manufacturers must furnish, under oath, in the form of reports or as otherwise specified by BIS, and at any time as may be required by BIS, complete information regarding any transaction involving the import of VCS hardware or the import or sale of completed connected vehicles incorporating covered software. This requirement applies regardless of whether such transaction is affected pursuant to a general or specific 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. Reports being submitted to BIS pursuant to this section must be retained for a period of 10 years, as specified in § 791.312.

(b) 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.

(c) Persons providing records to BIS pursuant to this section shall follow the electronic filing instructions on BIS's website, https://www.bis.gov/OICTS.

§ 791.314 Confidential Business Information.

(a) *Confidential business information.* Confidential Business Information is defined in 19 CFR 201.6.

(b) *Submission procedures.* Any information or material submitted to BIS which the entity or any other party desires to submit in confidence as a part of a Declaration of Conformity, specific authorization application, advisory opinion request, record to be furnished on demand, or is otherwise Confidential Business Information should be contained within a file beginning its name with the characters "CBI." Any page containing Confidential Business Information must be clearly marked "CONFIDENTIAL BUSINESS INFORMATION" on the top of the page. Any pages not containing Confidential Business Information should not be marked. By submitting information or material identified as Confidential Business Information, the entity or other party represents that the information is exempted from public disclosure, either by the Freedom of Information Act (5 U.S.C. 552 *et seq*.) or by another specific statutory exemption. Any request for Confidential Business Information treatment must be accompanied at the time of

submission by a statement justifying non-disclosure and referring to the specific legal authority claimed.

(c) *Confidentiality of information.* Confidentiality of information is subject to 15 CFR 791.102.

§ 791.315 Third-Party Verification and Assessments.

(a) *Overview.* U.S persons subject to this subpart may hire, consult, or otherwise contract with a third-party to ensure compliance with this rule. In certain cases, the use of a third-party assessor will be mandated in the terms of an approved specific authorization.

(b) *Third-Party Assessors.* U.S. persons should determine whether a third-party assessor is qualified and competent, such as through industry certification or standard, to examine, to verify, and attest to the U.S. person's compliance with and the effectiveness of the security requirements implemented for VCS hardware or covered software transactions.

(1) The third-party assessor cannot be a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

(2) In determining the reasonableness of an entity's reliance on a third-party assessment, BIS will consider the independence of the third-party, including any financial incentives between the third-party and the entity.

(c) *Scope.* The use of a third-party assessor for U.S. persons submitting Declarations of Conformity is voluntary; however, if utilized, BIS recommends such third-party assessments to:

(1) identify and examine the VCS hardware importer or connected vehicle manufacturer's VCS hardware and covered software supply chains in relation to the prohibitions in this subpart;

(2) examine compliance relating to each Declaration of Conformity, general authorization, or specific authorization pursuant to which an entity is conducting transactions;

(3) use a reliable methodology to conduct the third-party verification; and

(4) acknowledge that the assessment may be used by the U.S. government to verify compliance.

(d) *Assessment.* To utilize third-party verification to fulfill the due diligence requirement for a Declaration of Conformity, the third-party assessor should prepare and submit a written report to the VCS hardware importer or connected vehicle manufacturer. The third-party assessment should at minimum:

(1) identify the suppliers of each relevant component and describe the nature of any foreign interest;

(2) describe the methodology undertaken, including the policies and other documents reviewed, personnel interviewed, and any facilities, equipment, or systems examined;

(3) describe the effectiveness of the VCS hardware importer or connected vehicle manufacturer's corporate policies related to compliance with this rule;

(4) for VCS hardware importers or connected vehicle manufacturers conducting transactions under the auspices of a general authorization or specific authorization, describe any vulnerabilities or deficiencies in the implementation of the authorization; and

(5) recommend any improvements or changes to policies, practices, or other aspects to maintain compliance with this subpart, as applicable to each transaction.

(e) *Recordkeeping.* The third-party assessor must comply with all recordkeeping requirements, pursuant to § 791.312.

§ 791.316 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 and may include a responsive administrative action other than a civil monetary penalty. 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.

§ 791.317 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 either electronically or by mail 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. BIS will consider any voluntary disclosures of a violation prior to issuing such notice.

(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) *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.

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

§ 791.318 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 and therefore may be subject to additional penalties not specified in this section.

§ 791.319 Penalty imposition.

(a) If, after considering any written response to the pre-penalty notice and any relevant facts, including voluntary disclosure of a violation, 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.

§ 791.320 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 United States 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.

§ 791.321 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. 2025-00592 Filed: 1/14/2025 8:45 am; Publication Date: 1/16/2025]