BILLING CODE: 3510-33

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

15 CFR Part 7

[Docket No. 240227-0060]

RIN 0694-AJ56

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

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

ACTION: Advance notice of proposed rulemaking.

SUMMARY: In this advance notice of proposed rulemaking (ANPRM), the Department of Commerce's (Department) Bureau of Industry and Security (BIS) seeks public comment on issues and questions related to 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 foreign countries or foreign non-government persons identified in the Department's regulations, pursuant to the Executive Order (E.O.) entitled "Securing the Information and Communications Technology and Services Supply Chain," and that are integral to connected vehicles (CVs), as defined herein. This ANPRM will assist BIS in determining the technologies and market participants that may be most appropriate for regulation pursuant to the E.O.

DATES: Comments must be received on or before [insert date 60 days after publication in the FEDERAL REGISTER].

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

• *The Federal eRulemaking Portal*: https://www.*regulations.gov* at docket number BIS-2024-0005.

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

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

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

SUPPLEMENTARY INFORMATION:

I. Authorities

On May 15, 2019, the President issued E.O. 13873, "Securing the Information and Communications Technology and Services Supply Chain," pursuant to the President's authority under the Constitution and the laws of the United States, including the International Emergency Economic Powers Act (IEEPA), the National Emergencies Act (50 U.S.C. 1601, et seq.), and Section 301 of Title 3, United States Code. E.O. 13873 declares a national emergency regarding the ICTS supply chain, finding that "the unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign

policy, and economy of the United States." The E.O. further notes that "[t]his threat 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."

In accordance with the National Emergencies Act, the President has declared each year since E.O. 13873 was published that the national emergency continues in effect. *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).

To address identified risks to national security from ICTS transactions, E.O. 13873 grants the Secretary of Commerce (Secretary) (in consultation with other agency heads identified in the E.O.) the authority to review and, if necessary, impose mitigation measures on or prohibit any ICTS transaction, which includes any acquisition, importation, transfer, installation, dealing in, or use of any ICTS by any person, or with respect to any property, subject to United States jurisdiction, when the transaction involves any property in which a foreign country or national has any interest. In order to require mitigation for or to prohibit an ICTS transaction or class of transactions, the Secretary, in consultation with other agency heads, must first determine that the ICTS transaction or class of transactions at issue: (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, which the E.O. defines as "any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct

significantly adverse to the national security of the United States or security and safety of United States persons;" and (2) poses:

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

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

These factors are collectively referred to as "undue or unacceptable risks."

E.O. 13873 additionally provides the Secretary with the authority to issue rules establishing criteria by which particular technologies or market participants may be categorically included in or categorically excluded from prohibitions established pursuant to the E.O. To date, the Department has not pursued or used this authority to regulate ICTS transactions on a category- or class-wide basis. Furthermore, E.O. 13873 grants the Secretary the authority to identify a mechanism and relevant factors for the negotiation of mitigation measures that would allow approval of an otherwise prohibited transaction.

II. Background

a. Purpose

Pursuant to the authority delegated to the Secretary under E.O. 13873, BIS is considering proposing rules that would prohibit certain ICTS transactions or classes of ICTS transactions by or with persons who design, develop, manufacture, or supply ICTS integral to CVs and are owned by, controlled by, or subject to the jurisdiction or direction of foreign governments or foreign non-government persons identified at 15 CFR 7.4 (hereinafter referred to as "15 CFR 7.4 entities"). BIS is also considering proposing measures that would allow market participants to engage in otherwise prohibited transactions or classes of transactions if the undue or

unacceptable risks of those ICTS transactions can be sufficiently mitigated using measures that are monitorable.

The purpose of this ANPRM is to gather information to support BIS's potential development of a rule regarding ICTS integral to CVs. In particular, BIS seeks public input on certain definitions and its assessment of how a class of transactions involving ICTS integral to CVs, when designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity, could present undue or unacceptable risks to U.S. national security. These include risks related to threats from 15 CFR 7.4 entities, capabilities of CVs that may increase the likelihood of vulnerabilities, and consequences to U.S. persons and critical infrastructure if these vulnerabilities are exploited or intentionally inserted by 15 CFR 7.4 entities. BIS solicits input on the ICTS most integral to CVs and most vulnerable to compromise, as well as input on mechanisms to address identified risks through potential design, implementation standards and protocols, manufacturing integrity protection systems and procedures, or prohibitions.

BIS recognizes the benefits of CV technologies and does not imply through this ANPRM that technologies such as vehicle-to-everything (V2X) communications are generally unsafe for use in the United States. Indeed, these new vehicles often provide safer, more fuel-efficient travel. However, E.O. 13873 is focused on risks that ICTS transactions might present to national security. Therefore, this ANPRM, which is being issued pursuant to the authorities granted under E.O. 13873, seeks public comment on potential means to narrowly address involvement by persons owned by, controlled by, or subject to the jurisdiction or direction of 15 CFR 7.4 entities in the design, development, manufacture, or supply of ICTS integral to CVs where that involvement may create undue or unacceptable risk to U.S. national security.

Additionally, BIS seeks comment on whether to create a process for the public to request approval to engage in an otherwise prohibited transaction by demonstrating that a particular transaction adequately addresses the risk to U.S. national security. BIS encourages public

feedback to help inform the rulemaking process, particularly regarding transactions where ICTS supply chains may be impacted by any proposed rule.

b. Definitions

As an initial matter, BIS is interested in receiving comments on the applicable definition for *connected vehicle* or *CV* within the context of transactions involving ICTS incorporated into such vehicles. BIS could define a *connected vehicle* as an automotive vehicle that integrates onboard networked hardware with automotive software systems to communicate via dedicated short-range communication, cellular telecommunications connectivity, satellite communication, or other wireless spectrum connectivity with any other network or device. Such a definition would likely include automotive vehicles, whether personal or commercial, capable of global navigation satellite system (GNSS) communication for geolocation; communication with intelligent transportation systems; remote access or control; wireless software or firmware updates; or on-device roadside assistance.

CVs also integrate hardware that enables connectivity within the vehicle and/or external connectivity with devices, networks, applications, and services outside the vehicle. CV safety applications are designed to increase situational awareness and reduce traffic accidents through vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and increasingly, V2X communications, as contemplated in a series of Department of Transportation workshops focusing on V2X communications titled "Saving Lives with Connectivity." *See* Bill Canis, Cong. Research Serv., R46398, *Motor Vehicle Safety: Issues for Congress* 8 (2021), https://sgp.fas.org/crs/misc/R46398.pdf; U.S. Dep't of Transp., ITS V2X Communications Summit (2023), https://www.its.dot.gov/research_areas/emerging_tech/htm/ITS_V2X_CommunicationSummit.htm

BIS arrived at this definition by reviewing existing definitions for connected vehicles from trade associations and leading research publications including the Connected Vehicle Reference

Implementation Architecture, U.S. Department of Transportation's Intelligent Transportation Systems Joint Program Office, Institute of Electrical and Electronics Engineers research, and Society of Automotive Engineers standards.

Various terms exist across industry and the U.S. Government to refer to vehicles that exhibit the connected features explained above. In addition to input on the term *connected vehicle*, BIS is seeking comment on alternative terminology that might better correspond to the definition of *connected vehicle* discussed above. Such terminology could include "networked vehicles," "intelligent connected vehicles," "software-defined vehicles," or "connected autonomous vehicles."

This ANPRM seeks comment on the definitions to use for a rule regarding transactions involving ICTS integral to CVs, and specifically:

1. In what ways, if any, should BIS elaborate on or amend the potential definition of *connected vehicle* stated above? If amended, how will the revised definition enable BIS to better address national security risks arising from classes of transactions involving ICTS integral to CVs?

2. Is the term *connected vehicles* broad enough to include autonomous vehicles and related equipment, electric vehicles, or other alternative power sources and related technologies? Does a better term exist to describe the broader scope?

3. Are there other commonly used definitions for CVs that BIS should consider when defining a class of ICTS transactions, including definitions from industry, civil society, and foreign entities? If so, why would those definitions be more appropriate for the purposes of a rule?

c. *Risks associated with Connected Vehicles*

The automotive industry is constantly undergoing innovation and change, and as communications and broadband technology advance, so do the technologies used in automobiles. Particularly relevant for the purposes of this ANPRM, new technology has fueled a rise in

interconnectivity and autonomous capabilities in new vehicles. An automobile's value is no longer determined only by the engine, steering system, and other traditional automotive parts. Increasingly, an automobile is a compilation of on-board computers; sensors; cameras; batteries; and various other categories of ICTS software or hardware tied together through automotive software systems. Over time, vehicle connections to the internet will evolve even further and new communication technology will advance vehicle capabilities. These technological advances will continue to rely on significant data collection not only about the vehicle and its myriad components, but also the driver, the occupants, the vehicle's surroundings, and nearby infrastructure. Moreover, CVs allow for information to be gathered and shared to address both individual and societal transportation needs. These technologies may expose the vehicles, and the sectors they support, to new cyber-enabled attack vectors and vulnerabilities, with the potential to create novel and potentially profound risks to national security and public safety. Cyber-enabled vulnerabilities can be exacerbated if the ICTS integral to CVs is designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity.

i. Threat from 15 CFR 7.4 entities

E.O. 13873 defines the term "foreign adversary" to mean 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 U.S. persons. In the rules implementing the E.O. at 15 CFR 7.4(a), the Secretary has identified the following as foreign adversaries: the People's Republic of China, including the Hong Kong Special Administrative Region (PRC); Republic of Cuba; Islamic Republic of Iran; Democratic People's Republic of Korea; Russian Federation; and Venezuelan politician Nicolás Maduro (Maduro Regime).

The incorporation of ICTS products and services used in the United States from persons owned by, controlled by, or subject to the jurisdiction or direction of 15 CFR 7.4 entities' can

offer a direct entry point to sensitive U.S. technology and data and bypass measures intended to protect U.S. persons' safety and security. This may allow actors with insider access to gain entry to the systems the ICTS connects to and ultimately engage in malicious cyber activity. Consequently, this exploitation may result in undue risks to ICTS and critical infrastructure in the United States and unacceptable risks to national security.

The PRC presents a particularly acute and persistent threat to the United States ICTS supply chain. According to the Office of the Director of National Intelligence, the PRC likely represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks. *See* Off. Of the Director of Nat'l Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* 10 (2023), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf. The PRC is almost certainly capable of launching cyber-attacks that could disrupt critical infrastructure services within the United States and has conducted cyber espionage operations that have compromised telecommunications firms, providers of managed services, and broadly used software. *Id.* At 10. In short, the PRC has engaged in a pattern of hacking and cyber intrusion that demonstrates the PRC's intent to compromise and exploit U.S. ICTS supply chains and critical infrastructure, threatening U.S. national security.

The PRC's legal structure also gives broad authority to the state to co-opt private companies to pursue its objectives. A host of laws give the PRC government the authority to compel companies located in the PRC, including automakers and their suppliers, to cooperate with PRC intelligence and security services. The PRC's 2021 Data Security Law, for example, makes all private data available to the PRC state when it is needed for "national security." *See* National People's Congress, *Data Security Law of the People's Republic of China*, Art. 35, http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html. The PRC's 2017 National Intelligence Law imposes affirmative obligations on entities and persons subject to the PRC's jurisdiction to cooperate with intelligence agencies—Article 17 allows PRC

intelligence officials to take control of a private organization's facilities, including its communications equipment. *See* National People's Congress, *National Intelligence Law (as amended, 2018)*, http://www.npc.gov.cn/npc/c2/c30834/201905/t20190521_281475.html. The PRC's 2015 National Security Law obliges citizens and private companies to provide security and military agencies with all "necessary support and assistance." *See* State Council of the People's Republic of China, *National Security Law*, Art. 77 (5), https://www.gov.cn/zhengce/2015-07/01/content_2893902.htm. Beyond legal obligations, companies established in the PRC may be required to create internal Chinese Communist Party (CCP) committees that can exercise influence over corporate decisions. *See* National People's Congress, *Company Law of the People's Republic of China*, Art. 19, https://www.npc.gov.cn/zgrdw/npc/xinwen/2018-11/05/content_2065671.htm.

The combination of legal authorities and opaque CCP influence make private companies that are subject to the PRC's jurisdiction susceptible to requests from intelligence and military officials. PRC officials can compel PRC firms to provide the PRC government with data, logical access, encryption keys, and other vital technical information, as well as to install backdoors or bugs in equipment which create security flaws easily exploitable by PRC authorities. U.S. Dep't of Homeland Security, *Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the Peoples Republic of China* 2 (2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf. Original equipment manufacturers (OEMs) for vehicles in the PRC, due to the vast amounts of data generated by their products, are notable targets for government access. According to open-source reporting, over 200 automakers that operate in the PRC are legally obligated to transmit real-time vehicle data, including geolocation information, to government monitoring centers. *See* Erika Kinetz, *In China Your Car Could Be Talking To The Government*, ASSOCIATED PRESS NEWS (Nov. 29, 2018), https://apnews.com/article/4a749a4211904784826b45e812cff4ca. This pervasive data sharing,

which provides the PRC government with detailed information on the behaviors and habits of individuals, is indicative of a broader approach to co-opting private companies—one that raises significant concerns about how the PRC government might exploit the growing presence of PRC OEMs and manufacturers of ICTS integral to CVs in foreign markets. The combination of these factors uniquely elevates BIS's concern regarding PRC participation in the ICTS supply chain for CVs in the United States.

BIS seeks to better understand the role of persons owned by, controlled by, or subject to the jurisdiction or direction of 15 CFR 7.4 entities, particularly the PRC, in the ICTS supply chain for CVs, and the leverage these entities might exert as a result. In particular, the ANPRM seeks comments on the following issues:

4. Please describe the ICTS supply chain for CVs in the United States. Particularly useful responses may include information regarding:

a. categories of ICTS, such as software or hardware, that are integral to CVs operating in the United States;

b. market leaders for each distinct phase of the supply chain for ICTS integral to CVs (such as design, development, manufacturing, or supply) including, but not limited to: OEMs, tier one, tier two, and tier three suppliers, and service providers;

c. geographic locations where software (such as the vehicle operating system), hardware (such as light detection and ranging (LiDAR) sensors), or other ICTS components integral to CVs in use in the United States are designed, developed, manufactured, or supplied;

d. involvement in any sector or sub-sector of the U.S. ICTS supply chain for CVs by persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity; and

e. geographic locations where data from CVs in use in the United States is transmitted, stored, or analyzed.

5. Are there ICTS integral to CVs for which persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity are sole source suppliers? To what extent do OEMs of CVs in use in the United States rely upon suppliers wholly or partially owned by a company based in or under the control of a 15 CFR 7.4 entity?

6. In what ICTS hardware or software for CVs do persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity maintain a technological advantage over U.S. and other foreign counterparts and how may this dynamic evolve in the coming years?

7. How, and to what degree, does CV automotive software connect to GNSS systems that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity?

for geolocation and other functions?

8. How might a disruption to the supply of ICTS components for CVs in use in the United States, including hardware and software, from persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity affect OEMs of CVs in use in the United States and ICTS suppliers? Where possible, please specify which disruptions to component supply would be particularly detrimental.

9. To what extent can OEMs procure alternative sources of ICTS integral to CVs that do not constitute ICTS from persons owned by, controlled by, or subject to the jurisdiction or direction of 15 CFR 7.4 entities?

10. Please describe the relationship between OEMs of CVs in use in the United States and their ICTS suppliers. Particularly useful responses may include the type of information that is shared between OEMs of CVs in use in the United States and their ICTS suppliers in the normal course of business, how this information is shared, what access or administrative privileges are typically granted, and if suppliers have any capability for remote access or ability to provide firmware or software updates.

11. What risks might be posed by aftermarket ICTS integrated onboard CVs and interfaced with vehicle systems, such as tracking devices, cameras, and wireless-enabled diagnostic interfaces? Should aftermarket automotive systems or components be considered integral to CV operation?

12. To what extent are ICTS components of CVs designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity present in critical infrastructure sectors? Are there instances of municipal, state, or federal funding for procurement of such 15 CFR 7.4 entities' ICTS integral to CVs for use in critical infrastructure sectors?

13. What other instances exist where persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity, are integrated into the ICTS supply chain for CVs?

ii. Capabilities of Connected Vehicles may increase the likelihood of vulnerabilities 15 CFR 7.4 entities could exploit

CVs and the components that enable their functionality present opportunities for exploitation by 15 CFR 7.4 entities via insider access, which could potentially result in severe consequences to U.S. persons and critical infrastructure. Increasing the number and scope of wireless connected components in a vehicle also increases the attack surfaces through which a malicious actor can gain initial entry. As CVs gain new and different connectivity capabilities, design, implementation, and operational protocols need to be added to address new attack surfaces and maintain the confidentiality, integrity, and availability of the data that traverse any one functional system. As demonstrated in controlled environments, attack vectors can be exploited and may provide access to other functional systems within a CV. Moreover, once one subsystem has been compromised, depending on the nature of the vulnerability and the design of the vehicle network architecture, the attacker might have the ability to move laterally and eventually gain access to other functional automotive systems. While integrated functionality may provide seamless communication, comfort, and operability for the consumer, it is possible that unauthorized

remote access to a particular sensor system could be escalated to vehicle systems and operations, potentially resulting in injury, loss of life, and disruption to critical infrastructure networks.

Preliminarily, BIS has identified the following capabilities associated with CVs that may increase the likelihood of vulnerabilities that 15 CFR 7.4 entities could exploit:

Data Collection: CVs rely on the collection and integration of broad and varied data to improve the vehicle's functionality and safety. This data, which can encompass vehicle-level data (*e.g.*, driver behavior, vehicle status, geolocation, biometrics, driver mobile phone data) and environmental-level data (*e.g.*, detailed mapping data, object detection, traffic patterns), are extracted through various onboard systems and sensors. The Advanced Driver-Assistance System (ADAS) of a CV, for example, typically relies on a combination of sensors—radar, LiDAR, ultrasonic, audio, and video—that are constantly collecting and processing data. CVs now collect data inside the cockpit as well. Consumer and commercial CVs increasingly incorporate driver monitoring systems (DMS) to ensure the driver remains alert and fully able to take control of the car should autonomous systems fail, and to ensure commercial truck drivers remain on schedule. More sophisticated DMS feature driver-facing cameras—including eye tracking, facial recognition, and microphones—collect potentially sensitive information about drivers and passengers. This increases the sensitivity of the data that CVs collect, potentially providing 15 CFR 7.4 entities with access to biometric information in addition to environmental data.

Connectivity: CVs are connected to and can communicate with a range of external sources, including the OEM and third-party service providers, as well as in-car devices like smart phones. In an increasing subset of vehicles, telematics systems connect the vehicle with cloud-based services to provide onboard systems with external data streams (*e.g.*, geolocation, streaming service, assistance service, emergency notification) and underlie many of a CV's core functionalities. V2X systems, when widely implemented, will support the broadcast and reception of messages that enable safety alerts and mobility advisories. Providing broadcast

(radio) communication capabilities that facilitate driver assistance capabilities may open cybersecurity vectors that need to be addressed to ensure broadcast message integrity and authenticity through design, standards, implementation and manufacturing protocols, and to prevent possible message and transmission misbehavior.

Further, interconnectivity in the software or hardware components may amplify risks posed by ICTS integral to CVs that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity. For example, OEMs enable communication with their vehicle after sale even when a customer does not subscribe to services, including by providing software updates and refinements, as well as by enabling or disabling subscription-based features. This access by the OEM to the CV provides numerous opportunities for 15 CFR 7.4 entities that own, control, or have the ability to exert jurisdiction or direction over the OEM, to insert vulnerabilities allowing for future backdoor attacks and other malicious behavior. Additionally, individually connected components and sensors are capable of transmitting data separately from the vehicle's broader communications suite, including receiving over the air (OTA) updates without the knowledge or consent of the vehicle owner or OEM. BIS seeks to better understand the capabilities associated with technical trends—both current and future—in CV design and the ICTS components therein. In particular, the ANPRM seeks further comment on the following:

14. What is the full scope of data collection capabilities in CVs and the aggregation and scale of data that CVs could collect on U.S persons, entities, geography, and infrastructure? Who has authorized access to, or control of, data collected by CVs?

15. What types of remote access or control do OEMs have over their CVs? Please describe what software or other mechanisms allow for such remote access or control by the OEM to occur.

16. What cybersecurity concerns may arise from linkages between sensors in CVs? To what extent can individual sensors and components communicate OTA independently from the CV's Operating System (OS)?

17. What standards, best practices, and industry norms are used to secure the interconnection between vehicles and charging infrastructure? How are battery management systems (BMS) integrated into a vehicle's automotive software systems, and how are they protected from malware?

18. How do manufacturers supplement existing cybersecurity standards and best practices such as the National Highway Traffic Safety Administration's *Cybersecurity Best Practices for the Safety of Modern Vehicles* at each step of the CV supply chain, including design, manufacturing, and operation?

a. Particularly useful responses will be specific about the types of programs and practices used such as test and verification, bug bounties, white hat programs, or end-to-end encryption to secure the link between vehicle and server. *See* Nat'l Highway Traffic Safety Admin., *Cybersecurity Best Practices for the Safety of Modern Vehicles* (2022), https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf; *see also* Cybersecurity and Infrastructure Security Agency, *Autonomous Ground Vehicle Security Guide: Transportation Systems Sector* (2021), https://www.cisa.gov/resources-tools/resources/autonomous-ground-vehicle-security-guide

19. Please describe the automotive software development cycle. BIS is particularly interested in learning:

a. The degree to which OEMs license software, as opposed to developing it internally;

b. The extent to which software is developed outside the United States and, if so, where;

c. What measures are taken to ensure software security and integrity during the development cycle;

d. If OEMs partner or co-develop automotive software with any persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity; and

e. The extent to which software that is embedded in hardware (*e.g.*, firmware) is subject to the development cycle described above.

20. Please describe the relationship between CV OEMs and cloud service providers (CSPs). Particularly useful responses may describe what access privileges, controls, and remote capabilities with respect to CV OEM systems are afforded to the CSP. Additionally, what are the common shared responsibility models between a CSP and a CV OEM and how are the communication and systems protected?

21. How do CV OEMs verify the bill of materials and software bill of materials as authentic for vendors and suppliers, specifically regarding OS, telematic systems, ADAS, Automated Driving Systems (ADS), satellite or cellular telecommunication systems, and BMS? If a software bill of materials is required, to what extent does it provide information regarding software vulnerabilities, and how is this information used, stored, and protected?

22. To what extent is software from vendors and suppliers tested and verified to comply with OEM requirements?

23. What vendor-vetting and supply chain security practices do OEMs employ when procuring ICTS integral to CVs?

iii. Consequences

The ability of a 15 CFR 7.4 entity to compel private companies through applicable legal frameworks, combined with the exploitation of vulnerabilities created by the increase in capabilities of the ICTS integral to CVs, has the potential to create severe and, in certain instances, catastrophic consequences for U.S. persons and critical infrastructure. Through ICTS designed, developed, manufactured, or supplied by persons subject to the ownership, control, jurisdiction, or direction of a 15 CFR 7.4 entity, the intelligence agencies of that entity could obtain access to a wide range of information from companies in the CV ICTS supply chain to exfiltrate, collect, and aggregate sensitive data on U.S. persons. These data include location, traffic patterns, audio and video recordings of the inside and outside of the car, as well as

information about the driver's identity, finances, contacts, and home address, which can be collected by CVs themselves or by a passenger's mobile device connected to a CV.

In addition, backdoors embedded in a CV's software could enable a 15 CFR 7.4 entity under certain conditions to obtain control over various vehicle functions that could include the ability to disable the vehicle completely. A group of researchers were able to demonstrate a vulnerability in an OEM's Bluetooth software that allowed access to some vehicle control systems, initiating remote actions such as activating the brakes and turning the steering wheel. *See* Consumer Watchdog, *Kill Switch: Why Connected Cars Can Be Killing Machines and How to Turn Them Off* 37–40 (2019), https://consumerwatchdog.org/sites/default/files/2019-07/KILL%20SWITCH%20%207-29-19.pdf. A similar ability in the hands of a 15 CFR 7.4 entity that can control or direct an OEM could allow that entity to disable the controls on an individual vehicle while it was being driven or to sabotage entire fleets without having physical access to the vehicles. Finally, because of CVs' connectivity, they could be used to access multiple critical infrastructure systems with which they interact, including telecommunications networks, transportation systems, and the electrical grid. As CV technology advances, vehicles and charging infrastructure may increasingly communicate with these systems to manage traffic flows and grid load. As such, the proliferation of CVs containing vulnerable ICTS from persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity could provide that entity with a platform for launching distributed denial of service attacks against intelligent transportation systems, satellite or cellular communications hardware, or other critical infrastructure. *See* Mohammad Ali Sayed, et al., *Electric Vehicle Attack Impact on Power Grid Operation*, 137 INT'L J. ELECTRICAL POWER & ENERGY SYS. 107784 (2022), https://www.sciencedirect.com/science/article/abs/pii/S0142061521010048; Numaan Huq, et al., *Cybersecurity for Connected Cars: Exploring Risks in 5G, Cloud, and Other Connected Technologies*, TREND MICRO RES. (2021), https://documents.trendmicro.com/assets/white_papers/wp-cybersecurity-for-connected-cars-

exploring-risks-in-5g-cloud-and-other-connected-technologies.pdf; Anastasios Giannaros, et al., *Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions*, 3 J. OF CYBERSECURITY AND PRIVACY 493 (2023). Given these threats, vulnerabilities, and potential consequences, BIS is considering identifying the following automotive software systems as the ICTS integral to CVs most likely to present undue or unacceptable risks if exploited by 15 CFR 7.4 entities: (i) vehicle OS; (ii) telematics systems; (iii) ADAS; (iv) ADS; (v) satellite or cellular telecommunication systems; and (vi) BMS.

As BIS considers whether and how to regulate these software systems, it seeks additional information, including:

24. Are there ICTS integral to CVs other than those identified in this ANPRM that could present material risks if they were designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction of a 15 CFR 7.4 entity? If so, please discuss how the ICTS could be exploited to pose such a risk.

25. Of the ICTS integral to CVs identified in this ANPRM, which present the greatest risk to safety or security if they are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a 15 CFR 7.4 entity?

26. As ADS systems evolve and developers rely on cellular systems to communicate with ADS-enabled vehicles to support overall operational capability (*e.g.*, communications to a fleet management office), what should the U.S. government consider in order to support the development of this technology securely from 15 CFR 7.4 entity malign activity?

III. Additional Questions for Comment

This ANPRM seeks comment on processes and mechanisms that BIS could implement in a potential rule to authorize an otherwise prohibited ICTS transaction with the adoption of mitigation measures.

Authorizations and Mitigations

27. In what instances would granting a temporary authorization to engage in an otherwise prohibited transaction under a proposed rule be necessary and in the interest of the United States to avoid supply chain disruptions or other unintended consequences?

28. What review criteria should BIS implement when considering an application for a temporary authorization?

29. What specific standards, mitigation measures, or cybersecurity best practices should BIS consider when evaluating the appropriateness of a requested authorization?

30. Are there any U.S. government models, such as the Office of Foreign Assets Control's sanctions programs or the Export Administration Regulations, that this program should consider emulating in granting authorizations?

Economic Impact

31. What economic impacts to U.S. businesses or the public, if any, might be associated with the regulation of ICTS integral to CVs contemplated by this ANPRM? If responding from outside the United States, what economic impacts to local businesses and the public, if any, might be associated with regulations of ICTS integral to CVs?

32. What, if any, anticompetitive effects may result from regulation of ICTS that is integral to CVs as contemplated by this ANPRM? And what, if anything, can be done to mitigate the anticompetitive effects of regulation of ICTS?

33. What types of U.S. businesses or firms (*e.g.*, small businesses) would likely be most impacted by the program contemplated in this ANPRM? If responding from outside the United States, what types of local businesses or firms (*e.g.*, small businesses) would likely be most impacted by the program contemplated in this ANPRM?

34. What actions can BIS take, or provisions could it add to any proposed regulations, to minimize potential costs borne by U.S. businesses or the public? If responding from outside the United States, what actions can BIS take, or what provisions could it add to any proposed regulations, to minimize potential costs borne by local businesses or the public?

35. What new due diligence, compliance, and recordkeeping controls will U.S. persons anticipate needing to undertake to comply with any proposed regulations regarding ICTS integral to CVs that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of 15 CFR 7.4 entities?

Elizabeth L. D. Cannon,

Executive Director, Office of Information and Communications Technology and Services.

[FR Doc. 2024-04382 Filed: 2/29/2024 8:45 am; Publication Date: 3/1/2024]