ALLIANCE FOR AUTOMOTIVE INNOVATION

April 30, 2024

Elizabeth L.D. Cannon
Executive Director
Office of Information and Communications Technology and Services
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, D.C. 20230

RE: Advance Notice of Proposed Rulemaking on Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles

Dear Executive Director Cannon:

The Alliance for Automotive Innovation ("Auto Innovators") appreciates the opportunity to provide input to the Bureau of Industry and Security ("BIS") on its *Securing the Information and Communications Technology and Services Supply Chain: Connected Car* Advance Notice of Proposed Rulemaking ("ANPRM"). The auto industry welcomes the opportunity to provide input to and collaborate with BIS on this important topic.

Auto Innovators represents the manufacturers that produce most of the cars and light trucks sold in the U.S., original equipment suppliers, battery makers, technology companies, and other value chain partners within the automotive ecosystem. Representing approximately 5 percent of the country's GDP, responsible for supporting 10 million jobs, and driving $1 trillion in annual economic growth, the automotive industry is the nation's largest manufacturing sector.

The automotive industry is undergoing a once-in-a-century transformation to cleaner, safer, and smarter vehicles. This transformation has the potential to bring many societal, economic, and safety benefits to United States consumers and road users. The United States must continue to be the global leader in developing and producing these transformative technologies, establishing resilient supply chains, and defining the automotive future.

Our member companies are fully committed to United States national security. To this end, we share the goals of the ANPRM and appreciate the essential role that BIS has in ensuring that the national and economic security of the United States is preserved. We are fully committed to working with BIS to develop a framework for information and communications technology and services (ICTS) systems in connected vehicles that appropriately mitigates the risks associated with ICTS designed, developed, manufactured, maintained, or supplied by foreign countries of concern.

At the same time, modern vehicles are incredibly sophisticated and incorporate increasingly advanced technologies that are constantly improving and evolving. The automotive supply chain that has developed to support these advances is one of the world's largest and most complex. In addition, vehicle ICTS systems, including their hardware and software components, undergo extensive pre-production engineering, testing, and validation processes and, in general, cannot be easily swapped with systems or components from a different supplier. As BIS proceeds with this rulemaking, it will need to carefully consider these realities.

In the attached appendix, we have provided responses to specific questions posed by BIS in the ANPRM. We certainly welcome the opportunity to engage further with you and provide additional industry perspective and expertise on this consequential and precedential rulemaking.

Given the deep complexity of this topic, the broad sweep of the questions posed by this ANPRM, the uncertain scope of any potential rulemaking, and the relatively short timeframe our members and other stakeholders have had to gather data and formulate responses, we welcome the assurances of BIS that it will carefully review all ANPRM submissions and emphasize the need for us and other stakeholders to have meaningful, ongoing opportunities to provide supplemental materials, insights, and briefings to BIS as the rulemaking proceeds.

Sincerely,

Hilary M. Cain
Senior Vice President, Policy

APPENDIX: RESPONSES TO QUESTIONS POSED IN ANPRM

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?***

   In the ANPRM, BIS identifies the risks of Foreign Adversaries (as defined in Executive Order 13873) "exfiltrate[ing], collect[ing], and aggregate[ing] sensitive data on U.S. persons" and embedding backdoors in a connected vehicle's software to "obtain control over various vehicle functions that could include the ability to disable the vehicle completely."

   With respect to data, BIS concludes that connected vehicles "rely on significant data collection not only about the vehicle and its myriad components, but also the driver, the occupants, the vehicle's nearby surroundings, and nearby infrastructure." The ANPRM goes on to conclude that connected vehicles "allow for information to be gathered and shared." It is correct that modern vehicles are increasingly data dependent. Increasingly, safety and other onboard vehicle features require the exchange of data relating to the operation and function of the vehicle, its systems, and – periodically – its driver or passengers. The generation and onboard processing of this data occurs regardless of whether the vehicle is capable of transmitting that data externally. Auto Innovators agrees with BIS that the transmission of vehicle data to a Foreign Adversary may pose a national security risk.

   The existence of onboard networked hardware or automotive software systems is commonplace for modern vehicles. Although Auto Innovators is not aware of any cyberattack in a connected vehicle in the United States that has been attributable to ICTS supplied by an entity under the control of China or another Foreign Adversary, it is possible that a Foreign Adversary could attempt to use a wireless access point or a wired connection to issue control commands to vehicle systems. Auto Innovators agrees with BIS that the ability of a Foreign Adversary to perpetuate an attack on a vehicle through these means creates additional national security risk.

   In the ANPRM, BIS proposes to define "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, or other wireless spectrum connectivity with any other network or device." The focus of the proposed definition on ICTS systems, rather than individual ICTS components or parts, is appropriate and should be preserved as this rulemaking advances. Systems, which are generally understood to be a set of interrelated components that work together to implement a function or functions, are what facilitate the communication of vehicle data with networks or other devices and what enable the receipt of control commands from an external network or device. The specific national security risks that BIS is attempting to address are enabled through these ICTS systems.

We note that the conventional understanding of "connected vehicle" within the auto industry relates to the ability of a vehicle to communicate with networks or devices external to the vehicle. The term has not traditionally been used to describe communication capability onboard the vehicle. To avoid confusion or misunderstanding within the auto industry and among industry stakeholders, BIS may want to consider using the term "networked vehicle" rather than "connected vehicle" in relation to this rulemaking. For automotive industry stakeholders, "networked vehicle" may more clearly capture both the on-vehicle and off-vehicle exchange of data, information, and controls that BIS is seeking to address.

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?***

   The definition above would capture any vehicle, including an autonomous vehicle or an electric vehicle, if the vehicle integrates onboard networked hardware with automotive software systems to communicate with any other network or device. Auto Innovators suspects that autonomous vehicles, electric vehicles, and vehicles with other alternative power sources will almost universally have this capability.

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?***

   Auto Innovators does not have any other specific definitions of connected vehicles that BIS should consider when defining a class of ICTS transactions for purposes of this rulemaking. However, as noted previously, BIS should consider using the term "networked vehicle" rather than "connected vehicle" to avoid confusion or misunderstanding within the auto industry and among industry stakeholders.

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

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

      ICTS systems that are integral to most connected vehicles operating in the United States include software, operating systems, telematics systems, advanced driver assistance systems (ADAS), and satellite or cellular telecommunication systems. In addition, battery management systems (BMS) are integral to electric vehicles and automated driving systems (ADS) are integral to autonomous vehicles.

      Modern vehicle architectures are generally comprised of electronic control units (ECUs) distributed throughout the vehicle to support various vehicle functions. These ECUs -

which include microcontrollers, embedded control software, and memory - control different functions and systems in vehicles. For example, a brake ECU operates the vehicle's braking system, a power steering ECU operates the vehicle's power steering system, and an ADAS ECU operates driver assistance features (e.g., automatic emergency braking, pedestrian detection, front collision warnings, etc.).

ECUs receive various real-time inputs. For example, a door lock ECU receives input when a passenger pushes the door lock button in the vehicle or on a wireless key fob. An airbag ECU receives inputs from crash sensors and from seat sensors. An automatic emergency braking ECU receives inputs from external radar sensors that detect when a vehicle is approaching an object in the roadway.

ECUs then communicate with actuators to perform an action based on the inputs they receive. For example, a brake actuator forces the brake pads against the brake disc surfaces, decelerating or stopping the vehicle, based on inputs to the braking ECU or the automatic emergency braking ECU.

To simplify vehicle architectures in modern vehicles, auto manufacturers are beginning to integrate various ECUs into centralized control modules. These centralized control modules may be domain-based (i.e., combining control of similar functions into one control module, such as a powertrain domain module or an ADAS domain module) or zone-based (i.e., centralizing control of functions by location in the vehicle body).

In either traditional ECU-managed vehicle architecture or in more centralized architectures utilizing domain or zone control modules, a central gateway is generally used to manage communication between and among control units.

A telematics control unit (TCU) is common in vehicles with any of these architectures. In addition to microcontrollers, embedded software, and memory, the TCU also generally consists of a GNSS unit and one or more external interfaces for mobile communication (e.g., Wi-Fi, LTE, 5G, Bluetooth, V2X, etc.) through which communication occurs between a vehicle and an external network or device.

In addition, vehicles are increasingly outfitted with the capability to connect or pair a mobile phone or similar device to the vehicle for a variety of purposes, including making hands-free phone calls or streaming music. This integration of a phone or other mobile device with the vehicle leverages the external connectivity capability embedded in the phone or other device.

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

At this time, Auto Innovators does not have any insight to provide on market leaders for each distinct phase of the supply chain.

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;

Software, hardware, and other ICTS components integral to connected vehicles globally are largely developed in the United States, Europe, and Asia (including, in some cases, China). The extent to which the software, hardware, or other ICTS components integral to connected vehicles from each of these geographic locations is being integrated into connected vehicles for use in the United States is not currently known to Auto Innovators.

d. involvement in any sector or subsector 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

Auto Innovators is unable to provide any specific insight into involvement by persons owned by, controlled by, or subject to the jurisdiction or direction of a Foreign Adversary in any sector or subsector of the U.S. ICTS supply chain for connected vehicles.

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

To the extent that data is transmitted from a vehicle, it is generally transmitted to the auto manufacturer or the auto manufacturer's telematics service provider. The auto manufacturer maintains control of that data and determines who has access to it and whether it is shared with any third parties. In other words, a Foreign Adversary would not typically have access to data transmitted from a vehicle unless the auto manufacturer provides access to the data or shares the data with the Foreign Adversary or with a person owned by, controlled by, or subject to the jurisdiction or direction of a Foreign Adversary.

In addition, auto manufacturers typically encrypt some vehicle data during transmission, which may help prevent unauthorized access to the data even if it is intercepted by a third party, including a Foreign Adversary. Some auto manufacturers may also choose to store transmitted vehicle data in the global region where it was generated, which may further reduce the risk of unauthorized access by actors, including Foreign Adversaries, outside of that region.

Auto Innovators recognizes that, as noted in the ANPRM, a Foreign Adversary may demand access to or the sharing of such data if the auto manufacturer or a key ICTS system supplier is owned by, controlled by, or subject to the jurisdiction of a Foreign Adversary. In addition, Auto Innovators acknowledges that a Foreign Adversary may seek to breach an auto manufacturer's cybersecurity controls to obtain unauthorized access to a vehicle's ICTS systems to access such data. As BIS proceeds with this rulemaking, it will need to carefully consider these national security risks and how such risks can be effectively mitigated.

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?***

While Auto Innovators believes that there are instances in which an ICTS component or part integral to connected vehicles may be supplied only by persons owned by, controlled by, or subject to the jurisdiction of direction of a Foreign Adversary, Auto Innovators is not aware of any ICTS systems integral to connected vehicles for which persons owned by, controlled by, or subject to the jurisdiction or direction of a Foreign Adversary are sole source suppliers. For the reasons discussed elsewhere in these comments, even when an alternative ICTS system supplier exists, an auto manufacturer may be challenged to abruptly switch suppliers.

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?***

Auto Innovators is not aware that any Foreign Adversary maintains an insurmountable technological advantage over the United States and foreign allies with respect to ICTS systems for vehicles. However, China could be said to currently maintain an advantage – albeit not necessarily a technological advantage – over the United States and other foreign counterparts in the areas of raw materials extraction and processing, battery design and production, and thin film transistor screens. There is also a risk that, without additional supportive policies from the federal government, China could solidify its current advantage in these areas or gain a technological advantage in other areas (e.g., connected vehicle or autonomous vehicle technologies). Additionally, China is open about its industrial strategy to subsidize key technologies and promote their export, which could flood foreign markets with lower cost goods and undercut the ability of companies to compete in the U.S. and abroad. As these efforts continue, including in the mature node semiconductor sector, there is a risk that China could solidify its position and create a technological advantage in connected vehicles and related ICTS systems.

Becoming less reliant on Chinese supply chains in these areas is a top priority of the auto industry in the United States. Efforts to reimagine and restructure supply chains are currently underway, but will require further collaboration between industry and government.

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?***

   GNSS services support next-generation safety technologies in a variety of ways. For example, GNSS signals may be used to supplement wheel odometry and inertial measurements to detect and control sideslip and skidding through selective braking. The active safety features on advanced Level 2 and Level 3 automated vehicles may use precise GNSS to identify the lane on the road the vehicle occupies. Level 4 autonomous vehicles may use GNSS signals to supplement perception information from external sensors (including cameras, LIDAR, and radar) to precisely localize the vehicle to a map or use Coordinated Universal Time derived from GNSS for on-board sensor synchronization.

   It is the understanding of Auto Innovators that auto manufacturers currently operating in the U.S. generally rely on the United States-owned Global Positioning System for positioning, navigation, and timing services. Auto manufacturers operating in the U.S. may use foreign satellite navigation systems, such as Europe's Galileo, for supplemental or redundant GNSS sources.

   Auto Innovators is not currently aware of any auto manufacturer integrating GNSS systems that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a Foreign Adversary into vehicles for the United States market. Auto Innovators also understands that manufacturers owned by, controlled by, or subject to the jurisdiction or direction of Foreign Adversaries generally rely on GNSS systems that are also designed, developed, manufactured, or supplied by Foreign Adversaries.

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?***

   Auto Innovators believes that a focus on ICTS systems, rather than individual ICTS components or parts, will minimize any potential disruptions.

   However, it is important to recognize that the existing automotive supply chain, including the supply chain for ICTS systems for vehicles, consists of multiple tiers of suppliers that service automotive manufacturing operations in the United States and other markets around

the world. Efforts to reimagine and restructure supply chains are underway, but cannot happen overnight. Sudden disruptions to established supply chains may have unintended safety, economic, and environmental impacts and risk undercutting the competitiveness of the auto industry in the United States. In addition, such disruption may undermine efforts to position the United States as a leader in areas that create cleaner, safer, and smarter vehicles (i.e., electric, connected, and autonomous vehicles). For this reason, it is important for BIS to work closely with the auto industry to strike the right policy balance on these complex and urgent issues – including prioritization, scope, and timing – while avoiding unintended consequences that may harm the auto industry in the United States or limit availability of advanced automotive technologies.

At the same time, it is important to acknowledge that auto manufacturers currently operating in the United States are engaged in numerous collaborative activities to mitigate risks, including cybersecurity risks, to ICTS systems in vehicles. This includes efforts through the Automotive Information Sharing and Analysis Center (Auto ISAC), International Organization for Standardization (ISO), Society of Automotive Engineers (SAE), United Nations Economic Commission for Europe (UNECE), and others.

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?***

Generally, there are alternative sources of ICTS systems for vehicles that are not from persons owned by, controlled by, or subject to the jurisdiction or direction of a Foreign Adversary.

To the extent that an auto manufacturer is using an ICTS system supplier that poses a national security risk for vehicles in the United States market, BIS should recognize that efforts to reimagine and restructure supply chains are underway but cannot happen overnight. When establishing final rules and timelines, BIS should carefully consider the current availability, viability, and technological capabilities of alternative sources of ICTS systems for vehicles and whether any practices and safeguards implemented by an auto manufacturer are sufficient to effectively mitigate such risks.

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.***

The relationship between a supplier and an auto manufacturer - including with respect to the ability of a supplier to access vehicle data, to have remote access to a vehicle, or to provide firmware or software updates to the supplied component - is generally established through

proprietary contractual terms. These contracts will generally vary relationship to relationship and may be limited by component functionality.

Depending on the component, vehicle data related to the functioning and operation of a component or system, along with technical specifications and other relevant information for purposes of compliance with regulations or industry best practices, may be shared by an auto manufacturer with the supplier of the component or system for testing, validation, or quality control purposes. In most cases, when this occurs, this functional and operational data is transmitted from the vehicle to the auto manufacturer and then from the auto manufacturer to the relevant supplier. In other words, the relevant functional and operational data is not transmitted directly from the vehicle to the component's supplier.

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?***

    Some aftermarket devices can collect, process, and share data. For example, an aftermarket camera installed in or on a vehicle may gather images of the driver, passengers, or other road users. Similarly, an aftermarket tracking device installed on a vehicle can gather information about the location of the vehicle. However, these aftermarket devices typically generate their own data, rather than accessing vehicle-generated data or interacting with ICTS systems within the vehicle. For example, a tracking device installed on or in a vehicle most likely generates location information using its own GNSS capability and is not accessing the location information generated by the GNSS device in the vehicle.
    One possible exception exists for aftermarket devices that plug into the onboard diagnostic (OBD) port. By law, the onboard diagnostic port provides users with the ability to plug in a scan tool or OBD reader to retrieve certain data from the vehicle. There are aftermarket dongles with embedded wireless communication capability available to consumers in the United States today that can be plugged into the OBD port and are able to transmit vehicle data made available thought the OBD port to third parties, including possibly to Foreign Adversaries. The United States government should also be concerned about policy and legislative proposals (such as the REPAIR Act) that may expose onboard diagnostic systems to additional vulnerabilities from bad actors, including Foreign Adversaries.

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?***

    Presidential Policy Directive 21 identifies 16 critical infrastructure sectors whose assets, systems, and networks are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security,

national public health or safety, or any combination thereof. Critical infrastructure sectors include the energy sector and the transportation systems sector.

With respect to the critical energy infrastructure sector, the battery management system on an electric vehicle communicates with charging infrastructure while the vehicle is charging, and that charging infrastructure communicates with the electric utility grid. In some cases, an electric vehicle may have vehicle-to-grid capability through which the vehicle's electric battery feeds electricity back to the grid. In these cases, communication will take place between the vehicle and the grid.

Auto Innovators does not have visibility into the extent to which battery management systems or components of battery management systems are designed, developed, manufactured, or supplied by entities under the control or influence of a Foreign Adversary. However, Auto Innovators anticipates that electric vehicle tax-related provisions in the *Inflation Reduction Act* and subsequent regulatory guidance may also contribute to fewer battery management systems or components of battery management systems being designed, developed, manufactured, or supplied by entities under the control or influence of a Foreign Adversary for electric vehicles in the United States than there might otherwise have been.

In addition, Auto Innovators does not have visibility into the extent to which electronic vehicle charging infrastructure or components of electric vehicle charging infrastructure are designed, developed, manufactured, or supplied by entities under the influence or control of a Foreign Adversary. However, Auto Innovators is not aware that any of the top electric vehicle charging companies in the United States are owned by or under the control of a Foreign Adversary.

It is important to note that there is extensive work underway between the automotive industry and relevant stakeholders to mitigate risks to battery management systems and electronic vehicle charging infrastructure. For example, the Joint Program Office at the Department of Energy and Department of Transportation is developing cybersecurity resources for electronic vehicle charging infrastructure, including Sample Cybersecurity Clauses for EV Charging Infrastructure Procurements, which can be leveraged by industry and other stakeholders.

With respect to the critical transportation systems infrastructure sector, vehicles may also have the ability to send messages to or receive messages from roadside infrastructure (e.g., traffic signals, etc.) owned and maintained by state or local governments. At this time, Auto Innovators does not have visibility into the extent to which vehicle components or infrastructure components facilitating this type of communication are designed, developed, manufactured, or supplied by entities under the control or influence of a Foreign Adversary.

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?***

    Auto Innovators does not have any additional insight into other instances where persons owned by, controlled by, or subject to the jurisdiction or direction of a Foreign Adversary are integrated into the ICTS supply chain for connected vehicles.

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?***

    The scope of data collection capabilities in modern vehicles varies by auto manufacturer and even by vehicle model within an auto manufacturer's product line.

    However, the types of data that a modern vehicle may collect to support a variety of vehicles features and capabilities include: biometric information (to support theft prevention and/or personalization features); driver behavior information (to support improvements in next-generation systems or convenience features); external sensor images or videos (to support crash avoidance and/or automated driving systems); interior camera images or videos (to support a variety of occupant safety features); physiological or biological characteristics (to support driver impairment, medical emergency detection, or distracted driving detection systems); system operations and performance data (to support improvements in next-generation systems or to identify potential warranty or recall issues); vehicle location data (to support automated features and location-based services); vehicle health data (to provide owners with information about when a vehicle needs to be serviced); and voice recordings (when voice-activated features are used or when calls are made from the vehicle to a call center using the vehicle's embedded connectivity).

    In some cases, data that is generated by the vehicle remains on the vehicle and is not transmitted to the auto manufacturer. In addition, there are instances where data is generated but is not maintained or stored on the vehicle to preserve adequate processing capability for critical vehicle safety and operating processes.

    Generally speaking, auto manufacturers maintain control of any vehicle-generated data that is transmitted to them. For the data to be shared with other entities, the auto manufacturer would have to proactively share that data with a third party or authorize access to that data by a third party. Moreover, under the auto industry's existing Privacy Principles, the sharing of sensitive vehicle data (i.e., geolocation, biometric, or driver behavior information) with an unaffiliated third party requires the affirmative consent of the vehicle owner. Vehicle data that is transmitted to the auto manufacturer is typically encrypted to help protect against interception by an unauthorized third party.

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?***

    The ability to remotely access or control a vehicle varies by auto manufacturer. In general, any commands sent to a vehicle by an auto manufacturer occur through a secured authentication mechanism.

    Some auto manufacturers provide stolen vehicle assistance features to their customers that may allow the auto manufacturer to work with law enforcement to stop the vehicle's engine from starting once it has been turned off or safely slow the vehicle down to a stop if the stolen vehicle is being pursued by law enforcement.

    Auto manufacturers are also increasingly making mobile phone apps available to their customers that allow the owner or user of a vehicle to interact with their vehicle remotely. These remote interactions may include, for example, the ability for the owner or user to lock or unlock the doors of the vehicle, check their vehicle's location, start or stop the engine of their vehicle, check the vehicle's current charge or fuel state, or – in some cases – view images captured from the vehicle's external cameras.

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)?***

    Communication between ECUs, ECU inputs, and ECU outputs as well as communication between ECUs via a gateway takes place onboard the vehicle. Auto manufacturers currently operating in the United States have implemented a variety of measures (for instance, UN R155 and R156) to help secure communications within the gateway to reduce the risk of cyberattack. Auto manufacturers may also enhance security through the design of their vehicle's electronic architecture. This may include isolating some functions from each other, such as separating telematics systems from safety critical systems (e.g., braking or steering).

    Although Auto Innovators is not aware of specific instances of this occurring, it is possible for a supplier to embed wireless communications capability into a component separate and apart from the wireless communications capability provided by the auto manufacturer that could receive over-the-air updates to the component directly from the supplier. Generally, this capability would be known and visible to the auto manufacturer.

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?***

Stakeholders are currently leveraging and/or engaging in industry-led standards development efforts to help secure the interconnection between vehicle and charging infrastructure. Examples include ISO/IEC 15118 (specifying the communication between an electric vehicle and electric vehicle supply equipment) and work being conducted through SAE International's Electric Vehicle Public Key Infrastructure Consortium. In addition, the Department of Energy's and Department of Transportation's Joint Program Office is developing cybersecurity resources for charging infrastructure, including Sample Cybersecurity Clauses for EV Charging Infrastructure Procurements, which can be leveraged by companies currently operating in the United States.

In terms of integration into a vehicle's automotive software system, the battery management system is typically incorporated as another ECU on the vehicle which, in some cases, may be integrated within the battery pack itself. As between other ECUs, communication between the battery management system and other ECUs on the vehicle would generally take place via the gateway.

Auto manufacturers currently operating in the United States generally employ various cybersecurity protections for ECUs, including battery management system ECUs. One of the primary industry resources in this area is the *Cybersecurity Best Practices for the Safety of Modern Vehicles* developed by the National Highway Traffic Safety Administration (NHTSA), which identifies a variety of technical vehicle cybersecurity best practices for securing automotive computing systems. Other resources that are widely used in the automotive industry include the automotive cybersecurity standards from SAE. In fact, SAE produces and publishes the standards that NHTSA often refers to or references in its directives.

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), see also Cybersecurity and Infrastructure Security Agency, Autonomous Ground Vehicle Security Guide: Transportation Systems Sector (2021)***

    The auto industry relies on a variety of programs and best practices to supplement NHTSA's *Cybersecurity Best Practices for the Safety of Modern Vehicles*. These include ISO/SAE 21434 (specifying engineering requirements for cybersecurity risk management of electrical and electronic systems in vehicles, including their components and interfaces), UNECE R 155 (cyber security and cyber security management system) and UNECE R 156 (software update and software management system), ISO 26262

(functional safety for vehicles), and best practices developed by the Auto ISAC (including – among others – security development lifecycle and threat detection, monitoring, and analysis). Auto manufacturers currently operating in the United States may also use programs and practices such as cybersecurity validation plans, bug bounty programs, white hat programs, and end-to-end encryption. Finally, these auto manufacturers may require their suppliers, through contracts, to implement and certify compliance with similar programs and processes.

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;

The degree to which software is licensed varies among auto manufacturers currently operating in the United States. Auto manufacturers may sometimes rely on the supplier of an ECU to also supply the software embedded in that ECU.

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

The extent to which software is developed outside of the United States varies among auto manufacturers and suppliers. Suppliers may develop software in the country or region in which they are developing or manufacturing the relevant component or may outsource software development, in whole or in part, to lower tier suppliers in other parts of the world.

It is relevant to note that India is increasingly playing a key role in the development of automotive software for auto manufactures and automotive suppliers throughout the world.

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

The measures taken to ensure software security and integrity during the development cycle vary among automotive manufacturers and suppliers currently operating in the United States. In managing software securing and integrity during the development cycle, these automotive manufacturers and suppliers generally leverage industry standards and best practices. Examples include ISO/SAE 21434 (specifying engineering requirements for cybersecurity risk management of electrical and electronic systems in vehicles, including their components and interfaces), UNECE R 155 (cyber security and cyber security management system) and UNECE R 156 (software update and software update management system), and the security development lifecycle standard (ASPICE) developed by ISO and IEC.

Additional examples of practices that auto manufacturers currently operating in the United States may incorporate into the software development cycle to enhance the security and integrity of software applications include:

- Threat modeling to identify potential security threats and vulnerabilities early in the development process allows developers to design appropriate security tools;
- Regular code reviews by peers or through automated tools to help catch security issues early in the development process;
- Static code analysis to identify security vulnerabilities, coding errors, and adherence to coding standards;
- Dynamic Application Security Testing (DAST) to assess the security of running applications by simulating attacks and analyzing responses for vulnerabilities;
- Comprehensive security testing, including penetration testing, fuzz testing, and vulnerability scanning, to help identify and remediate security weaknesses;
- Secure software configuration management to help ensure that software and infrastructure configurations adhere to security best practices to prevent misconfigurations that can lead to vulnerabilities;
- Secure storage for any personally identifiable information stored within the head unit;
- Secure Development Lifecycle (SDL) frameworks to integrate security practices into every phase of the software development process;
- Dedicated internal security expert teams to evaluate trends and create policies and frameworks for auto manufacturers and suppliers to follow; and
- Product cybersecurity incident response plans to help ensure a thorough and appropriate response to incidents.

Further, auto manufacturers currently operating in the United States are engaged in numerous activities to collaboratively mitigate risks to ICTS systems in vehicles. These include collaborative efforts through the Auto ISAC, ISO, the Society of Automotive Engineers (SAE), and UNECE.

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

It is Auto Innovators' understanding that auto manufacturers currently operating in the United States do not typically partner or co-develop automotive software with persons owned by Foreign Adversaries for use in the United States.

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

In general, software embedded in hardware will follow the same development cycle as described in c. 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?***

Vehicle data transmitted from a vehicle to an auto manufacturer through wireless connectivity capability is generally stored and processed in a cloud service platform managed by the auto manufacturer. Auto manufacturers generally rely on cloud service platforms provided by third-party cloud service providers.

The access privileges, controls, and remote capabilities afforded to cloud service providers vary among auto manufacturers and are generally established through proprietary contractual terms between an auto manufacturer and its cloud service provider.

End-to-end communication between an auto manufacturer and its service providers may be protected through measures including encryption, provisioning, multi-factor authentication, patch management of system software, vulnerability management of the application software, 24-hour monitoring by security operations, key management by hardware security modules, threat modeling, and risk assessments.

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?***

The specific practices for verifying bill of materials and Software Bill of Materials (SBOM) varies among auto manufacturers currently operating in the United States. This may include using software configuration management systems with specified access controls for traceability, security, and quality assurance. Auto manufacturers currently operating in the United States may also employ penetration testing and fuzz testing to assess vulnerabilities and probe unknown issues. The industry is currently engaged in collaborative work through

the Auto ISAC to develop informational references for auto manufacturers on SBOM.

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

    The extent to which software from vendors and suppliers is tested and verified to comply with requirements varies among auto manufacturers currently operating in the United States. These auto manufacturers generally conduct exhaustive testing for software at the component level (i.e., the ECU), system level (i.e., with dependent ECUs connected), and vehicle level (i.e., in a test vehicle). Auto manufacturers currently operating in the United States also frequently develop gating criteria to evaluate software during testing and maintain processes to log issues and track them to resolution. For these manufacturers, tests are generally performed under different driving scenarios before products are launched in the United States market.

    The auto industry is currently working to develop resources that auto manufacturers can leverage to test and verify vendor and supplier compliance with requirements. These include SAE J3322 (Cybersecurity Testing, Verification, and Validation Methods) and ISO/SAE AWI TR 8477 (Cybersecurity Verification and Validation).

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

    The vendor-vetting and supply chain security practices employed when procuring ICTS systems for vehicles vary among auto manufacturers currently operating in the United States. These practices may include requiring suppliers to deliver a scan of vulnerabilities and measures of risk and using qualitative methodology (i.e., Common Vulnerability Scoring System). Related ICTS system hardware may be subjected to additional controls and technical specifications to help ensure that relevant suppliers conform to the auto manufacturer's requirements for cybersecurity assurance, firmware authentication, component hardening, cryptography, and vulnerability management.

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?***

    Auto Innovators does not have additional insight into other ICTS integral to connected vehicles 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 Foreign Adversary.

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?

The ICTS systems identified by BIS in the ANPRM have the potential to present national security risks if they are designed, developed, manufactured, or supplied by a person under the control or influence of a Foreign Adversary. The risks may be greater if these ICTS systems are integrated into vehicles that are also designed, developed, manufactured, or supplied by an auto manufacturer under the control or influence of a Foreign Adversary. In addition, ICTS systems that enable the communication of vehicle data with external networks or devices or that are capable of receiving control commands from an external network or device likely present a greater risk if those systems are designed, developed, manufactured, or supplied by a supplier under the control or influence of a Foreign Adversary.

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?***

    The United States government should consider the security of the infrastructure, including cellular systems, on which ADS systems may rely or with ADS systems may communicate. This includes the development of secure applications at the infrastructure level, the harmonization of secure protocols for exchanging vehicle data with infrastructure, and ability to trust services dispatched by the infrastructure. The government should also be concerned with policy proposals that would open access to such systems.

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?***

    If the rule appropriately focuses on ICTS systems, rather than individual ICTS components or parts, there should be minimal supply chain disruptions.

    However, in the instance that there are major, sustained, and unanticipated supply chain disruptions, BIS should consider creating a process or mechanism that could be used to grant temporary authorization to engage in an otherwise prohibited transaction. These temporary authorizations should be considered in cases where prohibiting the transaction is likely to harm the competitiveness of the auto industry in the United States or impede the availability of advanced safety or environmental technologies for consumers in the United States, but only if the risks to national security have been sufficiently mitigated.

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

If the government creates a temporary authorization program to allow transactions that would otherwise be prohibited for national security reasons, the threshold for allowing a temporary authorization should be high. To that end, when considering an application for a temporary authorization, BIS should review whether the auto manufacturer has demonstrated commitment to and compliance with specified privacy and security best practices to effectively mitigate risk and the degree to which the auto manufacturer and/or the ICTS system supplier is under the control or influence of a Foreign Adversary. To facilitate this, BIS may want to consider developing a trusted partner program through which an auto manufacturer could demonstrate such commitment and compliance. Once an auto manufacturer and supplier have been admitted into the trusted partner program, the auto manufacturer can self-certify continued compliance for temporary authorization of otherwise prohibited transactions related to ICTS systems.

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

When evaluating the appropriateness of a requested authorization, BIS should consider – among other things – whether the auto manufacturer has identified a responsible security officer to serve as a point of contact, meets minimum foundational and operational security standards, and maintains a supply chain cybersecurity profile that details how the company meets and maintains minimum security standards and guidance. This could include, for example, the standards and guidance documents referenced earlier, as well as SAE J3101 (Hardware Protected Security for Ground Vehicles). In addition, BIS should consider requiring any auto manufacturer that requests such authorization to ensure that the supplier of a relevant ICTS system does not have access to vehicle data (other than perhaps non-identifiable data relating to the operation, function, or performance of that specific ICTS system) and is not able to remotely access the vehicle or the vehicle's systems. Finally, BIS should consider requiring the auto manufacturer to demonstrate acceptable results of penetration testing or other objective means of analyzing risk.

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

BIS should review and consider the Customs Trade Partnership Against Terrorism (CTPAT) program at the U.S. Customs and Border Protection as a potential model for a trusted partner program.

In addition, BIS should review and consider the Office of Foreign Assets Control and BIS licensing processes, as well as the Committee on Foreign Investment in the United States investigation process, as a potential model. These programs involve: collaborative threat assessments by the Intelligence Community and the Department of Defense; meaningful interagency consultation and consensus; narrowly tailored, case-specific authorizations; appropriate conditions and/or mitigation measures; and post-authorization or post-clearance

monitoring.

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?***

    Any potential economic impacts depend on the final scope of the regulations. Focusing on ICTS systems, rather than individual ICTS components or parts, should limit adverse impact on U.S. businesses or the public.

    However, there is the potential for economic impacts associated with the regulation of ICTS systems in vehicles. This includes potential costs to affected manufacturers associated with: (a) vetting and contracting with new suppliers; (b) purchasing higher-cost ICTS systems from alternative suppliers; and (c) developing ICTS systems that are functionally-equivalent to the ones on which the auto manufacturer currently relies.

    There may also be costs to affected auto manufacturers associated with potential delays in producing vehicles for the United States market or in deploying some advanced vehicle technologies in the United States as they restructure supply chains in response to regulation of ICTS systems. For most auto manufacturers, the vehicle development cycle is considerably longer than other consumer products. In general, auto manufacturers are finalizing vehicle architectures and selecting suppliers for the components and systems comprising that architecture years before a vehicle is manufactured. Any changes to vehicle architecture or to suppliers within a few years of vehicle production has the potential to create significant challenges to the auto manufacturer in the form of production delays.

    In the cases where an auto manufacturer's preferred supplier of a particular ICTS system is under the control of China or another Foreign Adversary, there is a possibility that alternative suppliers currently available to that auto manufacturer may not make systems of the same quality or performance available to the manufacturer. In these cases, there is the potential that the affected manufacturer may need to – at least in the interim – settle for a lower quality or lower performing ICTS system from an alternative supplier. This could impact overall customer satisfaction, vehicle sales, and the functioning or performance of safety or environmental systems for the affected manufacturer.

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?***

    Auto Innovators does not expect significant anticompetitive effects if BIS focuses on ICTS systems, rather than individual ICTS components or parts.

However, as noted above, there is a possibility that an affected auto manufacturer may have to use a lower quality or lower performing ICTS system from an alternative supplier. In these cases, the competitive positioning of the manufacturer vis-à-vis other auto manufacturers around the world – particularly those that maintain or have secured access to a higher quality or better performing system – may be impacted. There is also the possibility that an affected auto manufacturer may experience delays in producing vehicles for the United States market or deploying some advanced vehicle technologies in the United States as it restructures its ICTS system supply chains or if supply chain disruptions create a bottleneck for such systems.

33. ***What types of U.S. businesses or firms (e.g., small businesses) would likely be most impacted by the program contemplated by 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 ANRPM?***

The greatest impact from the program contemplated by this ANPRM will likely be felt by automotive manufacturers and automotive suppliers, although the impact can be minimized if the rule appropriately focuses on ICTS systems, rather than individual ICTS components or parts. There is also a chance that consumers will be impacted if an affected auto manufacturer is forced to raise the prices of its vehicles to offset a higher cost ICTS system from alternative supplier.

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?***

A focus by BIS on ICTS systems, rather than individual ICTS components, should minimize potential costs borne by United States businesses or the public.

However, to further minimize potential costs, BIS should consider the following actions:

- Focus on transactions that pose the highest risk to United States national security.
- Provide sufficient lead time to auto manufacturers that may need to restructure supply chains. In addition to identifying and securing new suppliers, an impacted auto manufacturer would need to complete engineering, validation, and safety studies and tests with respect to any new ICTS system integrated into its vehicles.
- Establish a transparent and predictable process or mechanism under which BIS can grant temporary authorizations to engage in otherwise prohibited transactions.

- Work with allies around world to establish and implement cybersecurity and privacy best practices to mitigate risks to ICTS systems in vehicles from entities under the control or influence of a Foreign Adversary.

- Provide detailed guidance on best practices or standards to mitigate risk to ICTS systems in vehicles under the control or influence of a Foreign Adversary.

- Work within the Department of Commerce and other federal agencies, including the Department of Energy and the Department of Transportation, to leverage federal funds and federal regulations to foster and accelerate the development of competitive domestic ICTS systems supply chains and markets for vehicles.

- Provide clear guidance that leverages existing guidance and past practices (e.g., CHIPS and Science Act guidance) on the applicability of any new restrictions on employees of auto manufacturers, suppliers, and contractors who access, or have access to, vehicle data, software, or other ICTS systems-related items subject to the regulation in the normal course of their work.

- Foster flexibility, adaptability, and resiliency throughout the ICTS supply chain.

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?

There will almost certainly be compliance costs and burdens to automotive manufacturers and automotive suppliers for instituting due diligence, compliance and recordkeeping associated with any new supply chain requirements for ICTS systems in vehicles. However, auto manufacturers have already instituted significant supply chain compliance programs for a variety of business, due diligence, recordkeeping, and other compliance reasons that Auto Innovators suspect will be leveraged for these new requirements.