Consumer Technology Association™

1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

April 30, 2024

BY ELECTRONIC SUBMISSION

Elizabeth L.D. Cannon
Executive Director
Office of Information and Communications Technology and Services
1401 Constitution Ave. NW
Washington, DC 20230

Re: Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles
Docket No. 240227-0060

Dear Executive Director Cannon:

The Consumer Technology Association ("CTA") appreciates the opportunity to submit the following comments in response to the Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles advance notice of proposed rulemaking (ANPRM) issued by the U.S. Department of Commerce ("Department") Bureau of Industry and Security ("BIS" or "Agency"). BIS is soliciting 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").[1]

As North America's largest technology trade association, CTA represents the $505 billion U.S. consumer technology industry, which supports more than 18 million U.S. jobs. Members of CTA are diverse and include companies at the forefront of vehicle technology, including vehicle and component manufacturers, software developers, transportation platforms, and companies engaged in a multidisciplinary approach to this evolving industry.

CTA appreciates the importance of this rulemaking, to narrowly address the involvement of persons which are owned by, controlled by, or under the jurisdiction of 15 CFR 7.4 entities—namely (1) The People's Republic of China, including the Hong Kong Special Administrative Region (China); (2) Republic of Cuba (Cuba); (3) Islamic Republic of Iran (Iran); (4) Democratic People's Republic of Korea (North Korea); (5) Russian Federation (Russia); and (6) Venezuelan

[1] Department of Commerce, 89 FR 15066 (March 1, 2024) [hereinafter *ANPRM*) at 15067].

politician Nicolás Maduro (Maduro Regime). CTA acknowledges there is a legitimate potential national security risk that is appropriate for the Department and BIS to examine. Concurrently, CTA emphasizes the importance of a narrowly tailored approach to address this potential risk while also minimizing collateral impacts to American leadership in the CV industry. CTA welcomes further collaboration between the Agency and industry participants on this matter.

It is important that any final rule addresses a clearly defined U.S. national security risk. The final rule should integrate existing standards and best practices to capitalize on the efficiency, consensus, and safety protections already in place.

In addition, we appreciate the Agency's clarity regarding the types of threats they seek to better understand. Specifically, the threats can be separated into three categories: (1) the national security risk that a foreign adversary would have access to or control over sensitive and personal data captured by connected vehicles (2) the national security risk of remote manipulation of the vehicle's controls or operating systems by a foreign adversary, or (3) a combination of the two.

With these points in mind, CTA's comments focus on three primary objectives while providing useful information to BIS: (1) addressing potential national security risks related to specific aspects of vehicle communication technologies with solutions that limit unintended consequences (2) promoting development and use of automated driver-assistance systems (ADAS), automated driving systems (ADS or AV) and Vehicle-to-Everything (V2X) technologies in the U.S., and (3) ensuring the U.S. can compete at parity with the global market for CVs while keeping trade barriers to a minimum and staying committed to working with our allies.

CTA is pleased to submit the following comments in response to specific Agency questions and topic areas in the 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?

The ANPRM proposes defining 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.

The proposed 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.[2] Many of these CVs have integrated key technologies like automated driving systems (ADS), advanced driver assisted systems (ADAS), cellular connectivity, and Bluetooth connectivity; further defining these technologies in a final rule requires precision. Accordingly, CTA recommends that the Department consider preexisting definitions and alternate terminology in use by, for example, the Department of Transportation (DOT) to ensure consistency.

[2] ANPRM at 6.

For example, the Department of Transportation defines CV technologies specifically as equipment, applications, or systems that use V2X communications to address safety, system efficiency, or mobility on our roadways. DOT focuses on CVs' ability to use data from short-range communication broadcasts and peer-to-peer exchanges to understand what hazards (vehicles, bicyclists, pedestrians, wheelchairs, motorcycles, buses, trucks, and others) exist nearby. This understanding of CVs and their function comes in part from the Society of Automotive Engineers (SAE) J2945 standard, which is an industry-developed definition that USDOT has cited in previous rulemakings.

Relating to automated/autonomous vehicles (AVs) specifically, the SAE J3016 classification system for automated vehicles serves as an important, industry-accepted reference regarding AV capabilities.[3] This document is useful for its taxonomy of automation and descriptions of the range of automation features used in AVs. The Department of Energy has already begun incorporating this terminology when discussing the impacts to energy efficiency.[4]

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?

Yes, this term would likely include the types of vehicles and equipment listed above. The notice indicates that Commerce is considering identifying the following technologies as integral to connected vehicles: vehicle operating systems, telematic systems, ADAS, ADS, satellite or cellular telecommunication systems and battery management systems. BIS should focus next steps on defining and scoping these and any other relevant connected vehicle ICTS systems.

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?

BIS should consider existing definitions and terminology already in use when defining a class of ICTS transactions. This will ensure consistency across government agencies and offer certainty to the regulated community. CTA also encourages the use of precise terms of art when possible, such as V2X, ADAS, or ADS technologies, to prevent any confusion.

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

1. **Categories of ICTS, such as software or hardware, that are integral to CVs operating in the United States;**
2. **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;**

[3] SAE INT'L, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, (2021) https://www.sae.org/standards/content/j3016_202104/.
[4] U.S. DEPT. OF ENERGY, OFFICE OF ENERGY EFFICIENCY & RENEWABLE ENERGY, INTELLIGENT TRANSPORTATION SYSTEMS, (April 8, 2024), https://www.its.dot.gov/cv_basics/cv_basics_federal.htm.

3. **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;**
4. **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**
5. **Geographic locations where data from CVs in use in the United States is transmitted, stored, or analyzed.**

#2, #4:

The United States has one of the largest automotive markets worldwide, with approximately 14.5 million lightweight vehicle sales in 2020 alone.[5] Consequently, the ICTS supply chain is both large and complex.

CTA highlights that many automotive components associated with ADAS or ADS systems, such as cameras, Light Detection and Ranging (LiDAR), and radar sensors, do not have connectivity capabilities (e.g. Bluetooth or WiFi) and therefore should not be included in the scope of the final rule. However, it should be understood that these components may be connected to other modules such as ADAS microcontrollers (MCU) where there is a direct connection to networks outside of the vehicle.

Because BIS is primarily focused on national security concerns around vehicle safety and vehicle data privacy protections, BIS should focus any potential rulemaking on key CV ICTS systems, rather than low- or non-connected hardware components, and on gathering information about the processes industry is using to protect vehicles' embedded operating system from foreign adversaries to determine if there are gaps, as well as the best practices around control and access to data generated in vehicle operations.

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?

Individual component parts alone pose a low cybersecurity risk and are widely available from a variety of sources, including sources outside foreign adversary countries. Although integrated components alone pose limited risk, such risk may be elevated depending on how they are integrated and operated within systems on the connected vehicle, which tend to be developed by and proprietary to, the OEM or Tier-1 system supplier.

CTA emphasizes that unnecessary trade barriers should not be placed on the free market as national security and cybersecurity protections are considered.

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?

[5] INTERNATIONAL TRADE ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE, AUTOMOTIVE INDUSTRY OVERVIEW, https://www.trade.gov/selectusa-automotive-industry.

CTA is not aware of any key connected vehicle ICTS system in which such persons maintain an insurmountable technological advantage over the U.S. and other foreign counterparts.

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.

Each OEM has a proprietary vehicle platform that requires different implementations. In general, OEMs are undergoing a transition in how they manage their relationships with component suppliers.[6] No singular approach to acquiring ICTS components has yet prevailed; instead, a myriad of approaches—from the development of in-house capabilities to the creation of intricate partnership ecosystems—are used by OEMs.[7] However, many, if not most, OEMs and Tier 1s have developed or are developing their own proprietary ICTS systems for integrating and operating such components.

Because ICTS acquisition practices vary, CTA focuses on the applicable best practices in existence that apply across the board and set guidance related to information sharing, administrative access, and remote privileges. First, CTA supports NHTSA's best practice stating that manufacturers should document any actions, design choices, or analyses related to vehicle cybersecurity.[8] By doing so, manufacturers will have an accurate and immediate understanding of vehicle capabilities that can be remotely accessed in the event that remote malfeasance by an unauthorized entity occurs. Second, to limit remote access, CTA refers to two key recommendations in NHTSA's best practices for cybersecurity: (1) limiting access to vehicle computing platforms via use of cryptographic credentials, and (2) limiting vehicle diagnostic procedures to specific modes of operation. Cryptographic credentials can help mediate access to vehicle computing resources via use of passwords, public key infrastructure (PKI) certificates, and encryption keys. The International Telecommunication Standardization Sector (ITU-T) Recommendation for Secure Software Update Capability for Intelligent Transportation System Communication Devices,[9] which is specifically recommended as a standardization reference by the DOT in relevant automated vehicle guidance,[10] makes practical recommendations for car manufacturers with varying security capabilities to reduce cybersecurity risks for secure software updates.

---

[6] Relationship of OEMs and Component Suppliers in Auto Ecosystem, DELOITTE, https://www2.deloitte.com/cn/en/pages/risk/articles/relationship-of-oems-and-components-suppliers-in-auto-ecosystem.html

[7] Weseem Haider, *Connected Cars: OEM Car Maker Strategies–Where Does the Network Operator Fit In?*, MTN CONSULTING (2021), https://www.mtn-c.com/connected-cars-oem-car-maker-strategies-where-does-the-network-operator-fit-in/.

[8] NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION, DEPARTMENT OF TRANSPORTATION, CYBERSECURITY BEST PRACTICES FOR THE SAFETY OF MODERN VEHICLES 13 (2022) [hereinafter *NHTSA Best Practices*].

[9] International Telecommunication Standardization Sector (ITU-T), Recommendation Secure Software Update Capability for Intelligent Transportation System Communication Devices, INTERNATIONAL TELECOMMUNICATIONS UNION (2017), file:///C:/Users/goffck/Downloads/T-REC-X.1373-201703-I!!PDF-E%20(2).pdf.

[10] U.S. DEPT. OF TRANSPORTATION, AUTOMATED VEHICLES 3.0: PREPARING FOR THE FUTURE OF TRANSPORTATION, (2024), https://www.transportation.gov/av/3.

Second, limiting diagnostic features to a specific mode of operation can prevent dangerous unintended consequences from cybersecurity threats. For example, limiting diagnostic features that impact vehicle brakes to low speeds, and prohibiting all brakes from being impacted at once, can prevent cyber threats that could alter brakes and threaten safety.

While it is possible entities owned by, controlled by, or subject to the jurisdiction of a foreign adversary may not (or may not be permitted) to fully adhere to these best practices, these best practices exist currently and are widely used by the industry.

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?

CVs can collect data from the environment around them to inform the vehicle's safety operation, provide those using the vehicle with necessary information, and enhance the vehicle's performance. AVs, in particular, must accurately and reliably perceive objects and vehicles to safely travel on public roads. Accordingly, AV developers equip their vehicles with a combination of ultra-high-definition cameras, radars, and LiDARs. These sensors collect data that is stored locally in log files that is often manually offloaded by a developer and uploaded to a secure cloud service to facilitate the development process. These systems are able to discard unneeded information to allow the CV to keep only the data that is most useful—including data legally required to be maintained in the case of a crash—thereby potentially limiting the amount of data that is vulnerable to malfeasance, assuming that the CV ICTS system is used as intended and that the operator of the CV chooses the system in this way.

CTA acknowledges the significant responsibility associated with data collection and emphasizes that—while CV data collection capabilities may be misused by entities owned by, controlled by, or subject to the jurisdiction of a foreign adversary—many industry stakeholders already adhere to best practices to prevent unauthorized access to, or control of, data collected by CVs. For example, as outlined in CTA's response to BIS's question 10, best practices outlined by NHTSA recommend limiting access to computing platforms with the use of cryptographic credentials and limiting vehicle diagnostic procedures to specific modes.[11] These measures limit the scope of persons with access to data collected and restrict the scope of possible negative consequences should malfeasance occur.

[11] NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION, DEPARTMENT OF TRANSPORTATION, CYBERSECURITY BEST PRACTICES FOR THE SAFETY OF MODERN VEHICLES 13 (2022).

To ensure the advantages of connectivity can be capitalized on, safety-focused coalitions like the Automated Vehicle Safety Consortium (AVSC) have also developed best practices to standardize data collection and maximize safety, especially as related to crash prevention. To address cybersecurity concerns, AVSC's best practices recommend that only an authorized user who has "received authorization from the ADS supplier or manufacturer" be able to access data from the event. AVSC also cautions that the recording system should be "tamper resistant" in compliance with ISO/SAE 21434 and SAE J3061, as well as other industry wide standards. ISO/IEC 27001 sets requirements related to protecting sensitive data residing in "backend systems' such as those found on cloud networks. The standard also provides a framework "for managing information security risks that could impact the security and safety of vehicles and Cloud Battery Management Systems (CBMS)." CTA acknowledges that voluntary, non-enforceable best practices like these do not abate the national security risk from foreign adversary control.

The industry is motivated to continue implementing these best practices related to data collection for intellectual property and cybersecurity reasons.

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)?

Many of the individual sensors associated with ADAS or ADS systems, like camera, LiDARs, and radar sensors, do not have the same connectivity capabilities as CV ICTS systems.

AV developers do not consider their sensors to be connected devices, since they are housed in internal networks that are separate from the internet and communicate to the AV computer through secure gateways using ethernet.

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?

Battery management systems (BMS) support safe and efficient high-power battery energy storage systems ("BESSs") in both vehicular and stationary settings.[12] Cloud BMS ("CBMS") can process big data with the use of cloud computing advancements. CTA recognizes that, along with enhanced safety and efficiency, these technologies can also present vulnerabilities that need to be accounted for. In response, U.S. and allied industry has already begun implementing best practices to prevent malware from disrupting the proper function of BMS.

[12] *See* Farshid Naseri et al., *Cyber-Physical Cloud Battery Management Systems: Review of Security Aspects*, BATTERIES, July 2023 at 8.

In general, it is in the interest of U.S. and allied industry participants to treat the connectivity and operating system aspects of CVs with extreme care. Doing so ensures the protection of proprietary data that these companies have invested in significantly. Many companies in this industry have dedicated teams of cybersecurity specialists to preventing malfeasance. Further, many of our members are actively involved in industry collaborations around this issue and have helped to develop best practices put forth by organizations such as SAE and NHTSA. Further, industry has already developed various methods to enhance the cybersecurity of BMS related to hardware security, software security, penetration tests, and code reviews.[13]

One way industry participants ward against malware is by using resilient software and operating system design to ensure that software is robust against cyberthreats. Further, encryption—the process of encoding BMS data information to prevent unauthorized access—can help ensure that battery information remains confidential, so that only authorized individuals and entities can access the data.[14] Similarly, user authentication can provide an additional layer of protection to ward off unauthorized access to battery-related data.[15]

Regarding specific best practices, ISO/IEC 27001 sets requirements related to protecting sensitive data on cloud networks and provides a framework "for managing information security risks that could impact the security and safety of vehicles and CBMS."

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?

In order to ensure that CVs driving on American roads are using the most up-to-date safety features, software updates may need to be performed. In some instances, this involves offering limited access privileges or remote capabilities with respect to CV OEM systems and cloud service providers. Preventing improper remote access to data during this process is in the best interests of regulators and stakeholders alike, and CTA seeks to highlight the existing best practices on this issue, such as SAE 24089, the AVSC Best Practices and NHTSA's Cybersecurity Best Practices, which are widely accepted in the industry.

[13] *See id.* at 18.
[14] *See id.* at 21-22.
[15] *Id.* at 24.

CTA recommends the Department consider existing best practices and standards while assessing whether additional related regulations are necessary, and if so, in developing any such regulations that are in alignment with the OEMs and suppliers. The AVSC Best Practice considers cloud storage an acceptable storage location for event-recorded data. Regarding manufacturers' access to this data, there are several mechanisms already embraced by best practices to limit remote access. In our answer to question 10, we mentioned several of these safeguards. We reiterate the importance of incorporating SAE's and NHTSA's existing best practices regarding remote access, including limiting access to vehicle computing resources using cryptography methods, and limiting the ability to remotely diagnose or alter vehicles' features in modes where doing so would be unsafe.[16] These existing measures decrease the risk of malfeasance related to remote access. Accordingly, co-opting existing procedures intended to limit harm caused by remote access will both protect drivers and limit disruption to the highly competitive CV market.

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

Because CV and ICTS technology is often proprietary and requires significant investment, U.S. and allied industry participants take significant care to vet the partners they work with. Guidance from national security agencies on vetting suppliers and securing supply chain are crucial. CTA also supports NHTSA's existing best practices, which incorporate standard ISO/SAE 21434 on the topic of vetting. NHTSA specifically recommends that manufacturers "evaluate all commercial off-the-shelf and open-source software components" against unknown vulnerabilities.[17] NHTSA also recommends that manufacturers employ testing for cybersecurity vulnerabilities, specifically by incorporating penetrating tests and test stages that require independent, qualified testers to identify remaining vulnerabilities.[18] For each identified vulnerability that is assessed, or new vulnerability identified through this process, NHTSA's best practices also recommend that manufacturers generate a "vulnerability analysis."[19] Lastly, as outlined in our answer to the Department's question ten, many companies already implement existing best practices and standards to limit authorized remote access by third-parties to vehicle software.

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?

[16] NHTSA Best Practices.
[17] *See id.* 6.
[18] *See id.*
[19] *See id.* at 7.

The National Telecommunications and Information Administration (NTIA) issued a Notice requesting public comment on key issues impacting technology deployment in the United States in 2016.[20] In 2017, after responses from numerous stakeholders including automotive manufacturers, NTIA issued its findings in a Greenpaper that addresses cybersecurity, privacy, intellectual property, and data collection in the United States.[21] The agency notes the importance of promoting technology-neutral standards and consensus multistakeholder approaches on issues such as U.S. security.

Federal Communications Commission Chairwoman Rosenworcel released a Further Notice of Proposed Rulemaking (FNPRM) announcing the FCC's plans to make a rulemaking regarding domestic abuse and connected cars.[22] Although the FNPRM is not yet public, CTA recommends BIS reference the materials in this proceeding when they are released.

Notably, the existing best practices regarding vetting, remote access related to software updates, and component part connectivity (as addressed under questions 10, 16, and 17), should also be considered as the standard for any rulemakings developed on these issues.

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?

Certain U.S-origin connected vehicles would be within scope of an ICTS order that restricts transactions at the component level. As outlined in our above responses, many components do not have connectivity abilities, thus limiting cybersecurity and national security concerns. To compete while addressing the national security risk, BIS should restrict or prohibit transactions focused on connected systems, not low-tech components.

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?

By narrowly tailoring the scope of the rule and Orders and building on industry efforts to address these real concerns, the Department can most efficiently work towards the desired policy outcomes while mitigating unintended consequences. CTA urges the Department to refrain from any overly broad actions that could disrupt the supply chain and negatively affect overall American technological competitiveness and leadership.

[20] Inquiry into the Internet of Things (IoT), 81 Fed. Reg. 19956.
[21] U.S. DEP'T. OF COMMERCE, FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS, 24, 30, 33, 39 (2017).
[22] Supporting Survivors of Domestic and Sexual Violence, Further Notice of Proposed Rulemaking, WC Docket No. 22-238, (April 8, 2024).

Thank you for the opportunity to provide these comments. CTA looks forward to continued collaboration with the Government on these important issues.

Sincerely,

/s/ Gary Shapiro
Gary Shapiro
President and CEO
Consumer Technology Association
1919 S Eads St.
Arlington, VA 22206

/s/ India Herdman
India Herdman
Senior Manager, Policy Affairs
Consumer Technology Association
1919 S Eads St.
Arlington, VA 22206

/s/ Finch Fulton
Finch Fulton
K&L Gates LLP
1601 K St., NW
Washington, DC 20006