COALITION FOR
Reimagined Mobility
Transportation Policy that Puts People First

SAFE

April 30, 2024

U.S. Department of Commerce
Bureau of Industry and Security
1401 Constitution Ave., NW
Washington, DC 20230

Docket: REG – 240227–0060: *Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles*

To Whom It May Concern:

The Coalition for Reimagined Mobility (ReMo), a global initiative of the organization SAFE, applauds the Department of Commerce (the Department) for its efforts to investigate the risk that information and communications technology and services that are integral to connected vehicles (CVs) may be controlled or exploited by foreign countries or foreign non-government persons.[1]

Advanced vehicle technologies will define the automotive and transportation sectors for the next several decades and the United States must act to maintain, and in some cases reclaim, our position as the global leader in this industry. Earlier this year, ReMo published its flagship report, *Unlocking a 21st Century Mobility System: How to Rethink the Future of Mobility and Restore Leadership in Transportation Innovation*, which highlighted these risks and documented the extent of action required by the U.S. government and industry to remain both globally competitive and secure.

As an organization that brings together private and public sector leaders, ReMo appreciates the Department's investigation and effort to garner information from different stakeholders. As underlined below in our comments, the threats to the connected vehicle industry – and the broader automotive industry – are fundamental and pressing. Foreign adversaries are cornering and leveraging key supply chains to geopolitical and economic ends, creating a risk that they may be able to remotely access and use data for strategic intelligence and opening

[1] Note: ReMo brings together industry CEOs, public sector leaders and practitioners across transportation, technology, and sustainability to advance public policy and real-world solutions to improve the movement of people and goods worldwide. The Coalition is part of SAFE, a bipartisan, nonprofit accelerating the real-world deployment of secure, resilient, and sustainable transportation and energy solutions that enhance the country's economic and energy security. For more information, visit https://reimaginedmobility.org/.

vulnerabilities to cyber-attacks on U.S. soil. The scope, scale, and urgency of this national security risk comes at the same time the automotive industry is experiencing a transformational shift. New technologies are being adopted quickly, which means the complexity of the threat facing the United States will only accelerate over the next several years. We look forward to working with the Department of Commerce and leaders in Congress to address the national security vulnerabilities that may be prevalent throughout the Information and Communications Technology and Services (ICTS) supply chain.

Our primary goal in submitting these comments is to assist the Department in considering how it can provide support to consumers and industry while developing secure supply chains for this critical sector of the economy to continue its contribution to our nation's economic growth, industrial base, and security. We hope that our comments inform the Department's thinking. If you have any questions or wish to discuss further, please contact Avery Ash at aash@secureenergy.org.

Summary

The transportation sector is experiencing a transformation driven by several concurrent trends, including connectivity, automation, electrification, and technologies like AI, robotics, and data analytics. Software-defined vehicles are growing in prominence, supported by enhanced communications infrastructure. This evolution allows vehicles to connect more seamlessly with external systems through telematics and cellular vehicle-to-everything (C-V2X) communications, improving consumer experiences, safety, and generating value for OEMs and other stakeholders in the automotive industry.[2] It is crucial to highlight the positive benefits of CVs to people and the planet and it is important to note that ReMo and SAFE fully support the technology's potential. The focus should be on expediting the integration of technologies that underlie CVs and safeguarding them from vulnerabilities and disruptions from foreign adversaries to ensure their functionality.

The United States led the world in production of CVs for much of the past two decades, and sold nearly 16 million vehicles in 2023, most of which were connected vehicles as defined by the Department.[3] However, China is now the clear global leader with the single largest car market, setting a record by selling more than 30 million vehicles in 2023.[4] The growth of China's auto manufacturing sector and its market for new vehicles are outpacing the production of CVs in the rest of the world.

CVs offer significant benefits to both consumers and the industry, including enhanced safety, reduced traffic congestion, and improved fuel efficiency. These benefits could potentially prevent more than 500,000 crashes annually, resulting in 1,000 fewer fatalities, reduce fuel

[2] Coalition for Reimagined Mobility, *Unlocking a 21st Century Mobility System: How to Rethink the Future of Mobility and Restore Leadership in Transportation Innovation*, January 8, 2024, at Pg. 11.
[3] Cox Automotive Inc., "Harness the power of connected data for game-changing results," April 16, 2024.
[4] CK Tan, "China's 2023 auto sales grow 12% on overseas demand for EVs," Nikkei Asia, January 11, 2024.

consumption by 10 percent, and cut congestion-related delays on highways by 60 percent.[5] Low-income and minority communities stand to benefit from these innovations, as a city-specific study shows that even a modest increase in the number of connected and shared vehicles can lead to a 40 percent reduction in fine particulate matter (PM2.5) emissions and a 61 percent decrease in noise from vehicle trips.[6]

While connected vehicle technology, historically known as telematics, developed in the 1980s, it was General Motors' introduction of the OnStar telematics system in 1997 that paved the way for wider adoption.[7] As technology advanced, most personal and commercial vehicles manufactured after 2010 started offering internet connectivity.[8] This broader connectivity enables crucial technologies like GPS tracking, over-the-air updates and emergency SOS notifications, besides daily comforts like remotely unlocking doors or heating seats and remote parking. This vehicular connectivity also comes with significant data generation.

Connected vehicles can generate significant amounts of data, up to 25 gigabytes (GB) per hour from around 200 sensors on the lower end to 19 terabytes (TB) per hour for autonomous CVs.[9] Not all this data leaves a vehicle, but some amount is transmitted through in-vehicle cellular connections and initially stored in data centers or cloud platforms owned by original equipment manufacturers (OEMs).[10] Some data may also be sent directly to Tier-One suppliers or third parties with onboard devices. However, this data is at an individual vehicle level and there are limited consistent formats or data standards across OEMs, so the data requires additional processing to be useful beyond vehicle diagnostics or services. Data aggregators take deidentified data from multiple sources and extract aggregate insights to make it more usable and valuable (e.g. to help a department of transportation manage the road network effectively or understand changes in travel patterns for planning purposes). It is also important to consider that the key features of CVs and a 21st-century transportation system rely on connected infrastructure and cloud-based systems that generate and store similar data. As CVs become more prevalent, the threats of compromising or controlling associated assets, including vehicle

[5] Alliance for Automotive Innovation, "HAVS | Highly Automated Vehicles", 2024 (n.d.), and Jon Peha, "Leading the Way: A National Task Force on Connected Vehicles," Carnegie Mellon University: Traffic21, August 7, 2020.
[6] Coalition for Reimagined Mobility, "Environmental and Equity Implications of Electric, Shared Autonomous Vehicles (SAVs) in Urban Transportation: A Case Study of San Francisco," November 3, 2023, at Pg. 4.
[7] Coalition for Reimagined Mobility, *Unlocking a 21st Century Mobility System: How to Rethink the Future of Mobility and Restore Leadership in Transportation Innovation*, January 8, 2024, at Pg. 31.
[8] Michael Hill, "Connected Vehicles: The Next Big Security Challenge?," Infosecurity Magazine, September 15, 2016.
[9] John Verdi, "A Privacy Playbook for Connected Car Data", Future of Privacy Forum. October, 2019; and Coalition for Reimagined Mobility, *Unlocking a 21st Century Mobility System: How to Rethink the Future of Mobility and Restore Leadership in Transportation Innovation*, January 8, 2024, at Pg. 65; and Note: Approximately 90-95% of data generated by sensors is processed internally and in most instances isn't even stored. This data is processed locally with low latency for vehicle operations like collision avoidance, ice detection or blind spot warnings. A small percentage of data is transmitted to the manufacturer for diagnostics or driver assistance services. For context, an over-the-air (OTA) vehicle update can range from 300 megabytes to ten gigabytes.
[10] Mario Ortegon-Cabrera, et al. "Automotive Connected Fleets - Azure Architecture Center," Microsoft Learn, May 10, 2023.

physical condition and control; data related to vehicles or occupants; and connected infrastructure, will increase.

These threats raise the specter of harm to not just the individual or a vehicle, but also to critical infrastructure that can affect our national security, as well as offering a strategic benefit to foreign adversaries who might gain access to this data. A summary of some key areas of concern is provided below:

1. **Supply Chain Dependency**: The benefits of CVs have led to their predictable rise and at the same time made it imperative for countries to secure their ICTS supply chain and the integrity of their components. While adversarial foreign entities may not always be the primary innovators in connected vehicle technologies, they do form a very important part of the ICTS supply chain and possess intellectual property (IP) and expertise related to CVs.[11]

   The current automotive supply chain involves multiple tiers of suppliers and integrators, with OEMs and Tier-1 suppliers centralizing component assembly. Chinese firms dominate the production of many essential components for CVs, often entering the American automotive supply chain as sub-component suppliers for parts manufactured in Mexico and Canada. In 2023, Mexico was the largest auto parts supplier to the United States, with China ranking third, but China was also the second-largest auto parts supplier for Mexico.[12]

   The importance of China in the automotive supply chain cannot be understated. The Chinese auto parts industry has seen significant growth, with thirteen Chinese companies making the Automotive News Top 100 Global OEM Parts Suppliers list in 2023, supplying directly to OEMs and often having a U.S.-based subsidiary.[13] For context, in 2007, there were no China-based auto suppliers listed in the Top 100. Despite this growth, most Chinese companies are Tier-2 and Tier-3 suppliers but are steadily expanding their market share as Chinese car exports increase globally and progress towards manufacturing more technologically advanced components.

   However, despite being a significant source of auto parts, China is not a major exporter of assembled vehicles to the United States. This situation highlights the specialized nature of China's export relationship with the U.S. automotive market, focusing on components rather than finished vehicles.[14]

---

[11] Coalition for Reimagined Mobility, *Unlocking a 21st Century Mobility System: How to Rethink the Future of Mobility and Restore Leadership in Transportation Innovation*, January 8, 2024, at Pg. 16.
[12] Óscar Goytia, "Mexico Supplies 42.5% of US Auto Parts Imports," Mexico Business News. April 9, 2024.
[13] Automotive News, "Automotive News Top Suppliers, Ranked by Total OE Automotive Parts Sales," June 25, 2023.
[14] Note: ReMo and SAFE define the U.S. automotive market as one that encompasses the manufacturing, sale, and distribution of automobiles within the United States, including vehicles produced by domestic and allied international OEMs. This market also includes Tier-1/2/3 suppliers manufacturing and assembling vehicles and components within the U.S.

China's role as a major importer of auto parts and its robust network of tier-2 and tier-3 suppliers are critical to the global automotive supply chain, including the U.S. market. This network underpins efficiency and innovation in the automotive sector, allowing U.S. manufacturers to source high-quality components at competitive prices. However, this dependency also exposes U.S. manufacturers to several risks, such as supply chain disruptions from geopolitical tensions, trade policies, and quality control issues that can arise from reliance on foreign suppliers.

2. **Data Privacy and Security**: CVs generate vast amounts of data, including geolocation, driving patterns, and vehicle diagnostics. Current estimates peg the data generated per hour by conventional vehicles at 25GB (equivalent to 125 hours of High-Definition video) to more sophisticated vehicles at 19TB (equivalent to 5,000 hours of HD video).[15] There are concerns that data generated by Chinese-made components or software could be accessed or controlled by the Chinese government, which would raise privacy and security risks for individuals and organizations. A recent executive order to limit the transfer of sensitive personal and geolocation data to foreign entities of concern marks an initial effort to grapple with this complex issue, signaling the start of a broader, more nuanced approach that will be required.[16]

   If a foreign adversary were to gain access to CV data – either coming off of the vehicle directly or stored remotely – they could use it for strategic intelligence. Additionally, access to vehicle data or components could open vulnerabilities to cyber-attacks on U.S. soil. Over the last five years, the number of global cybersecurity attacks on CVs or associated platforms doubled to 295 incidents in 2023 alone.[17] Of these, half were high-impact incidents affecting millions of users, and nearly all were conducted remotely over Bluetooth, Wi-Fi, or 3/4/5G networks.[18] These often come at a high price and a single incident can cost companies $42 million to $50 million USD in remediation, legal settlements, fines, or loss of reputation.[19] Most cyber-attacks were attributed to Advanced Persistent Threats (APTs) or state-sponsored groups that typically carry out prolonged attacks. Notable adversaries highlighted by the Cybersecurity and Infrastructure Security Agency (CISA) include the People's Republic of China (PRC), Russia, and the Democratic People's Republic of Korea (DPRK).[20]

[15] John Verdi, "A Privacy Playbook for Connected Car Data", Future of Privacy Forum, October, 2019; and Coalition for Reimagined Mobility, *Unlocking a 21st Century Mobility System: How to Rethink the Future of Mobility and Restore Leadership in Transportation Innovation*, January 8, 2024, at Pg. 65.
[16] The White House, "Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," February 28, 2024.
[17] Yoav Levy et al., "Upstream's 2024 Global Automotive Cybersecurity report," Upstream Security, February 7, 2024, at Pg. 6.
[18] Ibid.
[19] Id., at Pg. 19.
[20] Cybersecurity and Infrastructure Security Agency (CISA), "Nation-State Cyber Actors," 2024.

In a 2023 incident involving a Chinese component, the UK Prime Minister's official car was monitored using a tracking device embedded in the vehicle to determine meeting locations and infer daily routines or relevant persons met.[21] The SIM card-enabled tracker was found in a sealed part imported from China in a forensic sweep conducted by UK intelligence officials. This kind of embedded risk is exacerbated and challenging to detect if it were a fully assembled vehicle manufactured by a foreign adversary. Since a majority of modern cars sold today are connected vehicles, the risk of compromised systems sold as a whole, particularly by China is immense. China is the world's largest auto exporter having quintupled its exports in the last four years and is rapidly expanding its global presence.[22] Chinese electric vehicle shipments into the European Union surged by 361 percent since 2021, in part due to state-subsidized EV manufacturers deploying a competitive pricing strategy (e.g., EVs are 25 percent lower in cost than competitors), offering advanced technological features like Automated Driving Systems (ADS) and freebies like unlimited charging to attract consumers.[23] There is growing concern that these fully assembled vehicles could potentially be a digital Trojan horse.[24]

In the Internet of Things (IoT), products are equipped with digital capabilities like cellular IoT modules (CIMs), ranging from electric vehicles to smart home devices. These modules generate and share data across networked devices and can receive remote updates and repairs. However, this connectivity poses significant cybersecurity risks, as both cyber attackers and manufacturers could potentially access the system and/or data.[25] A scenario where hackers or a foreign adversary might infiltrate a CV system to track movement at secure installations or remotely collect information about people and other assets is a possibility. Additionally, groups like Volt Typhoon, a state-sponsored actor from the People's Republic of China, have been known to target such vulnerabilities for espionage, emphasizing the critical need for robust cybersecurity measures in IoT devices.[26] While OEMs and automotive suppliers take multiple measures to secure the integrity of data generated by CVs, any federal action must be proportional to the increasing level of risk associated with vulnerable components.

3. **Cybersecurity Risks**: CVs rely on complex software systems and communication networks, making them vulnerable to cyberattacks. After the decline of vertical integration in the automotive industry during the 1980s, OEMs began outsourcing most vehicle component sourcing, including both hardware and software. For example, one

[21] Adam Forrest, "China tracked Rishi Sunak using device hidden in car, says ex-Tory leader," The Independent, August 7, 2023.
[22] Keith Bradsher, "What to Know About China's Export Dominance," The New York Times, April 19, 2024
[23] H.J Mai, "Chinese Electric Carmakers are Taking on Europeans on Their Own Turf — and Succeeding," NPR, February 18, 2024.
[24] Matthew Henderson, "China could use its electric cars to attack the West," The Telegraph, March 23, 2024.
[25] Ibid.
[26] MITRE ATT&CK®, "Volt Typhoon, BRONZE SILHOUETTE, Group G1017," 2024; and Sam Sabin, "China's attacks on U.S. infrastructure aren't going anywhere," Axios, April 14, 2024.

leading OEM reported that only 10 percent of the software code in their vehicles was developed in-house, with the remainder sourced from various suppliers.[27] This shift has introduced multiple complexities and dependencies into the supply chain.[28]

OEMs and Tier-1 suppliers source different components like sensors, cameras, telematic trackers, and diagnostic devices from multiple Tier-2 and Tier-3 suppliers. Each component's quality and safety are the responsibility of its manufacturer and assembler. Due to this cascading multi-tiered supply chain, even a single flaw or unaddressed vulnerability in a module can affect millions of vehicles. Data from publicly reported automotive-related vulnerabilities shows that more than 70 percent of all cyber vulnerabilities are reported from Tier-2 and Tier-3 suppliers.[29]

The interconnected nature of the supply chain emphasizes the need to secure every component, including the foundational hardware layer, embedded operating system, and user applications, to prevent supply chain cyberattacks like the SolarWinds Orion breach in 2020.[30] The SolarWinds Orion platform, a widely used American network management tool, was hacked by Russian state-sponsored groups who compromised the tool's software update mechanism. Malicious code inserted in the software updates enabled hackers to then gain access to the networks of numerous organizations, including U.S. government agencies and major corporations. This breach was notable for its scale, stealth, and the high-profile nature of the targets affected.

Last year, ORBCOMM, a U.S.-based satellite telecom and logistics company, was targeted in a ransomware attack that disrupted its trucking fleet management systems.[31] The attack caused service outages for thousands of electronic logging devices (ELDs), which track drivers' hours in compliance with federal regulations. This outage lasted for three weeks and affected some of the largest U.S. freight transportation companies. In response, the Federal Motor Carrier Safety Administration (FMCSA) issued an exemption allowing truckers to use paper logs to track their hours and location of inventory in the absence of working GPS-enabled ELDs.[32] The risks that such an attack poses to the operations of the nation's critical infrastructure like ports, highways and other supply chains are dramatic and increasing in both likelihood and potential scope.

---

[27] Henry Man, "Volkswagen to Develop In-House Software for Next-Gen Cars," CarExpert, 22 June, 2020.
[28] Robert Charette, "How software is eating the car," *IEEE Spectrum*, March 29, 2023.
[29] Yoav Levy et al., "Upstream's 2024 Global Automotive Cybersecurity report," Upstream Security, February 7, 2024, at Pg. 43-44.
[30] See, e.g., Cybersecurity and Infrastructure Security Agency (CISA), "ED 21-01: Mitigate SolarWinds Orion Code Compromises," December 13, 2020.
[31] See, e.g., Lawrence Abrams, "ORBCOMM Ransomware Attack Causes Trucking Fleet Management Outage," BleepingComputer, September 15, 2023.
[32] Federal Motor Carrier Safety Administration, United States Department of Transportation, "Extension for the Use of Paper Records of Duty Status for Users of Electronic Logging Devices Registered by ORBCOMM", September 12, 2023.

Demonstrating the continued vulnerability of ELDs, researchers from Colorado State University in 2024, found multiple ELD brands that can be exploited to remotely control, manipulate data, and spread malware in more than 14 million medium- and heavy-duty trucks in the United States.[33] This highlights the transportation sector's vulnerability to cyber threats and the ease with which national security and economic activities can be sabotaged.

These examples not only illustrate the susceptibility of transportation technologies to cyberattacks but also set the stage for understanding how these vulnerabilities can extend into even more personal aspects of technology use. In 2015, two security researchers wirelessly hacked into a Jeep Cherokee's entertainment system to take control of its steering, brakes, transmission and infotainment system and guided the vehicle into a ditch.[34] A Wall Street Journal investigation showed the ease of physically and digitally hacking into an electric charging unit, subsequently infiltrating the home Wi-Fi system and potentially tracking internet usage and credentials across the household.[35] A hacked charger can lead to broader issues, including, in theory, the disruption of the power grid. While an individual charging unit might not have a direct connection to the entire power grid, vulnerabilities in the charging infrastructure can be exploited by state-sponsored hackers to gain access to multiple chargers or a charging network. This can potentially bring down or disrupt the operations of an entire power grid.[36] This highlights the increasingly critical role that OEMs, Tier-1 suppliers, and cyber security providers have in preparing for, mitigating, and monitoring these risks.

Although OEMs and Tier-1 suppliers do a good job securing and controlling gateways to assembled vehicles, Chinese-made components or software might contain hidden backdoors or vulnerabilities that could be exploited by malicious actors, including state-sponsored hackers, to gain unauthorized access to vehicle systems or compromise safety-critical functions.[37] China's significant involvement in supplying crucial components, coupled with the potential exploitation of cyber vulnerabilities to access valuable and sensitive information from CVs, adds a layer of concern. Therefore, it is crucial for the United States and its allies to proactively monitor and holistically address these risks to avoid yielding significant ground to adversarial foreign entities across various spheres, including technology, economy, and defense.

4. **Intellectual Property Theft**: China's increasing prominence in connected and autonomous vehicle (CAV) technologies presents several challenges internationally,

[33] Jake Jepson et al., "Commercial Vehicle Electronic Logging Device Security: Unmasking the risk of Truck-to-Truck Cyber worms," *Symposium on Vehicles Security and Privacy,* February 26, 2024.
[34] "Hackers remotely kill a jeep on a highway," WIRED Channel, YouTube Video, July 21, 2015.
[35] "This is how easy it is to hack EV chargers, The Wall Street Journal Channel, YouTube Video, March 18, 2024.
[36] Tik Root, "EV charger hacking poses a Catastrophic risk," WIRED, July 5, 2023.
[37] Note: The Upstream 2024 Global Automotive Cybersecurity report highlights the total publicly disclosed attacks on the automotive supply chain. Very few are conducted via or on a connected vehicle, the attacks are majorly on associated infrastructure like dealership networks, OEM websites or third-party brokers.

especially for the United States and its allies. In the past, Chinese companies have been accused of engaging in intellectual property theft and industrial espionage to acquire advanced technologies related to CVs. This poses a national security concern as it could undermine the competitiveness of Western companies and compromise valuable intellectual property assets.

For example, driven by strong industrial policies and strategic acquisitions, Chinese firms such as Hesai dominate the global automotive light detection and ranging sensors (LiDAR) market with the support of government subsidies and potentially discriminatory practices.[38] LiDAR is a key enabling technology for CVs as well as automated driving systems and military applications. Hesai's ongoing arbitration with an American company, Ouster, underscores an ongoing pattern of IP theft allegations against Chinese companies.[39] Hesai, accused by Ouster of infringing on several patents, holds a dominant share of the LiDAR market and is often cited for its quick development and lower costs, thanks to substantial scale and subsidy advantages.[40]

This market dominance not only gives Chinese entities control over crucial intellectual property but also raises concerns about personal privacy and the pace of technological innovation. Moreover, as advanced transportation technologies often overlap with military applications, China's leading position in setting international transportation standards and leveraging subsidies to corner the market for key strategic parts of the supply chain could strengthen its global influence and ultimately undercut U.S. military capabilities and economic competitiveness.

The integration of advanced technologies like LiDAR, GPS navigation systems, and wireless communication protocols into CVs presents dual-use potential that could extend to military or intelligence applications. Modern military vehicles, for example, integrate technologies like the Controller Area Network bus (CAN bus), initially developed for commercial vehicles. It serves as the nerve center for a vehicle, and with the integration of wireless connectivity modules can support the remote monitoring of vehicle performance and maintenance needs. Furthermore, military vehicles are increasingly networked, linking computers, data sources, radios, sensors, and navigation systems that are essential for operational and mission-critical activities. These advancements mirror the sophisticated network systems now standard in civilian vehicles. Control over such technologies that have a dual-use again can raise significant concerns if the involved company has links to a foreign adversary's military or intelligence sectors opening the possibility of sensitive technologies to be transferred in ways that might affect national security.

[38] See, e.g., Karen M. Sutter et al., "U.S.-China Competition in Emerging Technologies: LiDAR," Congressional Research Service, August 14, 2023.
[39] See, e.g., Federal Bureau of Investigation, "Executive Summary - China: The Risk to Corporate America," 2019
[40] Molly Bignon, "In China-U.S. Lidar Fight, National Security Threats are more Speculation than Smoking Gun," Automotive News, October 18, 2023.

The situation is further complicated by the blurred lines between state and private ownership by foreign adversaries, in particular China. From 2000 to 2019, there was a dramatic increase in the number of private owners with direct and indirect state ties – nearly tripling for direct ties and increasing fifty-fold for indirect ties.[41] This mixed ownership model in China, where private entities may also have state roles or connections, underscores the complexity of assessing and managing the risks associated with the transfer of potentially sensitive technologies.

These broader trends suggest that the rapid growth and technological advancement in China's automotive and connected vehicle sectors, supported in part by state connections, could have broader implications beyond commercial success, influencing sectors as critical as national defense and intelligence.

5. **Geopolitical Influence**: The Chinese government and other foreign adversaries have strategic interests in promoting their domestic automotive industry and expanding their influence in global markets. As such these investments in foreign automotive companies or infrastructure projects related to CVs may be driven by geopolitical considerations, potentially leading to or even designed to establish strategic vulnerabilities or dependencies for other countries. As the examples above have shown, the automotive and ICTS supply chains have key strategic dependencies on Chinese companies and technologies that can be potentially leveraged in political or economic negotiations and might influence the policies or economic decisions of other countries. Simultaneously, China's "Delete A" initiative, formally known as Document 79 aims to remove any reliance on American technology by mandating the replacement of American-made software and hardware by 2027.[42] This strategy is part of a larger effort by China to assert its sovereignty over its technological developments, reduce vulnerabilities from international tensions, and potentially lead in new technological arenas that could serve its broader geopolitical objectives.

Overall, the integration of CVs and their enabling technologies presents complex national security challenges, particularly in the context of the Chinese government's involvement. Addressing these concerns requires a multifaceted approach involving collaboration between governments, industry stakeholders, and cybersecurity experts to mitigate risks and ensure the security and integrity of connected vehicle systems. In order to effectively address these concerns, the Department should further clarify what constitutes "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries…" For example, ReMo does not believe that any particular level of ownership or legal control of a company is required for a foreign adversary to exercise "control" over an entity subject to its jurisdiction, or even entities with U.S. subsidiaries. In addition, the governments of foreign adversaries are likely to maintain the ability to exercise

[41] Chong-En Bai et al., "The Rise of State-Connected Private Owners in China," *National Bureau of Economic Research*, December 2020

[42] Liza Lin, "China Intensifies Push to 'Delete America' From Its Technology," Wall Street Journal, March 7, 2024.

control over businesses in their jurisdiction even in the absence of an ownership stake in the company. Given the myriad of ways through which foreign adversaries may use leverage over so-called "privately owned" companies, further clarification will be beneficial. Below we have provided selected answers to the specific questions asked in the ANPRM where ReMo has specific expertise that maybe of value to the Department.

Issue 1: Definitions

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 term "connected vehicle" is sufficiently broad, and could apply to the vast majority of new vehicles and many existing vehicles on U.S. roads. Contrary to some popular perception that CVs must have built-in telematics or a dedicated electronics control unit with an embedded SIM, even vehicles from two decades ago that incorporate local connectivity options like Bluetooth or USB ports qualify as CVs. These older models along with modern vehicles that offer over-the-air updates or turn-by-turn directions are all part of the connected vehicle spectrum.[43] Based on the Federal Reserve Economic Data (FRED), almost 70 percent of vehicles (200 million of 283 million vehicles) on American roads are potentially CVs. This percentage continues to rise as older, non-connected vehicles are retired, and new vehicles – approximately 16 million, more than 90 percent of which come equipped with built-in connectivity – are added to the U.S. fleet.[44] These vehicles can be traditional internal combustion engine (ICE) vehicles, electric vehicles (EVs), hybrids, or vehicles powered by alternative fuels.

In addition, the non-vehicle technology infrastructure that CVs connect to, such as cloud services, physical infrastructure, third-party vendor technology, or consumer devices, should be captured within the scope of the existing ICTS regulations and therefore may be pulled into the scope of any proposed regulation. The increase in the number of CVs will coincide with the surge in broader technological advancements in urban environments, notably the development of smart cities. GSMA Intelligence forecasts that there will be 1 billion smart city IoT connections by 2030.[45] The provided definition ensures that all aspects of the ecosystem surrounding CVs are considered for security, privacy, and compliance, providing a more holistic approach to managing the risks associated with CV technology. Such regulations are vital to safeguard the interconnected nature of these technologies and to protect against potential vulnerabilities that could arise from their integration.

[43] Andrea Amico, "P4CS Five levels of Vehicle Connectivity," Privacy4Cars, May 15, 2022.
[44] ReMo analysis based on data from the Federal Economic Reserve Data and ABI Research.
[45] Roger Berg, "The Role Of Infrastructure in Connected Vehicle Services," Automotive Edge Computing Consortium, June 23, 2023.

Issue 2: Risks: Supply Chain, Manufacturing and Assembling origins

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

Current Supply Chain

The ICTS supply chain for CVs is a highly complex, characterized by third-party integrators and contract manufacturing.[46] In the late 1980s, automotive companies responding to declining profits and structural and technology changes, moved away from a vertical-integrated supply structure to sourcing from multiple suppliers. As parts suppliers spun out of OEMs, the percentage of parts that independent suppliers assembled in a vehicle went up from 40 percent in the 1990s to 70 percent in 2017.[47] OEMs and Tier-1 suppliers centralize the assembly of various components before they are built into a vehicle. OEMs focus on overall vehicle design, vehicle and system assembly, portfolio balance, marketing, sales strategy, vehicle support and maintenance, and other key tasks. On the other hand, Tier-1 suppliers design and develop complete systems or modules by sourcing individual components from Tier-2 suppliers, who, in turn, procure materials and parts from Tier-3 suppliers.

This complex supply chain structure, with its multiple levels of sourcing and assembly, introduces significant security risks, especially when components like vehicle tracking devices come with potential backdoor vulnerabilities. For example, an aftermarket vehicle tracking device manufactured by MiCODUS, a Tier-3 supplier based in Shenzhen, China, could be integrated into a telematics module at a supplier's plant in Mexico.[48] The assembled module would then be shipped to a U.S.-based user for connection to their. Once connected, the telematics system can access vehicle data such as location, speed, and engine diagnostics. MiCODUS's popular MV720 GPS trackers installed in over 1.5 million vehicles were found to be vulnerable to real-time tracking by unauthorized users who could access historical routes and cut off the engine while the vehicle was in motion.[49] Another example is the Minth Group, based in Ningbo, China, which transitioned from being a Tier-2 supplier to directly selling to OEMs and is now listed among the top 100 OEM Tier-1 suppliers.[50] Part of Minth's portfolio includes manufacturing seat frame systems (seatbelts, trims, and seat tracks) that used to be sent to a seat producer in China or Mexico to be integrated into seats before being sent to a vehicle manufacturer.[51] Now, the Minth Group has a separate American subsidiary that owns a growing Tennessee facility that caters to major automakers.[52]

[46] John Joyce, "OEM and Tier Suppliers: What a Tangled Web They Weave, Brennan Blog, June 24, 2022.
[47] Department of Commerce, "Report on the Effect of Imports of Automobiles and Automobile Parts on the National Security," November 8, 2021.
[48] MICODUS, "Professional Global Positioning Solutions Provider," 2024.
[49] Zack Whittaker, "Security flaws in a popular GPS tracker are exposing a million vehicle locations," TechCrunch, July 19, 2022.
[50] "Automotive News Top Suppliers, Ranked by Total OE Automotive Parts Sales," Automotive News, June 25, 2023.
[51] The Minth Group 敏实集团, "Product Development," 2024 and David Coffin, "China's Growing Role in U.S. Automotive Supply Chains," Office of Industries Working Paper, August 2019 at Pg. 8.
[52] Audrey LaForest, "Minth Group to invest $87M in auto parts facility in Tennessee," Plastics News, January 22, 2020.

U.S. Strategic Reliance on China and its Importance in the Auto Supply Chain
While not all supplier relationships pose a national security risk, it is important to highlight that a complete ban or decoupling from Chinese suppliers would likely have adverse effects. Instead, the emphasis should be on securing the supply chain of components, particularly those controlling connectivity or off-vehicle data storage, that are critical to addressing national security concerns.

The reliance of U.S.-based OEMs on imported auto parts is illustrated by the fact that Mexico is the primary supplier of auto parts to the United States, accounting for roughly 40 percent of U.S. imports.[53] Notably, Canada and China are the next largest suppliers and both account for roughly 10 percent of U.S. imports.[54] China though, is unique among the top auto parts supplier countries in not also being a significant source of vehicle imports into the United States.[55] Chinese-made auto parts enter the U.S. automotive supply chain as sub-component suppliers for parts produced in Mexico and Canada. Nearly half of the auto imports from China are under a NAICS-coded 'Other Parts' basket category that includes a wide range of parts and accessories like seat and seat belt parts, windshield wipers and truck bed components.[56] The other major components imported include electronics (generators, lighting and wiring sets), brake rotors, lithium-ion batteries and engines (spark ignition and diesel engines).[57]

The Chinese auto parts industry has seen significant growth over the past two decades, driven initially by increased domestic demand, government policies, and later by their integration into global supply chains. In 2007, no Chinese companies were listed in the Automotive News Top 100 Global OEM Parts Suppliers list. In 2023, thirteen Chinese companies made the list directly supplying to OEMs and, in many instances, have a U.S.-based subsidiary. Contemporary Amperex Technology Co., Limited (CATL), the global leader in EV battery manufacturing leads the pack, followed by companies like Yanfeng, specializing in automotive interiors, and others like Joyson Electronics, Beijing Hainachuan Automotive Parts Co. Ltd (BHAP), CITIC Dicastal Co., Johnson Electric Group, Ningbo Huaxiang Electronic Co., the Minth Group, Nobo Automotive Systems, Huizhou Desay SV Automotive Co., Ningbo Tuopu Group and Anhui Zhongding Sealing Parts Co., which supply a range of automotive parts to global customers.[58] Despite their growth, most top Chinese suppliers are Tier-2 and Tier-3 suppliers, a fact lamented by the Chinese Communist Party's political advisory body.[59] It is difficult to disentangle these companies from the crucial role they play in the supply chain, but it is not unforeseeable to see more Chinese

[53] Óscar Goytia, "Mexico Supplies 42.5% of US Auto Parts Imports," Mexico Business News. April 9, 2024
[54] Ibid.
[55] David Coffin, "China's Growing Role in U.S. Automotive Supply Chains," Office of Industries Working Paper, August 2019 at Pg. 8
[56] Ibid. Pg 11.
[57] Ibid. Pg 8-11; and Note: Chinese companies supply 80 percent of the world's battery cells and account for nearly 60 percent of the EV battery market.
[58] "Automotive News Top Suppliers, Ranked by Total OE Automotive Parts Sales," Automotive News, June 25, 2023.
[59] China Briefing News, "China still a Tier-3 Manufacturer in Global Rankings," Dezan Shira and Associates, March 19, 2021.

Tier-2/3 suppliers making the Top 100 list and graduating from wipers to producing sensitive advanced components for the increasing number of CVs in the United States and other countries.

Given the above-described interconnected nature of the connected vehicle supply chain, the role of OEMs and Tier-1 suppliers to secure every component is essential to prevent potential vulnerabilities. Categories of ICTS integral to CVs operating in the United States include:

> **Foundational hardware layer**, the physical connected components of the vehicle including the chip on which an embedded operating system is installed (e.g. sensors, cameras, LIDAR, Radar, engine control units, tire pressure and battery management systems, controllers and Advanced Driver Assistance Systems (ADAS));
> **Embedded operating system**, a digital layer that connects the hardware to a user-facing, analytics and tracking platform and;
> **User applications**, software and services that interact directly with the driver (e.g. data analytics, cloud services, infotainment and driver control systems).

Although a supplier might have secure gateways, integrating different technologies from various manufacturers without a comprehensive understanding of potential risks and vulnerabilities can pose significant challenges. Even with secure gateways, unrecognized vulnerabilities can potentially lead to supply chain cyberattacks, compromising the security of the target organization by exploiting vulnerabilities in third-party suppliers. The largest cyberattack to date affected SolarWinds, an American company that develops software for businesses to manage their IT infrastructure. In 2020, a breach in their Orion platform affected 18,000 public and private organizations by distributing malicious code through software updates authorized by SolarWinds and granting state-sponsored Russian hackers unauthorized access to networks and systems. The attack remained undetected for two years due to the malware's ability to blend in with legitimate activity, enabling sustained access and data theft. As the global automotive industry continues to evolve, the intricate and layered supply chain for CVs highlights a critical area of concern, especially regarding national security and technological sovereignty. Over three decades, the shift towards relying heavily on external suppliers, particularly from China, has not only reshaped the landscape of automotive manufacturing but also raised potential cybersecurity risks. The only effective mechanism to counter these risks is for the United States and its allies to bolster its domestic capabilities in automotive technologies and reduce vulnerabilities within its supply chains. Strengthening these aspects is crucial to maintaining technological leadership and ensuring the security of critical infrastructure, particularly as the intersection of automotive technology and cybersecurity becomes increasingly prominent on the national stage.

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?**

LiDAR is one technology in which China is building a dominant market position. LiDAR is a remote sensing method that uses light in the form of a pulsed laser to measure distances to objects. LiDAR is critical to reimagining (civilian) mobility because most vehicles with autonomous capabilities use LiDAR sensors to detect and avoid obstacles, map their surroundings, and navigate roads safely.[60] LiDAR is also used as part of ADAS systems, helping with object detection and collision avoidance, pedestrian detection, lane assistance, adaptive cruise control, and parking assistance among other functions. LiDAR is also installed in fixed hardware for purposes of monitoring and/or data collection as part of an extended smart cities ecosystem. There are also extensive military applications for LiDAR technology.

LiDAR is relevant to several critical technology sectors identified as important to the national security of the United States on a Critical and Emerging Technologies List, which was prepared by the National Science and Technology Council.[61] Hesai Technology, headquartered in Shanghai, China, has emerged as a leading provider of LiDAR solutions globally. The company has garnered attention for its cutting-edge LiDAR sensors, which offer high performance, reliability, and affordability, making them accessible to a wide range of industries and applications. The company invests significantly in innovation, continuously refining its products to meet evolving industry needs and standards. As LiDAR technology continues to play a crucial role in shaping the future of transportation and urban development, Hesai Technology's contributions are poised to drive significant advancements in autonomy, safety, and efficiency. Hesai and other Chinese firms now hold 58 percent of the global market share in the automotive LiDAR segment.[62] The CCP is considering imposing an export ban on LiDAR technologies, underlining this technology's strategic importance.[63]

While ReMo believes the immediate national security risk of Chinese-supplied LiDAR is limited, provided OEMs and Tier-1 suppliers effectively oversee their installation and operation and they cannot transmit data independently, we believe there is medium- and long-term risk to not developing and supporting robust supply chains for this technology that are not controlled by or influenced by foreign adversaries. Such domestic and allied supply chains are necessary not only to derisk consumer and commercial vehicle applications but imperative when considering the needs of key defense applications.

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.**

[60] Naseeb Souweidane, et al., "State of ADAS, Automation, and Connectivity," Center for Automotive Research, March 2023.
[61] "Critical and Emerging Technologies List Update," National Science and Technology Council, March 2022.
[62] Steve Dyer et al., "China's Proposed Export Ban on LiDAR Technology: What Impact Will It Have on the Automotive Industry?" AlixPartners, April 5, 2023.
[63] Patricia Nilsson et al., "Carmakers raise concerns at Chinese dominance over connectivity patents," Financial Times, April 29, 2023.

First, disruptions to the supply of ICTS components for CVs can indeed have significant ramifications for OEMs of CVs in the United States and ICTS suppliers. The semiconductor shortage following COVID-19 provides an example of supply chain disruption and mitigation for a critical component in vehicle manufacturing. As demand for vehicles soared, manufacturers experienced a semiconductor shortage that constrained production for two years.[64] This shortage led to the removal of more than 11 million vehicles from production lines in 2021.[65] Consequently, global car sales experienced a decline of more than 12 percent compared to 2019 figures, resulting in an estimated revenue loss of approximately $210 million US for the global automotive industry.[66] In the first half of 2023, losses directly attributed to the semiconductor shortage decreased to approximately 524,000 units worldwide.[67] While the supply of semiconductors continues to be limited, the more predictable availability has enabled automakers to adjust their production schedules accordingly. Like the semiconductor shortage, policy changes around ICTS components are likely to cause disruptions and have the potential to constrain vehicle manufacturing in the near term. Over the long term, the United States stands to benefit from efforts to eliminate potential chokepoints in the ICTS supply chain. Second, it is important to acknowledge that not all ICTS components will be equally affected by disruptions. During the 2020 semiconductor shortage, industries experienced uneven effects because certain semiconductor components were in varying degrees of short supply. Consumer, communications, and computer electronics hold 70 percent of the demand for semiconductor chips, followed by the industrial and automotive demand which each represents 14% respectively. The final 2% of demand comes from government applications.[68] Technological advances in the automotive industry, such as vehicle electrification, automation, and connectivity, have brought with them a need for a greater quantity of more advanced chips. This is why during the semiconductor shortage, the automotive industry experienced the bulk of the disruption due to the need for more advanced chips. Likewise, certain U.S. ICTS-reliant companies may experience disruptions more acutely than others. The disruption can occur via hardware or software, therefore, it is imperative to conduct a thorough analysis to identify and prioritize these vulnerabilities and implement targeted mitigation strategies.

Further, there are clear advantages to both localization and diversification of the ICTS supply chain. Localizing the supply chain in the United States can enhance resilience by reducing dependence on foreign sources for critical components, thereby mitigating the risk of disruptions caused by geopolitical tensions. Additionally, diversifying the supply chain in collaboration with allies can offer increased flexibility and redundancy, ensuring that alternative sources are available in the event of disruptions.

[64] See, e.g., Ben Klayman, "Ford's Pain Underscores Uneven Impact of Two-Year Auto Chip Shortage," Reuters, February 3, 2023.
[65] Applied Energy Systems, "Navigating Complexities: The Semiconductor Shortage's Effect on the Auto Industry," November 30, 2023.
[66] Ibid.
[67] IHS Markit, "The semiconductor shortage is – mostly – over for the auto industry," July 12, 2023.
[68] *2023 Factbook*. (n.d.). Semiconductor Industry Association. May, 2023.

In conclusion, while disruptions to the supply of ICTS components for CVs present significant challenges for OEMs and ICTS suppliers in the short term, there is an opportunity to leverage these challenges as catalysts for long-term improvements in supply chain resiliency. By proactively identifying vulnerabilities and implementing strategic mitigation measures, the United States can strengthen its position as a global leader in connected vehicle technology while minimizing the impact of adversarial disruptions.

Issue 3: ***Risks: Data Security, Cybersecurity and Connectivity***

While the amount of data generated by a CV has increased exponentially over the past decade (25 gigabytes per hour on older models to 19 terabytes per hour on newer, more advanced vehicles), the bulk of data is processed onboard and only an extremely limited amount is transmitted from the vehicle for discrete purposes including remote diagnostics, maintenance and performance, and cloud-based services.[69] Similarly, data brought onto the vehicle competes for a limited and managed bandwidth via a discrete number of transmission points (e.g., 5G cellular systems installed by the OEM for connected services and telematics, a mobile device connected via a USB port, the OBD port, or a Wi-Fi connection). Similar to a computer or cellphone, these connections and what access they have with regard to the underlying software and hardware of the vehicle, are controlled by the device manufacturer and operating system(s) installed.

When identifying the direct national security risks (not considering economic competitiveness or indirect geopolitical risk) of foreign adversary influence or control over parts of the connected vehicle ecosystem, the focus should be on the mechanisms to transmit to a vehicle, remove data from a vehicle, and to store, access, and analyze this data. Focusing on these connection points, data access, and data storage and where they provide opportunities for foreign adversaries to exercise designed or malicious action will be the most immediate and effective way to consider the broader national security risks of CVs and their supporting ecosystem.

ReMo has identified two of the Department's questions below to highlight where we believe additional consideration and discussion is appropriate in the context of national security.

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)?

As outlined above, cybersecurity concerns surrounding connection points in a CV should primarily address unauthorized access beyond the intended scope defined and integrated by the OEM. Sensors in and of themselves do not pose an inherent and direct national security

[69] John Verdi, "A Privacy Playbook for Connected Car Data", Future of Privacy Forum. October, 2019; and Coalition for Reimagined Mobility, *Unlocking a 21st Century Mobility System: How to Rethink the Future of Mobility and Restore Leadership in Transportation Innovation*, January 8, 2024, at Pg. 65;

concern, absent their ability to transmit data independently off the vehicle or circumvent permissions to utilize a connection point. While an individual sensor or component might have its stand-alone connectivity (e.g., a tire pressure monitoring system or installed telematics system) the expectation is that these are known and considered by the OEM during the vehicle design and assembly process, and are limited in their permissions to access or update the system accordingly (e.g., a device connected via the OBD or USB port within the vehicle should be limited in its ability to send/receive data). Additionally, the operating system installed on the vehicle and the cybersecurity processes implemented are expressly designed to limit access and identify unexpected or malicious attempts to circumvent installed security principles.

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?

Data storage and transmission are critical aspects of CVs, as they involve the generation, processing, and sharing of vast amounts of potentially sensitive information. This includes not only vehicle operation data but also personal and location data of drivers and passengers. If these functions are handled by entities under the influence of foreign jurisdictions, especially those with inadequate data protection laws or government-mandated data access requirements, it significantly heightens the risk of unauthorized access, data breaches, and potential exploitation by malicious actors. This creates a substantial risk of data misuse, espionage, or sabotage, posing serious threats to the safety, security, and privacy of CVs and their users.

Research shows that data leaks from message queuing telemetry transport (MQTT) brokers is a weak point in the automotive data ecosystem.[70] MQTT brokers serve as a critical component in the automotive data ecosystem, facilitating the exchange of data between various components of CVs, such as sensors, control units, and backend servers.[71] They pose a risk of data leaks due to factors such as insecure configurations, lack of end-to-end encryption, insufficient authentication and authorization mechanisms, data retention practices, and integration with legacy systems. These vulnerabilities could lead to unauthorized access, interception, or modification of sensitive data transmitted through the brokers. The world's largest open-source MQTT broker is Chinese-based EQMX.[72]

MQTT brokers subject to the jurisdiction or direction outlined in 15 CFR 7.4, particularly those associated with certain foreign governments or entities, may be compelled to share data with foreign intelligence services or other entities, even if such actions are illegal or unethical under the laws of the jurisdiction where the data is generated or processed.[73] This creates a

[70] Numaan Huq et al., "Automotive Data: Opportunities, Monetization, and Cybersecurity Threats in the Connected Vehicle Landscape," Trend Research for VicOne, December 3, 2023.
[71] Numaan Huq et al., "Preempting Threats to Connected Cars: The Importance of Cybersecurity in a Data-Driven Automotive Ecosystem," Trend Research for VicOne, November 15, 2023.
[72] EMQX, "About the Company," 2024.
[73] Ryan Flores, "MQTT and M2M: Do You Know Who Owns Your Machine's Data?" Trend Micro, October 9, 2023.

substantial risk of data misuse, espionage, or sabotage, posing serious threats to the safety, security, and privacy of CVs and their users.

Therefore, ensuring that data storage and data transmission in CVs are entrusted or facilitated by entities with robust data security measures, transparent data handling practices, and adherence to stringent privacy regulations is paramount for safeguarding national security and protecting the integrity of the connected vehicle ecosystem.

Issue 4: Authorizations & Mitigation

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?

ReMo and SAFE, as outlined in detail above, are concerned about the threats to the connected vehicle and broader automotive industry. Foreign adversaries are cornering and leveraging key supply chains to geopolitical and economic ends, setting up the risk of access to remote data collection for strategic intelligence and opening vulnerabilities to cyber-attacks on U.S. soil. The scope, scale, and urgency of this national security risk comes at the same time the automotive industry is experiencing a transformational shift that offers tremendous potential to improve the convenience, safety, and efficiency of our transportation system.

ReMo recognizes that in prohibiting some categories of transactions the Department is trying to strike a balance between two goals in tension: not hindering the adoption of advanced technology critical to safety, fuel efficiency, and competitiveness, and ensuring that ICTS supply chains are developed in a manner that is secure and does not undermine the national security of the United States and its citizens. It is therefore our view that there should be very few instances, if the Department were to prohibit a transaction, that temporary authorizations should be offered. If the Department were to offer temporary authorizations, the Department should carefully consider providing only the minimum time necessary for the industry to shift and find alternatives in the event of a supply chain disruption. Such a decision may not be easy but is necessary for the long-term security of our nation.

# # #

III. Conclusion

The Coalition for Reimagined Mobility (ReMo) is committed to advancing a vision for new mobility technologies and services to shape transportation outcomes that are more efficient, secure, sustainable, and resilient for people and the planet. The Coalition pursues this reimagined transportation future by convening global leaders, developing bold strategies, advocating for outcomes and deploying solutions that address consumer challenges, regulatory hurdles, and system-level dynamics in our global transportation systems.

ReMo prioritizes high-impact initiatives to reduce political and policy gridlock and enable bold action to improve mobility for people and goods. In this context, the threats to the connected vehicle industry – and the broader automotive industry – are fundamental and pressing. Foreign adversaries, especially the People's Republic of China, are dominating and exploiting critical supply chains for geopolitical and economic advantages, posing the risk of remote data access for strategic intelligence gathering and increasing the vulnerability to cyber-attacks with the U.S. The scope, scale, and urgency of this national security risk comes at the same time the automotive industry is experiencing a transformational shift. New technologies are being adopted quickly, which means the complexity of the threat facing the United States will only accelerate in the coming years. We look forward to working with the Department and leaders in Congress to address the national security vulnerabilities that may be prevalent throughout the ICTS supply chain.

Our primary objective in submitting these comments is to assist the Department in its efforts to support both consumers and the industry while fostering secure supply chains essential for this critical economic sector's continued contribution to our nation's economic growth, industrial base, and security. We hope our insights will be valuable in shaping the Department's strategies.

Again, we would welcome the opportunity to answer any questions about these comments or discuss them with officials from the Department of Commerce. If you have any questions about our comments or the issues therein, please contact Avery Ash at aash@secureenergy.org or (202) 674-3794.

Thank you for the opportunity to offer comments concerning the CV industry and its related ICTS supply chain.

Sincerely,

Avery Ash

Executive Director, Coalition for Reimagined Mobility (ReMo)
Senior Vice President of Government Affairs and Special Initiatives, SAFE