COALITION FOR
Reimagined Mobility
Transportation Policy that Puts People First

SAFE

October 28, 2024

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

RE: (RIN 0694-AJ56) Docket Number BIS-2024-0005, 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 SAFE, commends the Department of Commerce and the Bureau of Industry and Security (BIS) for taking critical steps to address the national security risks posed by foreign adversaries, particularly the People's Republic of China (PRC) and Russia, in the connected vehicle ecosystem. The Notice of Proposed Rulemaking (NPRM) titled *Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles*, outlines important measures to prohibit the sale or import of connected vehicles and components with a nexus to these adversaries, helping safeguard U.S. drivers and critical infrastructure from potential exploitation and manipulation. While coordinated action across federal agencies and internationally with our allies is ultimately necessary to address the broad risks of an adversary leveraging supply chains to undermine our economic or national security, we believe this proposed rule by the Department will meaningfully mitigate the national security implications in the connected vehicle supply chain.

ReMo believes 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. We are glad to see the Department has taken many of the risks and necessary actions recommended in our initial comments into consideration when drafting this rule for maximal impact and minimal disruption.

While we support the proactive direction of this rule, we believe there are opportunities to further strengthen its impact and make its protections less susceptible to circumvention. By refining certain provisions and addressing areas such as more precise definitions of critical technologies, deeper consideration of software supply chains, and greater clarity on partnerships and joint ventures, the rule can more effectively mitigate the risks posed to our automotive supply chains. We have outlined those areas for refinement below.

1. **Clarification on Foreign Adversary Definition**

   The NPRM adopts a broad interpretation of persons or entities "owned by, controlled by, or subject to the jurisdiction or direction" of the Peoples Republic of China or Russia, as outlined in Executive Order 13873. Under this definition, a "foreign adversary" refers to any foreign government or non-government entity that engages in a consistent pattern or significant acts of behavior that pose a serious threat to the national security of the United States or the safety and security of its citizens.

   While this comprehensive approach aligns with the national security imperatives, we suggest providing more detailed guidance on how these terms apply to complex corporate or technology development structures, particularly in situations where:

   - foreign entities hold minority shares that include veto or indirect influence through investment funds
   - technology transfers and licensing agreements are in place
   - code that is written by third-party providers and integrated by a Tier-2 supplier
   - covered software for a Vehicle Connectivity System (VCS) or Automated Driving System (ADS) that is not developed by a person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, but such a person is relied on or has access to the software as part of development. For example, if such a person provides key testing, security, or development tools for the development or operation of this software, and as such has influence, knowledge, or access to the system as a result.

   While ReMo recognizes that it is not possible to address all national security risks with this rule, we believe that there is opportunity to strengthen the impact of the Department's action by further clarifying and prohibiting instances where the PRC or Russia may seek to exploit access to the supply chain to undermine U.S. national security.

   Additionally, while we agree with the Department on the need for clear definitions and strong prohibitions on the business structures, ownership models, and relationships that companies might have that should disqualify them from supplying vehicles on U.S. roads, it is important that these rules cannot be leveraged against U.S. companies. We would be particularly concerned that the CCP or Russia could leverage this rule to strategically undercut U.S. businesses by purchasing, investing in, or otherwise establishing a relationship with a VCS or ADS supplier that would void the ability for a manufacturer to be able to sell finished products in the United States. An example of how this might happen is below.

Example:
Company A, incorporated in the United States, is a manufacturer of connected vehicles. Company A contracts with Company B to supply VCS hardware. Company B is a U.S.-based supplier that is not owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. Company B receives a significant minority investment from Company C, a state-owned enterprise of the PRC or Russia. Due to Company C's investment, Company A's use of VCS components from Company B would render the final vehicles ineligible for sale in the United States under the proposed rule. Under the proposed rule, Company A would have 30 days to notify the Department of the change to the hardware bill of materials (HBOM) and would be unable to sell vehicles that are using this supplier.

In this example the proposed rule would effectively address national security by preventing a foreign adversary from access to the connected vehicle supply chain. However, this prohibition would cause significant impact to the U.S. manufacturer who would be unable to sell finished vehicles with parts from this supplier until a replacement supplier that is not owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary can be sourced and integrated into the manufacturing process.

While it will not be possible to prevent the sorts of financial transactions that would disqualify a supplier, particularly where the supplier might not be based in the United States, we would suggest the Department include language in the final rule that outlines the pathway for the Department to provide a specific authorization that would allow the manufacturer an appropriate period to adjust their supply chain without undercutting their ability to service the U.S. market in the interim.

2. **Clarification on the Definition of ADS for Connected Vehicles**

BIS defines “Automated Driving System” to mean hardware and software that, collectively, are capable of performing the entire dynamic driving task for a completed connected vehicle on a sustained basis, regardless of whether it is limited to a specific Operational Design Domain (ODD). This definition is consistent with the terminology industry uses for systems that operate at certain advanced levels of autonomy. It is also consistent with definitions issued by NHTSA. Specifically, this definition corresponds to automation levels 3, 4, and 5 as defined by SAE International standard J3016.

BIS also defines a “completed connected vehicle” to mean a connected vehicle that requires no further manufacturing operations to perform its intended function. This definition is consistent with definitions issued by NHTSA. Additionally, for the purposes of this proposed definition, the integration of an ADS into a connected vehicle constitutes a manufacturing operation for a completed connected vehicle. BIS intends this caveat to clarify that a person owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia, whose sole manufacturing or assembly operation is integrating ADS into an otherwise completed connected vehicle, would be subject to the prohibitions in the rule and would need to obtain a Specific Authorization before importing or selling that completed connected vehicle in the United States.

While BIS proposes clear definitions for ADS and completed connected vehicles, the NPRM clarifies that a vehicle becomes a "completed connected vehicle" only after the ADS (hardware and software) is fully integrated. Therefore, the rule applies to both the system and the entire vehicle once the ADS has been installed. This means that prior to ADS installation, the vehicle would not yet be classified as an autonomous vehicle (AV) or a completed connected vehicle under the rule.

If ADS is understood strictly as a software layer or system, the primary regulatory focus may fall on software compliance, potentially limiting scrutiny of hardware components integrated into the vehicle. However, if an automated vehicle is considered to encompass both VCS software and hardware and ADS software, this broader definition would likely require compliance measures that address the vehicle's entire operational system, especially once it is equipped with Level 3 or higher autonomy.

Clarification on this matter is essential to ensure consistency in compliance across the industry, as it directly impacts how manufacturers design, certify, and market their vehicles. The distinction will also influence regulatory oversight for both software-driven systems and the physical hardware that enables advanced autonomy, ultimately shaping the trajectory of innovation and safety standards in the connected vehicle ecosystem.

3. Considering Differences in Light-Duty Passenger vs. Medium- and Heavy-Duty Commercial Connected Vehicles

ReMo appreciates the agency's recognition of light-duty passenger vehicles as well as medium- and heavy-duty connected vehicles within its definition. However, the proposed rule should account for key distinctions in how supply chains and "completed vehicles" are understood between these two categories, particularly in commercial vehicles where supply chain dynamics are more constrained.

a. Supply Chain Flexibility:

Commercial vehicles generally operate in lower-volume markets compared to passenger vehicles, which can limit the availability of alternative suppliers for critical components like Vehicle Communication Systems (VCS) or Automated Driving Systems (ADS). Due to this reduced volume, commercial vehicle manufacturers often have fewer options when it comes to pivoting away from foreign suppliers or retooling their supply chains in response to regulatory changes. Unlike the passenger vehicle market, where economies of scale allow for a broader array of suppliers, commercial vehicle manufacturers may be disproportionately burdened by sudden changes in sourcing requirements.

While a change to the rule may not be necessary, we urge the agency to consider the supply chain limitations for commercial vehicles when providing General or Specific Authorizations to avoid unintended impacts on U.S. commercial vehicle manufacturers and suppliers.

b. Understanding "Completed Vehicle":

The definition of a "completed vehicle" in the context of commercial vehicles also differs significantly from passenger vehicles. In many cases, commercial vehicle manufacturers supply a basic or unfinished vehicle to a third party, who then outfits or customizes the vehicle before selling it to the end user. This process means that the original manufacturer may not have control over, or visibility into, the entire supply chain at the point of sale.

c. Regulatory Burden on Final Fitting Entities:

Under the current rule as proposed, the definition of "finished vehicle" and "sale" might unintentionally place the burden of securing and documenting the supply chain of VCS or ADS on the entities performing this final fitting. These smaller, downstream firms may lack the necessary resources or expertise to assess the compliance of VCS or ADS components, creating an undue burden on businesses that did not manufacture the critical systems themselves. In practice, this could shift significant compliance responsibility from manufacturers—who control the bulk of the supply chain—to less equipped companies, potentially undermining the intent of the rule.

ReMo recommends revising the rule to clearly delineate responsibilities for supply chain security, particularly ensuring that the burden of compliance remains with the primary manufacturer of the vehicle or critical system, rather than being passed to those engaged in final customization or distribution. This clarification will help ensure that commercial vehicle manufacturers, who have greater visibility into their supply chains, remain responsible for the integrity of VCS and ADS, while alleviating unnecessary regulatory burdens on downstream parties.

4. **Concerns with Submission of HBOM and SBOM**

While ReMo supports the need for robust transparency and supply chain security in connected vehicle systems, requiring companies to submit HBOM and SBOM inventories through a Declaration of Conformity and the storage and transmission of this sensitive data raises concerns.

a. Cybersecurity Risks of Sensitive Data:

Centralized repositories of sensitive data present attractive targets for cyberattacks. Consolidating hardware bill of materials (HBOM) and software bill of materials (SBOM) information in a single database creates a significant vulnerability, as a breach could expose critical information across multiple companies. This would provide adversaries with detailed knowledge of connected vehicle components and software supply chains, potentially allowing them to exploit security weaknesses or otherwise undermine the supply chain to undercut U.S. national security.

b. Proprietary and Confidential Business Information:

HBOMs and SBOMs regularly include proprietary and confidential details. Requiring companies to submit these inventories to a central database increases the risk of exposing sensitive business information, which would undermine U.S. companies' ability to compete globally.

With these concerns in mind, ReMo recommends that companies be required to prepare and maintain up-to-date HBOM and SBOM inventories but should only provide this information to the Department upon request, rather than submitting it to the Department by default. This approach has several key benefits:

- Enhanced Security: Decentralizing the storage of HBOM and SBOM data lowers the risk of widespread breach, as each company would be responsible for securing its own sensitive information. This would reduce the risk of a single point cyberattack that could compromise the entire industry's security.
- Protection of Proprietary Information: Companies retain control over the handling and distribution of proprietary data, ensuring it is only shared with the Department when necessary. This reduces the likelihood of competitive or operational information being exposed to adversaries or competitors.

Requiring companies to maintain these inventories but submit them only upon request strikes a balance between ensuring national security and protecting sensitive business information. This would strengthen supply chain oversight while minimizing the risks associated with centralizing sensitive data in one location.

5. **Addressing Broader Concerns Regarding Data Security**

While the NPRM takes important steps to address security risks from foreign adversary-controlled ICTS components, there remains a need for greater clarity on what happens to the data once it leaves the vehicle. We understand that this may be outside the scope of what the Department hopes to address with this rule, but we believe that it is necessary to understand this essential part of the connected car ecosystem that raises many of the same national security concerns posed by the Department as an impetus for this rule.

Connected cars 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.[1] Not all this data leaves a vehicle, but parts of it are transmitted through in-vehicle cellular connections and initially stored in data centers or cloud platforms owned by original equipment

[1] 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.

manufacturers (OEMs).[2] 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 to more effectively manage the road network or understand changes in travel patterns for planning purposes). It is also important to consider that key features of CVs and a 21st-century transportation system also 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 the physical condition and control of vehicles, data related to vehicles or occupants, and connected infrastructure, will increase.

ReMo believes that being able to effectively aggregate and leverage this data is essential to delivering a high-quality, efficient transportation system to move people and goods.
In addition to Commerce's efforts, we recognize that the Department of Justice (DOJ) is also working to address national security risks related to data access by foreign adversaries through its new Executive Order focusing on preventing access to Americans' bulk sensitive personal data.[3] This groundbreaking initiative, targeting countries of concern like China and Russia, highlights the critical importance of securing personal data from malicious exploitation.

We encourage the Department of Commerce to collaborate closely with the DOJ to ensure that a comprehensive data protection framework is in place. Such collaboration would strengthen efforts to protect sensitive information, particularly in connected vehicles where vast amounts of personal data can be at risk. By aligning Commerce's regulations on connected vehicle supply chains with DOJ's data protection initiatives, we can ensure a cohesive and robust approach to safeguarding U.S. national security and privacy.

Conclusion

The Coalition for Reimagined Mobility (ReMo) thanks the Department of Commerce and BIS for their commitment to addressing the national security risks in the connected vehicle supply chain. We believe the NPRM is an important step toward mitigating these risks, and we appreciate the opportunity to provide feedback.

Our comments have outlined several areas where the proposed rule can be refined to strengthen its protections, particularly around clarifying definitions of key terms, addressing supply chain complexities, and ensuring the rule's scope is comprehensive without disproportionately impacting U.S. businesses. We emphasize the importance of clear, actionable guidance that addresses the evolving threats posed by foreign adversaries and the need to protect critical sectors like transportation from exploitation.

[2] Mario Ortegon-Cabrera, et al. "Automotive Connected Fleets - Azure Architecture Center," Microsoft Learn, May 10, 2023.
[3] Department of Justice, "Justice Department to Implement Groundbreaking Executive Order Addressing National Security Risks and Data Security," Press Release, February 28, 2024.

While the proposed rule is a significant step forward, we urge the Department to continue identifying additional actions necessary to secure not only the transportation sector but also other key industries that are integral to national security. The rapid evolution of connected vehicle technologies, combined with the complexities of global supply chains, will require ongoing vigilance and adaptability.

We look forward to working alongside the Department to ensure these regulations are effectively implemented and stand ready to serve as a resource on this topic as it is helpful. If you have any questions about our comments or the issues therein, please contact Avery Ash at aash@secureenergy.org or (202) 674-3794 or Ashley Simmons at asimmons@reimaginedmobility.org.

Sincerely,

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

Ashley Simmons

Ashley Simmons, Deputy Director, Coalition for Reimagined Mobility (ReMo)