EXPLAINER

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

Cybersecurity Legislative Analysis Series

Bill Summary: This proposed rule establishes restrictions on the sale or import of connected vehicles using hardware or software from countries of concern—particularly China and Russia—to safeguard U.S. cybersecurity and national security.

Rating: CYBER POSITIVE This proposed rule has potential to enhance the safety and security of information and communications technology and services (ICTS) used in connected vehicles by reducing U.S. reliance on foreign hardware and software from nation-state threat actors, thereby mitigating cybersecurity vulnerabilities.

Status: Latest draft updated Sept. 26, 2024, with public comments accepted by the Department of Commerce's Bureau of Industry and Security (BIS) through Oct. 28, 2024. Possible adoption following the public comment review period, with the rule taking effect 60 days after publication in the Federal Register.

Last updated: Nov. 18, 2024

Key Provisions

- Prohibits ICTS transactions involving vehicle connectivity system (VCS) hardware and automated driving system (ADS) software components designed, developed, manufactured, or supplied by entities controlled by or under the jurisdiction of China or Russia
- Requires companies to submit an annual Declaration of Conformity demonstrating that prohibited transactions have not occurred and documenting compliance with restrictions
- Allows companies to apply for general or specific authorizations for certain restricted transactions if they can explain how any potential undue risks to U.S. national security can be reasonably managed based on established criteria
- Incentivizes connected vehicle manufacturers, VCS hardware importers, and related suppliers to voluntarily adopt more measures to help secure the U.S. ICTS supply chain for connected vehicles

Background

The continued growth of connected vehicles in the global market has introduced increasingly sophisticated software and hardware systems to enhance safety and convenience through features like light detection and ranging, advanced driver-assistance systems, and vehicle-to-everything communication. Despite the transformative benefits of these technological advancements, this expansion also presents significant challenges to U.S. national security and cybersecurity. Along with multiple points of connectivity, the sheer amount of data that connected vehicles collect creates an especially attractive target for cyberattacks. In particular, China's ongoing ambitions to dominate the global connected vehicle market and Russia's more recent push into the industry pose high risks. Both China and Russia have long used the private sector to support government-backed objectives, which could lead them to manipulate or exfiltrate data, disrupt operations, or even interfere with American vehicle control systems.

Recognizing these growing cybersecurity and national security threats, the Biden administration released a fact sheet in February 2024 directing the Department of Commerce to "investigate the

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

Cybersecurity Legislative Analysis Series

Background continued

potential national security risks from connected vehicles that incorporate technology from countries of concern, including China, and consider regulations to address those risks." This direction builds upon prior regulatory efforts, including President Donald J. Trump's EO 13873 from 2019, which declared a national emergency concerning the ICTS supply chain and allowed for additional scrutiny and restrictions on foreign-sourced technology to safeguard U.S. national security. Together, these executive actions lay the foundation for stronger regulation of critical technologies.

Furthering the regulatory objectives and principles established by these actions, the BIS issued an advance notice of proposed rulemaking (ANPRM) in March 2024, seeking public comment on how to secure and minimize national security risks posed by ICTS used in connected vehicles. The BIS received 57 comments from original equipment manufacturers, component suppliers, nonprofit organizations, individuals, and two foreign governments. Stakeholder comments were pivotal in shaping the draft rule, reflecting consensus on the cybersecurity risks in connected vehicles and the need for stronger security measures. However, concerns emerged about balancing these measures with economic realities—particularly global supply chain dependencies and competitive pressures.

The BIS revised the draft rule to incorporate stakeholder feedback, prioritizing mitigation of the most critical cybersecurity risks while addressing economic concerns. For example, the current draft of the proposed rule provides a delayed implementation timeline to accommodate industry stakeholders who need substantial lead time to identify new suppliers or source from alternative suppliers. Moreover, the BIS deliberately chose to exclude other technological systems highlighted in its initial ANPRM—such as vehicle operating systems, battery management systems, and ADS—unless they have VCS components and hardware. In doing so, the proposed rule targets the technological systems that most directly facilitate the transmission of data to and from the vehicle.

Submissions are currently under review. If adopted as written, the finalized regulation would take effect 60 days after publication in the Federal Register, representing a significant step toward securing connected vehicle technologies and safeguarding U.S. national security.

Key Takeaways

- The "cyber positive" rating reflects the proposed rule's targeted approach: Ban high-risk ICTS components in connected vehicles, enhance supply chain security, and offer a phased timeline with tailored exemptions to mitigate economic disruptions while preserving U.S. national security.
- The proposed rule establishes an adaptable framework to curtail adversarial influence in the connected vehicle market, securing U.S. technologies and data while fostering a more resilient and trustworthy ICTS supply chain.
- Early regulatory action could disrupt China's efforts to dominate the global connected vehicle market, reducing dependencies that pose military and diplomatic risks and making it easier for U.S. allies to isolate or impose effective sanctions on China during geopolitical tensions.

Cybersecurity Analysis

FACTORS	ANALYSIS
Access provisions	The use of VCS hardware and ADS software components designed, developed, manufactured, or supplied by entities linked to foreign threats—particularly China or Russia—is prohibited. This restriction aims to limit access to U.S. connected vehicle technology and data that could be vulnerable to exploitation by nation-state threat actors.
Applicability	This proposed rule applies to any company importing VCS hardware and ADS software into the United States, as well as manufacturers and suppliers of connected vehicles that use these components. The scope includes third-party suppliers and other entities involved in the production, sale, or integration of these technologies into connected vehicles, ensuring comprehensive coverage of the global ICTS supply chain and addressing any potential overlaps that could inadvertently introduce cybersecurity vulnerabilities within the U.S. market.
Impact on cyber actions	By banning the use of VCS hardware and ADS software components from foreign adversaries, the proposed rule mitigates potential national security risks, such as espionage, sabotage, or cyberattacks. These risks could otherwise allow threat actors to exploit vulnerabilities in connected vehicle systems, leading to significant data exfiltration or even physical manipulation of vehicle functions. In addition to preventing access to sensitive systems, the proposed rule strengthens supply chain security by ensuring that critical components are sourced only from trusted, non-adversarial countries. This reduces the likelihood of compromised hardware or software being introduced into U.S. vehicles, safeguarding against potential backdoors or vulnerabilities that could be exploited for nefarious purposes, including remote hijacking of vehicles.
Business impact	Auto manufacturers in the United States could face increased manufacturing costs that may be passed on to consumers, raising the price of connected vehicles in the U.S. market. Shifting to new supply chains and complying with the proposed rule's requirements to exclude targeted foreign hardware and software could introduce compromises in certain ICTS components, potentially affecting vehicle performance, consumer safety, and overall product quality. Paired with global market pressures, these challenges may divert resources from innovation in connected and autonomous vehicle technologies, increase operational costs, and reduce incentives for high-cost research and development. Public comments on the March 2024 ANPRM emphasized that compliance burdens could hinder the U.S. auto industry's ability to maintain leadership in emerging automotive technologies.

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

Cybersecurity Legislative Analysis Series

FACTORS	ANALYSIS
Data privacy and security	The ban on VCS hardware and ADS software systems from these countries aims to prevent the potential interception, extraction, or manipulation of sensitive data—such as driver biometric data, vehicle data, navigation data, and critical infrastructure data—from being transmitted between connected vehicles and external networks. If effectively implemented and enforced, this proposed rule would strengthen data privacy protections for U.S. consumers and businesses, safeguarding vehicle diagnostic data, user information, and critical national infrastructure from potential foreign interference.
Rulemaking or update mechanisms	The public comment period concluded on Oct. 28, 2024, and the BIS is now reviewing and considering the submissions received. Following this review, the BIS may issue the final rule, which—if adopted as currently written—would take effect 60 days after its publication in the Federal Register. The BIS will continue providing guidance on the application and approval process for general and specific authorizations as well as advisory opinions that allow manufacturers and importers to seek clarification on compliance and authorization issues as needed.
Exemptions, exceptions, and defenses	• **VCS hardware importers** are exempt if they meet one or more of the following criteria: – The hardware units are not associated with a vehicle model year – The hardware is imported before Jan. 1, 2029 – The hardware is associated with a vehicle model year prior to 2030 – The hardware is imported as a part of a connected vehicle manufactured prior to model year 2030 • **Connected vehicle manufacturers** are exempt if the vehicle incorporating covered software was manufactured prior to model year 2027. • **Connected vehicle manufacturers associated with China or Russia** are exempt if the vehicle incorporating VCS hardware or covered software was manufactured before model year 2027.
Enforcement mechanisms	As delegated by EO 13873, the enforcement of this proposed rule is primarily grounded in the International Emergency Economic Powers Act. Under this authority, the BIS has the power to regulate and prohibit transactions involving foreign adversaries, particularly those from China and Russia, when they pose unacceptable risks to U.S. national security.
Other notes	The BIS proposes to include a mechanism for the bureau to issue advisory opinions to connected vehicle manufacturers, VCS hardware importers, and other interested parties seeking greater clarity around how to comply with the proposed rule. The BIS is not proposing to adopt cybersecurity standards and best practices as part of this rule; however, it may consider the scope and nature of adoption on a case-by-case basis as part of the specific authorization process. The BIS has also left open the possibility of future expansions to cover additional foreign countries of concern or ICTS technologies, representing a continuous effort by the U.S. government to safeguard national security by proactively adapting restrictions on foreign access to sensitive technologies and data based on risk levels.