Connected Vehicle Security Act of 2026

Connected Vehicles are able to collect massive amounts of data. Equipped with internet access and wireless technologies, they can track your location, driving patterns, personal information, and even map the infrastructure around you. If Chinese companies like BYD and Geely control this technology inside of vehicles within the U.S., that data can freely flow back to Beijing. Under China's national intelligence laws, this sensitive information can be exploited for espionage, surveillance, or worse: remote takeover of vehicles on American roads. They represent a national security threat to the American people.

Cheap Chinese autos look like a bargain for working families, but they're far from it. Heavily subsidized by the Chinese Communist Party, they are flooding foreign markets in Mexico, Europe, and elsewhere, crushing local industries with their artificially low prices. The U.S., and the Midwest in particular, has felt the effects of unfair Chinese competition for decades – and we must prevent it from spreading to the millions of American workers in the auto industry.

The answer is simple: we need to protect the U.S. auto market from Chinese connected vehicles, along with the software and hardware that support them. The *Connected Vehicle Security Act* delivers a clear solution: no Chinese vehicles or their connected components on American soil.

Background

- *Ban on Foreign Adversary Vehicles, Hardware, and Software:* Prohibits the importation, integration, manufacture, sale, and resale of connected vehicles, software, and hardware linked to China or other foreign adversaries, including those from joint ventures or entities under their control.
- *Empowers the Department of Commerce*: Authorizes the Secretary to identify and block high-risk vehicle technologies, components, and transactions that threaten U.S. economic or national security, with transparent waiver authorities to ensure Congressional oversight.
- *Enforcement Mechanisms*: Establishes compliance procedures, binding rulings, and civil penalties to ensure prohibited items are kept out of the U.S. market.
- *Phased Implementation*: Connected vehicle and software restrictions take effect in 2027, with hardware restrictions in 2030, giving U.S. industry time to secure domestic supply, in line with the Bureau of Industry and Security (BIS) Connected Vehicle Rule.

Please contact Rob_VanKirk@moreno.senate.gov for additional information or to be added as a co-sponsor.