



State of West Virginia  
Office of the Attorney General  
*Patrick Morrissey*  
Attorney General

October 28, 2024

The Honorable Elizabeth L.D. Cannon  
Executive Director  
Office of Information and Communications Technology and Services  
Bureau of Industry and Security  
U.S. Department of Commerce  
14th St. and Constitution Ave., NW  
Washington, DC 20230

Submitted via <https://www.regulations.gov>

**Re: Comments on the Notice of Proposed Rulemaking entitled “Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles,” 89 Fed. Reg. 79,088 (Sept. 26, 2024) (Docket No. 240919-0245)**

Dear Executive Director Cannon:

We appreciate the chance to comment on the Notice of Proposed Rulemaking from the Department of Commerce and its Bureau of Industry and Security entitled “Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles,” 89 Fed. Reg. 79,088 (Sept. 26, 2024).

Earlier this year, many of us applauded the Bureau’s decision to scrutinize connected vehicles from certain foreign adversaries—particularly China. As we explained in that comment (which we’ve attached here), connected vehicles present unique opportunities for exploitation by malicious actors. China, working through its state-owned or state-controlled enterprises, is positioned to exploit those opportunities for its own hostile ends. *See, e.g.*, Alliance for American Manufacturing, No. BIS-2024-0005-0047 (Apr. 30, 2024), <https://tinyurl.com/bdzyasa6> (“[Connected vehicles] afford foreign adversaries with unprecedented opportunities to compromise U.S. economic and national security.”). Especially considering how the present

administration is pushing for more connected, electric vehicles on the road, the risk of harm will only grow without immediate action.

Since we filed our comment, nothing has assuaged our initial concerns. Other comments submitted in response to the Bureau's advance notice of proposed rulemaking confirmed what we said: connected vehicles have many vulnerabilities, and those vulnerabilities can and will be used exploited by unfriendly actors. *See, e.g.*, Comment Letter of Ford Motor Co., No. BIS-2024-0005-0047 (Apr. 30, 2024), <https://tinyurl.com/2wvzz2f6> (describing “systems that could genuinely pose the highest potential national security risks, which includes systems that are software-enabled, engage in bidirectional data exchange, have an external internet connection, and have an element of control by a foreign adversary without oversight or compensating controls by a domestic automaker”); Comment Letter of Alliance for Automotive Innovation, No. BIS-2024-0005-0047 (Apr. 30, 2024), <https://tinyurl.com/22djyfa5> (acknowledging that “the transmission of vehicle data to a Foreign Adversary may pose a national security risk” and “the ability of a Foreign Adversary to perpetuate an attack” through “a wireless access point or a wired connection to issue control commands to vehicle systems” “creates additional national security risk”); Comment Letter of Volkswagen Group of America, Inc., No. BIS-2024-0005-0047 (Apr. 30, 2024), <https://tinyurl.com/3zm8knzd> (“[I]t is possible that a foreign adversary could attempt to use a wireless access point or a wired connection to vehicle systems to perpetuate ... an attack.”).

Original equipment manufacturers and suppliers note that they are already taking measures to address at least some of these concerns. Although we applaud their efforts, we see insufficient assurance that manufacturers and suppliers *based in hostile countries* are doing the same. Nor are we confident that efforts by domestic and other friendly manufacturers and suppliers can entirely mitigate the dangers presented by those based elsewhere. So while we're sympathetic to automakers' concerns about upsetting established supply chains, we also think accepting the status quo is not an option.

Again, consider the harm that connected vehicles could cause by:

- Providing access to sensitive data stored on vehicle systems (such as Chinese automaker GWM's T-box hardware), including data gathered from phones and other IoT devices;
- Permitting foreign actors to monitor in-cabin activities through recording and monitoring devices in the vehicle;
- Enabling hostile persons to spy, monitor, and surveil through sensors and cameras outside the vehicle;
- Creating exploitable access points to connected WiFi and other networks;
- Threatening critical infrastructure through coordinated attacks (as by “overloading” a power grid through electric vehicle charging systems);

- Gathering geolocation and behavioral data in sensitive environments, such as military bases; and
- Allowing remote controllers to seize control of vehicle systems (particularly in autonomous vehicles) and cause injury to passengers, bystanders, or physical facilities.

See Lukas Mäder, *Why Chinese-made Cars Could Threaten U.S. National Security*, NZZ (Oct. 4, 2024), <https://tinyurl.com/4nu9cf93>.

Indeed, even *domestic* manufacturers have used data gathered from connected vehicles in ways that have attracted concern—and litigation. See, e.g., Compl. ¶ 1, *Texas v. General Motors LLC*, No. 24-08-12392 (Tex. Dist. Ct. Aug. 13, 2024) (accusing GM LLC and OnStar of “deceptively” inducing consumers to “unwittingly opt[] into an all-seeing surveillance system”); see also Lars Daniel, *Your Car Is Spying On You And Sharing Data With Third Parties*, FORBES (Oct. 11, 2024, 1:03 PM), <https://tinyurl.com/39syf9kp>. If domestic entities are exploiting connected vehicles for commercial purposes, then it’s not hard to imagine a foreign adversary doing the same to serve broader geopolitical aims.

China itself recognizes these risks. Just a few days ago, “China’s state security ministry said that a foreign company had been found to have illegally conducted geographic mapping activities in the country under the guise of autonomous driving research.” *China says unidentified foreign company conducted illegal mapping services*, REUTERS (Oct. 16, 2024, 8:00 AM), <https://tinyurl.com/ex5425rm>. If China is keeping a lookout for these risks, then we should be, too.

We prefer free markets. And we disdain unnecessary federal government involvement. But the stakes here are too great to ignore, and the multinational nature of these problems requires national-level attention. No wonder this issue is producing a bipartisan consensus. See Theo Burman, *Trump Says He Will Ban Chinese-Made Self-Driving Cars as Elon Musk Launches Cybercab*, NEWSWEEK (Oct. 11, 2024, 1:29 PM), <https://tinyurl.com/5n6zhfdu> (President Trump calling Chinese autonomous vehicles “concerning”); Ireland Owens, *US Lawmakers Attempt To Enlist Newly-Inaugurated Mexican Leader In Battle Against Possible Threats From Chinese Cars*, DAILY CALLER (Oct. 1, 2024, 4:49 PM), <https://tinyurl.com/yp4rt46m> (“Nearly two dozen Democrats from Congress, ... wrote a letter to [Mexican President Claudia] Sheinbaum urging her to look into concerns over internet-connected vehicles produced in Mexico by Chinese automakers.”).

We encourage you to finalize the Proposed Rule as soon as possible. It would be a much-needed step toward ameliorating this threat. In the end, our States’ citizens should not have to worry about whether the vehicles that ferry them to and from work, home, or school are really a weapon from abroad.

Sincerely,



Patrick Morrisey  
West Virginia Attorney General



Steve Marshall  
Alabama Attorney General



Treg Taylor  
Alaska Attorney General



Tim Griffin  
Arkansas Attorney General



Ashley Moody  
Florida Attorney General



Raúl Labrador  
Idaho Attorney General



Todd Rokita  
Indiana Attorney General



Brenna Bird  
Iowa Attorney General



Kris Kobach  
Kansas Attorney General



Russell Coleman  
Kentucky Attorney General



Liz Murrill  
Louisiana Attorney General



Lynn Fitch  
Mississippi Attorney General



Andrew Bailey  
Missouri Attorney General



Austin Knudsen  
Montana Attorney General



Mike Hilgers  
Nebraska Attorney General



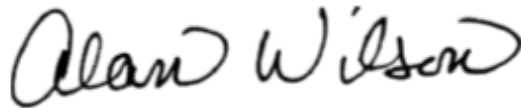
John M. Formella  
New Hampshire Attorney General



Drew Wrigley  
North Dakota Attorney General



Gentner F. Drummond  
Oklahoma Attorney General



Alan Wilson  
South Carolina Attorney General



Marty Jackley  
South Dakota Attorney General



Jonathan Skrmetti  
Tennessee Attorney General and Reporter



Sean D. Reyes  
Utah Attorney General



Jason Miyares  
Virginia Attorney General