SQUIRE PATTON BOGGS

Continuing Series of National Security Actions, White House Announces Review of Connected Vehicles

Teeing Up Potential Action Against Chinese Car Imports

March 2024

On February 29, 2024, US President Joe Biden announced that his administration will investigate the national security risks posed by "connected vehicles from countries of concern." The president's statement underscores the key role that advanced technologies and data play in today's cars and other vehicles, and the national security risks presented therein.

The administration is particularly concerned about the amount of sensitive data that can be collected on drivers, passengers and US infrastructure by connected cars through cameras, sensors, personal cell phones and other connected car data systems that could be used for espionage, remote control of the vehicle, and other exploitative actions. As part of the president's announcement, the US Department of Commerce (Commerce) initiated a rulemaking to investigate whether it should issue regulations on transactions involving connected vehicles and information and communications technology and services (ICTS) – notably, the first action taken by the administration under Executive Order (EO) 13873, "Securing the Information and Communications Technology and Services Supply Chain." New regulations and restrictions could have broad implications for joint ventures and cross-border investments, fleet tracking, digital management systems and countless other aspects of automotive manufacturing and operation in the 21st century.

Parallel and separately, future regulations could also serve as one of the first major actions against the perceived threats posed by Chinese electric vehicle (EV) imports into the US. US stakeholders representing a wide range of industries – including automakers, unions, parts suppliers and many more – are increasingly warning of the risks that Chinese EV imports pose to the domestic and international competitiveness of American-made cars, as well as to national security. While this action is being taken in response to perceived national security threats, future regulations could also support US industry against an anticipated onslaught of Chinese EV imports.

Following the president's announcement, Commerce released an advance notice of proposed rulemaking (ANPRM) titled, "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles." The ANPRM alleges that "the PRC has engaged in a pattern of hacking and cyber intrusion that demonstrates the PRC's intent to compromise and exploit US ICTS supply chains and critical infrastructure, threatening U.S. national security."

It directs the Bureau of Industry and Security (BIS) "to investigate national security risks posed by connected vehicles from countries of concern," according to a White House fact sheet. Through the ANPRM, Commerce seeks to solicit information from the industry and the public on the nature of the risks posed by connected vehicles using ICTS from China and other "countries of concern" that (1) collect US user data on drivers and passengers; (2) record US roads and infrastructure; and (3) can be controlled or disabled remotely. The ANPRM outlines that BIS is reviewing proposals to prohibit ICTS transactions in relation to connected vehicle technology produced by entities "owned by, controlled by or subject to the jurisdiction" of countries of concern. Public comments are due by April 30, 2024.

Specifically, BIS seeks public comments on the following issues: (1) its definition of connected vehicles; (2) categories of ICTS integral to connected vehicles; (3) market leaders in connected vehicle ICTS products; (4) geographic locations where ICTS hardware and software for connected vehicles are developed, including the extent to which these supply chains are influenced by countries of concern; (5) geographic locations where US data collected by connected vehicles is stored; (6) ICTS products for connected vehicles solely produced by entities in countries of concern; (7) ICTS hardware and software for which countries of concern hold a competitive advantage over US producers; (8) the degree to which automotive software connected to global navigation satellite systems are produced by entities from countries of concern; (9) the damage ICTS supply chain disruptions would cause to US automakers; (10) the extent to which US automakers can procure alternative ICTS products; (11) the relationships between US automakers and ICTS suppliers; (12) the risks arising from ICTS systems being integrated into connected vehicles; and (13) the extent to which ICTS components from countries of concern are present in US critical infrastructure sectors.

BIS further seeks comments on the risks of Chinese ICTS products, and those from other countries of concern, including (1) the scope of data collection capabilities in connected vehicles; (2) automakers' remote access to connected vehicles; (3) cybersecurity concerns; (4) industry best practices to secure the interconnection between vehicles and charging infrastructure; (5) supplementing cybersecurity standards across the connected vehicle supply chains; (6) the automotive software development cycle; (7) the relationship between connected vehicles and cloud service providers; (8) verification processes for automotive software procured from third-party suppliers; (9) the extent to which vendor software is verified by automakers; and (10) automakers' vendor vetting practices.

Finally, BIS requests input on regulating automotive software, including (1) other ICTS products integral to connected vehicles; (2) ICTS products that present the greatest risk to safety or security; and (3) regulatory considerations for automated driving systems. In addition, BIS solicits feedback on its cited authorizations and the economic impact of any resulting rule.

Any final rule is expected to target ICTS products originating from China regardless of their final assembly location to prevent circumvention through third-party countries – one of several envisioned actions targeting the near-shoring of Chinese EV manufacturing in countries that share a free trade agreement with the US. In January 2024, Commerce Secretary Gina Raimondo identified Chinese EVs as a national security risk, noting the "huge amount of information about the driver, the location of the vehicle and the surroundings of the vehicle," collected by these vehicles. In addition, the ANPRM coincides with two other high-profile Biden administration actions related to data security: a February 28 EO on data privacy and security, and a February 21 EO targeting maritime security and Chinese involvement in US port infrastructure.

Congress has also highlighted the potential threat of Chinese connected vehicles and related components in recent months. In November 2023, the House Energy and Commerce Committee and the House Select Committee on the Chinese Communist Party launched a joint investigation into 10 Chinese automated vehicle companies over their data management practices. Similarly, the fiscal year 2024 National Defense Authorization Act directed the Department of Defense to report to Congress "on the national security threats associated with Chinese autonomous ground vehicles operating in the US."

The connected vehicle ICTS ANPRM is the latest in a series of actions by the Biden administration intended to "de-risk" US supply chains and combat Chinese cyber- and espionage threats. The Federal Communications Commission has pursued actions over the past several years to secure US telecommunications networks, including revocations of operating authorizations previously granted to carriers allegedly under Chinese control. As China's automotive production capability has grown rapidly in recent years, the Biden administration has increasingly become concerned that Chinese products could undercut US suppliers and expose sensitive US data. Observers should watch closely for any reaction from Beijing to the announcement, especially given the deep ties some US automakers have to China, both as a market for products and as a key element of their supply chains. In the interim, the ANPRM will serve as the foundation for future regulatory action and provide significant opportunity for stakeholders to make real-world impacts on the form and substance of final regulations. These restrictions are coming, but the question is how administration officials balance national security and economic protections against the realities of global trade.

Contacts

David Stewart
Principal, Washington DC
T +1 202 457 6054
E david.stewart@squirepb.com

Kate Kim Tuma
Partner, Los Angeles
T +1 213 689 5147
E kate.tuma@squirepb.com

Bridget McGovern
Partner, Washington DC
T +1 202 457 6104
E bridget.mcgovern@squirepb.com

Everett Eissenstat
Partner, Washington DC
T +1 202 457 6535
E everett.eissenstat@squirepb.com

Ludmilla L. Kasulke
Partner, Washington DC
T +1 202 457 5125
E ludmilla.kasulke@squirepb.com

Robert B. Kelly
Partner, Washington DC
T +1 202 626 6216
E robert.kelly@squirepb.com

Pablo E. Carrillo
Of Counsel, Washington DC
T +1 202 457 6415
E pablo.carrillo@squirepb.com

Scott A. Warren
Partner, Tokyo
T +81 3 5774 1800
E scott.warren@squirepb.com

Daniel F. Roules
Partner, Shanghai
T +86 21 6103 6309
E daniel.roules@squirepb.com