King & Spalding

Client Alert

International Trade

MARCH 06, 2024

For more information, contact:

Jamieson Greer
+1 202 626 5509
jgreer@kslaw.com

Jarno Vanto
+1 212 556 2210
jvanto@kslaw.com

J. Philip Ludvigson
+1 202 626 9267
pludvigson@kslaw.com

Christine E. Savage
+1 202 626 5541
csavage@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Ave., NW
Suite 900
Washington, D.C. 20006
Tel. +1 202 737 0500

Biden Administration Initiates Inquiry Targeting "Connected Vehicles," With Chinese Electric Vehicles and Supply Chain as Clear Target For Regulation

The Biden Administration announced on February 29, 2024, that it is commencing an inquiry into whether the involvement of "foreign adversaries" in the information and communications technology and services ("ICTS") supply chain for "connected vehicles" ("CVs") poses a national security risk to the United States.[i] Chinese vehicles – particularly electric vehicles ("EVs") – are the express target of this inquiry.[ii] In commencing this inquiry, President Biden asserted that "China is determined to dominate the future of the auto market, including by using unfair practices. China's policies could flood our market with its vehicles, posing risks to our national security."[iii] The purpose of this initial inquiry is to identify "the technologies and market participants that may be most appropriate for regulation."[iv]

Trade in autos is the fourth largest sector accounting for global trade flows valued at well over $700 billion – not including the many electronic parts and components in the supply chain.[v] Thus, this inquiry and any resulting actions may realign global trade flows and have an enormous impact on companies in the automotive supply chain affected by U.S.-China cross-border operations, manufacturing, supply chains, investment, and data flows. Notably, the inquiry could affect operations in and inputs from third countries to the extent they involve Chinese companies or their foreign subsidiaries.

The broad legal authority used for this inquiry permits Commerce to implement a wide range of potential measures to address any identified

national security risk, at the level of individual transactions or an entire class of transactions. Such measures could include:

- monitoring, data collection, and reporting requirements;
- establishing lists of risky or prohibited suppliers or companies;
- extensive review and approval processes for transactions in the sector;
- outright prohibitions on the import of Chinese vehicles; or
- replacement of vehicle fleets used by the government or companies involved in critical infrastructure or other important sectors.

For companies in the sector that do not rely substantially on Chinese inputs for their business, this inquiry and any resulting measures may present an opportunity to gain a competitive advantage in the market due to their sourcing practices. For those companies whose business models depend on Chinese inputs or services, this inquiry and the potential risks associated with it must be carefully anticipated and managed. In either case, companies will have an opportunity to prepare and submit comments to the U.S. government to help shape this developing policy at the intersection of international trade and national security. Companies may be able to submit comments or portions thereof on a confidential basis. Any comments on this matter must be submitted to the U.S. Department of Commerce Bureau of Industry and Security ("BIS") by April 30, 2024.

U.S.-CHINA COMPETITION IN THE AUTOMOTIVE SECTOR

This inquiry should be understood as an expanding front in the U.S.-China competition on economic, technology, and security matters. In development strategies published in 2010 and 2015 – including the "Made in China 2025" strategy – the Chinese government announced its intent to dominate global markets in "new energy vehicles" and displace foreign automotive producers.[vi] For example, Chinese government policy documents for these plans outline efforts to develop "intelligent connected cars" and obtain "key systems to achieve bulk exports."[vii] In executing this strategy, the Chinese government has pursued forced technology transfer to obtain technologies in the automotive supply chain that are fundamental to producing vehicles, particularly EVs. Further, the Chinese government has provided major subsidies to domestic companies in the automotive supply chain, resulting in massive overcapacity in its automotive industry and the threat of flooding global markets with dumped and subsidized vehicles.[viii] On the U.S. side, a 25 percent tariff on Chinese vehicles and many auto parts has been in place since 2018 as a response to findings by the Office of the U.S. Trade Representative that the Chinese government engages in forced technology transfer, including with respect to the automotive industry. This investigation resulted in a cumulative 27.5 percent tariff on U.S. imports of Chinese vehicles and many auto parts that is still in place. Further, EV tax incentives in the Inflation Reduction Act exclude from eligibility vehicles made in China or that contain batteries with Chinese-origin raw materials or components.[ix]

Many government agencies and private sector entities have raised warnings about CVs as a vector for the collection or misuse of U.S. person data by foreign actors, particularly China. From allegations of surveillance equipment embedded in world leaders' vehicles to malware included in CVs or their components,[x] significant concerns about foreign exploitation of vulnerabilities and risk exposure have grown. The ICTS inquiry is a powerful tool the United States can use to identify and remediate these risks.

ICTS INQUIRY PROCESS

The U.S. Commerce Department ("Commerce") administers the ICTS supply chain review regime through the Office of ICTS and will conduct the inquiry into CVs. This review regime was established by Executive Order 13873 ("E.O. 13873") during the Trump Administration and was kept in place by the Biden Administration. E.O. 13873 is premised on a national emergency proclaimed by the President under the International Emergency Economic Powers Act. The Biden Administration has promulgated rules for the ICTS review process and hired substantial personnel to carry out the directives of E.O. 13873. Until now, Commerce has used the ICTS review mechanism only in a very narrow (and largely confidential) way.[xi]

In furtherance of the President's announcement of an inquiry, BIS issued an advance notice of proposed rulemaking ("ANPRM") seeking comment on the potential development of regulations to secure and safeguard the ICTS supply chain for connected vehicles ("CVs"). According to the ANPRM, Commerce is considering the regulation or control of CVs that may pose national security risks, particularly risks posed by CVs from China or Chinese companies. The ICTS regulations provide broad authority to Commerce to identify these risks, and the ANPRM provides substantial detail into its views on potential national security risks related to CVs. These include the extensive data collected by CVs, the connectivity of CVs, and the possible exploitation of such data by foreign adversaries for nefarious purposes. The ANPRM cites to risks such as launching cyberattacks on vehicles and vehicles fleets or on critical infrastructure to which CVs are connected. The notice cites to concerns regarding espionage, including through the forced disclosure of data by private parties subject to Chinese jurisdiction and involved in the ICTS supply chain.

Notably, the ICTS regime provides Commerce substantial discretion to determine which entities are considered to be controlled by or subject to the jurisdiction of a foreign adversary such as China. As a result, it is possible that Commerce could consider an entity located outside of China to be subject to regulation if that entity has a Chinese parent or is otherwise owned or controlled by such a party.

BIS is seeking input from industry and the broader public on a number of issues that will inform the possible establishment of transaction reviews involving ICTS items integral to CVs. Some of the primary issue areas where BIS is requesting information include:

- **The definition of "connected vehicle."** Commerce preliminarily defines a CV as "an automotive vehicle that integrates onboard networked hardware with automotive software systems to communicate via dedicated short-range communication, cellular telecommunications connectivity, satellite communication, or other wireless spectrum connectivity with any other network or device." This includes both personal and commercial vehicles, as well as those that are capable of "global navigation satellite system ("GNSS") communication for geolocation; communication with intelligent transportation systems; remote access or control; wireless software or firmware updates; or on-device roadside assistance." BIS has requested public comment on the scope of this definition and whether it should be modified.
- **An understanding of the U.S. ICTS supply chain for CVs.** BIS is seeking to collect information on the ICTS supply chain for CVs, including the hardware and software that are integral to CVs; the market leaders and suppliers at all tiers for these items and their components; the geographic location where such items are designed, developed, manufactured, or supplied; involvement of Chinese entities in the ICTS supply chain for CVs; and the geographic location of where data from CVs are transmitted, stored, or analyzed.

- **The role of persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries.** BIS has requested information regarding reliance on Chinese entities for ICTS items integral to CVs as well as any technological advantage such suppliers might have over U.S. and foreign competitors.
- **The effect of any disruption of ICTS items for CVs sourced from Chinese entities.** BIS is collecting information about the effects of disruption of sourcing ICTS items from Chinese entities, presumably to understand the potential impact of restrictions on such items for use in U.S. CVs. BIS is also seeking to understand whether there are alternative sources for these items.
- **The risks posed by aftermarket ICTS items used in CVs.** BIS is seeking to understand risks for ICTS equipment used with CVs after manufacture, "such as tracking devices, cameras, and wireless-enabled diagnostic interfaces." BIS is also considering whether such items should be considered "integral" to CVs.
- **The data collection and connectivity capabilities of ICTS items in CVs.** BIS highlights the vulnerabilities resulting from extensive data collection and the possibility of transmitting that data to third parties. BIS has requested information describing "the full scope of data collection capabilities in CVs," such as the use of sensors, biometrics, cameras, biometrics, video, and other systems to gather vehicle-level data and environmental-level data. BIS also wants to understand to what extent parties can control or authorize access to data collected from CVs.
- **Remote access or control of CVs.** BIS has requested information regarding the extent to which original equipment manufacturers ("OEMs") could exercise remote access or control over CVs they produced, including a description of the hardware and software that could permit such control.
- **Cybersecurity standards and practices.** The agency is seeking information regarding cybersecurity for the interconnection between CVs and charging infrastructure, such as a an EV's battery management system. BIS is particularly interested in specific programs or practices to enhance cybersecurity for CVs, such as end-to-end encryption, white hat programs and "bug bounties," and testing protocols.
- **The automotive software development cycle.** BIS has asked parties to comment on the process for developing automotive software, including whether OEMs develop software in-house or license it from third parties; the geographic location where such software is developed; security measures implemented during development; the role of any Chinese parties in the development cycles; and whether this development process extends to firmware incorporated into CV hardware.
- **The role of cloud services.** BIS has requested information regarding the role cloud services providers play with regarding to ICTS in CVs, such as their remote access capabilities and any shared responsibility for system security.
- **The extent of risk posed by ICTS items.** BIS is seeking comments regarding which ICTS items, including those not mentioned in the ANPRM, would pose a "material risk" if designed, developed, manufactured, or supplied by a Chinese entity. Of these, BIS would like to understand which pose the greatest risk to safety and security.
- **Economic impacts resulting from regulating ICTS items integral to CVs.** BIS is collecting information about any economic impacts that may result from potential regulation of ICTS items in CVs, including domestic and international effects. BIS is also interested in understanding which businesses and firms would be most affected

by regulations, including any anticompetitive impacts. BIS would like to know whether there are ways to mitigate any negative consequences from potential regulation of ICTS items for CVs.

- **Compliance requirements for ICTS regulation.** BIS has asked for comments on the compliance burden that will be associated with any regulation of ICTS items from foreign adversaries used in CVs, such as recordkeeping, due diligence, and other practices to monitor and comply with regulation involving Chinese entities in the ICTS supply chain.

In addition to seeking out detailed information on the ICTS supply chain for CVs and related risks, BIS has requested comments on how to handle any temporary authorizations for transactions involving ICTS items from Chinese entities:

- **The need for temporary authorizations for transactions with foreign adversary entities.** BIS has asked for information regarding whether temporary authorizations would be necessary or in the interest of the United States to avoid harmful supply chain disruptions or unintended consequences. BIS has also requested comments on the criteria the agency might use in assessing whether a temporary authorization is appropriate, including standards, best practices, or mitigation measures.
- **The review model for authorizations.** BIS is requesting public comment on the most effective way to consider and grant authorizations, such as the authorization processes used by BIS for export control authorizations or the Office of Foreign Assets Control sanctions program licenses.

This inquiry appears to be another major regulatory effort by the United States designed to identify and mitigate national security risks associated with China. The United States and China continue to manage their trade relationship through a variety of legislative initiatives, regulatory regimes, and agency practices. Companies involved in the automotive supply chain should closely monitor this inquiry and, where appropriate, contribute views and comments to the U.S. government to help shape the policy environment for automotive trade going forward.

[i] Statement from President Biden on Addressing National Security Risks to the U.S. Auto Industry, White House (Feb. 29, 2024), *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/29/statement-from-president-biden-on-addressing-national-security-risks-to-the-u-s-auto-industry/.

[ii] Other "foreign adversaries" include Cuba, Iran, North Korea, Russia, and the Maduro regime in Venezuela.

[iii] Statement from President Biden on Addressing National Security Risks to the U.S. Auto Industry, White House (Feb. 29, 2024), *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/29/statement-from-president-biden-on-addressing-national-security-risks-to-the-u-s-auto-industry/.

[iv] *Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles*, 89 Fed. Reg. 15066 (Dep't Commerce Mar. 1, 2024).

[v] *Cars*, Observatory of Economic Complexity, *available at* https://oec.world/en/profile/hs/cars.

[vi] *Made in China 2025: Global Ambitions Built On Local Protections*, U.S. Chamber of Commerce (2017) at 6-8, *available at* https://www.uschamber.com/assets/documents/final_made_in_china_2025_report_full.pdf; *State Council Decision on Accelerating the Development of Strategic Emerging Industries*, The State Council of the People's Republic of China, No. 32 (Oct. 10, 2010), *available at* https://www.lawinfochina.com/display.aspx?lib=law&id=8570.

[vii] *Made in China 2025*, The State Council of the People's Republic of China, *available at* https://english.www.gov.cn/2016special/madeinchina2025/.

[viii] *Findings of the Investigation Into China's Acts, Policies, and Practices Related To Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974*, Office of the United States Trade Representative (Mar. 22, 2018), at 29-32, *available at* https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

[ix] *See Section 30D Excluded Entities*, 88 Fed. Reg. 84098 (Treas. Dep't Dec. 4, 2023).

[x] *See, e.g.*, "Popular vehicle GPS tracker gives hackers admin privileges over SMS," BleepingComputer (July 19, 2022), *available at* https://www.bleepingcomputer.com/news/security/popular-vehicle-gps-tracker-gives-hackers-admin-privileges-over-sms/; *China tracked Rishi Sunak using device hidden in car, says ex-Tory leader*, The Independent (Aug. 7, 2023), *available at* https://www.independent.co.uk/news/uk/politics/rishi-sunak-china-spy-car-b2388890.html.

[xi] *See, e.g.,* "Exclusive: U.S. probes China's Huawei over equipment near missile silos," Reuters (July 21, 2022), *available at* https://www.reuters.com/world/us/exclusive-us-probes-chinas-huawei-over-equipment-near-missile-silos-2022-07-21/.