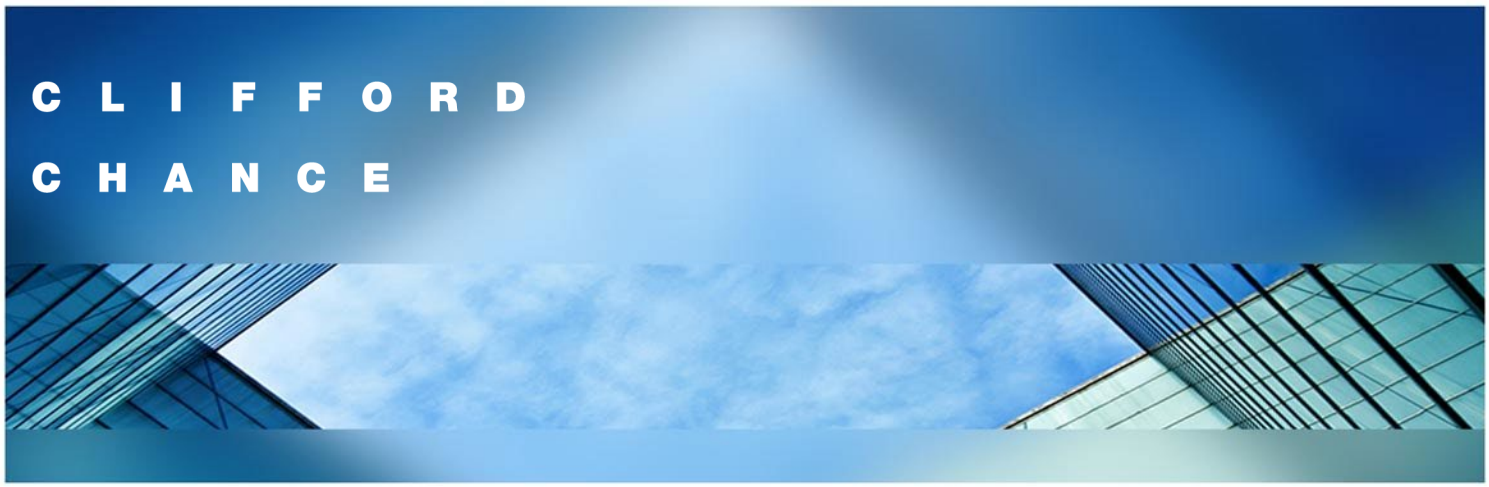

IMPACT OF US ICTS SUPPLY CHAIN FOCUS ON THE AUTOMOTIVE SECTOR

Foreign threats to the US information and communications technology and services (**ICTS**) supply chain constitute a national emergency. Executive Order 13873, titled "Securing the Information and Communications Technology and Services Supply Chain," issued on May 15, 2019 (**EO**), first declared the emergency and granted the Secretary of Commerce (**Secretary**) the authority to regulate ICTS transactions involving "foreign adversaries" that may pose undue or unacceptable risk to the United States or US persons. Following publication of an Interim Final Rule on January 19, 2021, the Department of Commerce (**Department**) implemented the EO in the Final Rule on December 6, 2024 (**Final Rule**). The Final Rule goes into effect on February 3, 2025.

WHAT ARE THE KEY UPDATES THE FINAL RULE INTRODUCES?

The Final Rule is designed to safeguard US national security by addressing risks posed by foreign adversaries who could exploit vulnerabilities in the ICTS supply chain. It authorizes the Secretary, in consultation with relevant agency heads, to review ICTS transactions. An "**ICTS transaction**" is "*any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download*." The Secretary assesses if a transaction constitutes a covered ICTS transaction and involves ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, and poses an undue or unacceptable risk. Here, "foreign adversaries" include People's Republic of China, Russia, Cuba, Iran, North Korea, and Venezuela. If such a risk exists, the Secretary can order mitigation or prohibit the transaction. Any entity, wherever located, engaging in a covered ICTS transaction, would be subject to the Final Rule.

The text of the Final Rule reflects significant comments from the industry, private trade groups and individuals, expands the rule's scope, and formalizes many procedures. Key aspects of the Final Rule include the following:

- **Scope of covered ICTS transactions.** The Final Rule retains a broad definition of covered ICTS transactions to address risks from foreign adversaries, focusing on ICTS pertaining to sensitive personal data, critical infrastructure, and critical and emerging technologies. It aligns definitions with the EO and National Security Memorandum 22, lists 16 critical sectors, and updates critical and emerging technologies to include 11 key categories, including artificial intelligence (AI), drones, and quantum computing. It removes numerical thresholds relating to processing of sensitive personal data, software use, and sales minimums because they "do not necessarily correlate with the risks presented." It simplifies the CFIUS exception to avoid duplicative reviews and applies retroactively to ICTS transactions initiated, pending, or completed on or after January 19, 2021.
- **Initial review of ICTS transactions; procedures for response and mitigation.** The Final Rule clarifies the procedure around how initial reviews can be initiated, outlines steps to determine whether a transaction is a "covered ICTS transaction," and refines criteria for evaluating the risks such a transaction poses. An initial review can lead to an initial determination of whether the transaction can be approved, can no longer proceed at all, or may require mitigation measures. The Final Rule also allows affected parties to respond to Initial Determinations with corrections or challenges to factual inaccuracies. It aims to enhance the response process by permitting a 30-day window to respond, with an option to extend for an additional 30-day period for good cause and requiring a 50-page limit for written responses. A Final Review will determine whether the transaction is approved, must cease, or requires further mitigation measures.
- **Interagency consultation.** The Final Rule clarifies procedure for interagency consultation processes. It requires notification to and comments from appropriate agency heads within 21 days for the first interagency notification. It mandates consultation with agency heads before issuing an Initial Determination, with a 21-day response period, and before issuing a Final Determination, with a 14-day response period.
- **Recordkeeping requirements.** The Final Rule requires the immediate retention of all records related to an ICTS transaction upon notification of review or of Initial Determination. Records must be kept for at least 10 years following the issuance of a Final Determination.
- **Penalties.** The Final Rule contains a list of activities that may lead to penalties. If a party engages in a prohibited activity, it may face civil penalties up to $250,000 per violation or twice the transaction amount, adjusted for inflation, and criminal penalties up to $1,000,000 or 20 years imprisonment, or both, for willful violations.

WHAT OTHER REGULATORY EFFORTS FOCUS ON SAFEGUARDING ICTS FOR NATIONAL SECURITY REASONS?

The above developments are part of a broader federal regulatory focus on safeguarding ICTS for national security reasons. Some examples of key initiatives include the following:

- On June 21, 2023, the Department published a final rule implementing Executive Order 14034, titled "Protecting Americans' Sensitive Data from Foreign Adversaries". The rule, more limited in scope than the IFR, created the term "connected software applications" and added specific factors for the Department to consider when reviewing ICTS transactions.
- On June 24, 2024, the Department brought an enforcement action against Kaspersky Lab Inc., prohibiting ICTS transactions supplied by a US subsidiary of this Russia-based cybersecurity company.
- In January 29, 2024, BIS issued a Proposed Rule, titled "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities". It addresses national security threats of foreign access to US Infrastructure as a Service (**IaaS**) resources, such as use of IaaS to develop AI tools to engage in cyberattacks. Among other requirements, it mandates that all US providers of US IaaS products and their foreign resellers maintain a customer identification program and report to the Department known instances of foreign persons training large AI models that could be used in malicious cyber enabled activity.
- On October 21, 2024, the US Department of Justice released a Notice of Proposed Rulemaking, titled "Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons". The notice addresses the national security threat posed by certain countries' access to and exploitation of US sensitive personal and government-related data by identifying a set of prohibited and restricted transactions involving those countries. See our analysis of this development here.
- On October 28, 2025, the US Department of the Treasury (**Treasury**) issued a final rule providing the regulations for the new "Outbound Investment Security Program". This rule implements the Executive Order 14105, titled "Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern". It requires US persons to notify the Treasury of certain direct or indirect transactions with covered foreign persons involving specified groups of sensitive technologies and products and prohibits US persons from engaging in other such transactions. The rule takes effect on January 2, 2025. See our analysis of this rule here.

WHAT ARE THE IMPACTS OF THE FINAL RULE ON THE AUTOMOTIVE SECTOR?

The automotive industry has embraced digital transformation, enabling connected vehicles to receive real-time traffic updates, remote diagnostics, over-the-air software updates, and communicate with other devices, with continuous rollouts of new features. Connected vehicles, which depend on seamless data exchange and integration with external networks, are particularly vulnerable to cyber threats. With the Final Rule taking effect in early 2025, manufacturers must ensure that all components, throughout their supply chain, from hardware to software, comply with the new security standards. In fact, anyone engaging in a covered ICTS transaction throughout the automotive, semiconductor, artificial intelligence,

quantum computing and potentially other sectors must prepare to comply with the updated requirements.

BUT THAT'S NOT ALL… OTHER ICTS-RELATED DEVELOPMENTS ARE ALSO IMPACTING THE AUTOMOTIVE SECTOR

Because automakers often work with global suppliers and technology firms, automakers will need to reassess these relationships to ensure compliance with security standards, particularly where such companies have a sufficient nexus to the PRC or Russia, as indicated by a recently issued Bureau of Industry and Security (**BIS**) Notice of Proposed Rulemaking (**NPRM**).

The NPRM, implemented under BIS's ICTS authority, would prohibit the import and sale of vehicles with certain Vehicle Connectivity Systems (**VCS**) and Automated Driving System (**ADS**) hardware or software that has a nexus to the PRC or Russia. The software prohibitions would take effect for Model Year 2027 and the hardware prohibitions would take effect for Model Year 2030, or January 1, 2029, for units with no model year. Additionally, the NPRM would prevent automakers with a nexus to the PRC or Russia from selling connected vehicles containing VCS hardware or software or ADS software in the United States, even if manufactured in the United States. Although not yet implemented in the regulations as a final rule, the NPRM reflects significant efforts by BIS to guard against cyber risk and national security threats in the automotive sector.

KEY TAKEAWAYS

Reevaluating supplier relationships will involve vetting third parties more rigorously, renegotiating contracts, and possibly seeking alternative sources for certain technologies. The Final Rule also underscores the importance of cybersecurity as a critical component of corporate governance in the automotive sector. Companies may need to invest in training and development to ensure that their workforce is equipped to handle the new security demands. This may involve hiring specialized personnel or working with external cybersecurity experts to enhance internal capabilities.

From a big picture perspective, we do not anticipate that the broader regulatory focus on securing ICTS for national security reasons will wane (including under the new incoming administration) and instead, initiatives mentioned above, and others will continue. Many of the supply chain regulations are based on the legal authority issued by President Trump during his first administration. Therefore, it is likely that the second Trump administration will continue to support these efforts.

Our team of trade, supply chain, compliance, technology and cybersecurity attorneys are monitoring these developments and assisting clients with risk-based and practical solutions given the evolving regulatory and geopolitical landscape.

CLIFFORD
CHANCE

CONTACTS

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Renée Latour
Partner

T +1 202 912 5509
E renee.latour
@cliffordchance.com

Michelle Williams
Partner

T +1 202 912 5011
E michelle.williams
@cliffordchance.com

Inna Jackson
Tech Knowledge & Innovation Attorney – Americas

T +1 212 878 3292
E inna.jackson
@cliffordchance.com

Nicolas Friedlich
Associate

T +1 202 912 5197
E nicolas.friedlich
@cliffordchance.com

Martina Kneifel
Associate

T +1 202 912 5066
E martina.kneifel
@cliffordchance.com

Curtis Sails III
Associate

T +1 202 912 5193
E curtis.sailsiii
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 2001 K Street NW, Washington, DC 20006-1001, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Riyadh* • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

*AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.