Published on *The National Law Review* https://natlawreview.com

Escalation of U.S. Crackdown on Chinese Technology and Telecoms: Emerging Issues

Article By:

Alan F. Enslen

Martin L. Stern

Julius H. Bodie

Stephen T. Sharbaugh

Executive Summary

In recent years, the U.S. has pursued a whole-of-government approach to target Chinese technology and service providers in furtherance of foreign policy and national security objectives. This includes the implementation of sweeping new export control initiatives, domestic restrictions on the use and procurement of Chinese telecommunications equipment and services, targeted economic and trade sanctions designations, heightened foreign direct investment scrutiny, and most recently outbound investment restrictions that seek to curtail investment in Chinese companies associated with certain sensitive and advanced technologies.

This alert summarizes key emerging issues in the U.S.-China regulatory space with respect to technology policy and provides insight into the evolving regulatory compliance obligations for U.S.

companies, investors, and government contractors. In particular, the Department of Commerce, Department of Treasury, and Federal Communications Commission have each implemented an array of new regulatory orders and directives that aim to combat and deter China's global technology influence in order to safeguard significant U.S. national security interests.

On August 9, 2023, President Biden issued a new Executive Order targeting outbound U.S. investments in Chinese technology companies, including those associated with sensitive national security-related technologies such as semiconductors and microelectronics, quantum information technologies, and certain artificial intelligence systems. While not expected to take full effect until 2024, these investment restrictions mark the most recent escalation of the U.S. government's crackdown on Chinese technology using a whole-of-government approach. Through a combination of evolving export control laws, economic and trade sanctions designations, government contracting prohibitions, investment regulations, and domestic telecom restrictions, the U.S. will continue to pursue multiple inter-agency efforts to deter China's global technology influence and protect significant domestic security interests.

Given the breadth of China-related technology policy initiatives that have been rolled out in recent years by the U.S. government, this alert is intended to provide a summary of key emerging issues in the U.S.-China regulatory space.

This includes cross-border initiatives such as:

- The newly announced outbound U.S. investment restrictions associated with Chinese technology companies (to be administered by the Departments of Treasury and

Commerce);
- The expansion of current U.S. export controls on semiconductor and advanced computing technology, and consideration of new export controls targeting advanced chips; and
- The increased use of restricted party lists and sanctions designations to target Chinese military, aerospace, defense, and technology companies.

Evolving domestic restrictions on Chinese telecommunications and technology companies have also been at the forefront of U.S. economic and national security policy, including:

- Federal Communications Commission ("FCC") national security restrictions on Chinese telecommunications companies, including via implementation of the Secure and Trusted Communications Networks Reimbursement Program;
- Government contracting prohibitions on the provision and use of certain covered Chinese telecommunications equipment and services, as well as Chinese semiconductor equipment; and
- Proposed federal legislation targeting Chinese telecommunications companies, military industrial efforts, and support for Chinese undersea cable projects.

In all likelihood, the technology cold war between Washington and Beijing is expected to continue, though as discussed below, there have been recent efforts to ease tensions between the two nations. Nonetheless, it will be critical for U.S. technology and telecommunications companies, government contractors, investors, and the like to actively monitor U.S. regulatory updates in connection with their respective compliance obligations—particularly as the U.S. government's enforcement posture has become

increasingly aggressive, focused, and robust. At the same time, companies might also consider the competitive implications of these initiatives in global markets where U.S. and Chinese technology and telecom companies compete.

I. Investment Restrictions and Export Controls

In recent years, U.S. export control regulations and foreign investment restrictions targeting China have been increasingly utilized for national security purposes. This includes the incremental expansion of foreign investment regulations administered by the Committee on Foreign Investment in the United States ("CFIUS"), as well as enhanced licensing requirements under the Export Administration Regulations ("EAR") with respect to the export of certain commodities and technology to China. Through a variety of Executive Orders and new legislation, the government continues to pursue multiple unprecedented regulatory strategies to target the rise of Chinese civil-military fusion policies, fortify domestic enforcement efforts, and further U.S. foreign policy and national security objectives.

A. Outbound Investment Restrictions – National Security Technologies in China

CFIUS is an interagency committee lead by the Department of the Treasury that has the authority to review, and potentially reject, certain types of foreign acquisitions and investments in U.S. businesses for their impact on national security. In recent years, CFIUS's jurisdiction has increased significantly in terms of the types of foreign investment that falls within its purview - including certain non-controlling investments involving U.S. businesses that deal with various aspects of critical technologies, critical infrastructure, and/or sensitive personal data. Chinese foreign

investment in particular has been met with substantial scrutiny by CFIUS in recent years. However, there has never been a parallel U.S. regulatory infrastructure that monitors or restricts *outbound* investment by U.S. parties.

Chinese foreign investment in particular has been met with substantial scrutiny by CFIUS in recent years. However, there has never been a parallel U.S. regulatory infrastructure that monitors or restricts *outbound* investment by U.S. parties.

In an Executive Order issued August 9, 2023, the Biden Administration announced the first steps of a proposed regulatory regime intended to restrict certain categories of outbound U.S. investment into China, specifically targeting certain advanced sensitive technologies. The Executive Order (E.O. 14105), along with a corresponding advance notice of proposed rulemaking ("ANPR") issued by the Department of Treasury, lays out newly proposed notice requirements and U.S. investment prohibitions involving Chinese entities engaged in the development and production of (i) semiconductor and microelectronics technologies,

(ii) quantum information technologies, and (iii) certain artificial intelligence systems.

Specifically, the outbound investment regulatory program would focus on certain categories of covered transactions, including the acquisition of equity interests (*e.g.*, via mergers and acquisitions, private equity, venture capital, and other arrangements), greenfield investments, joint ventures, and certain debt financing transactions that are convertible to equity. The restrictions would then apply to investments in Chinese entities that are engaged in activities related to the defined subsets of technologies and products. The ANPR seeks public comment on a range of related definitions and elements of the program, so it remains to be seen how the exact investment restrictions will be further defined and implemented. However, the program will be designed to include both (i) notifiable transaction activity (for those that involve technologies and products that "may contribute to the threat to the national security of the United States"), and (ii) expressly prohibited transaction activity (for those that involve technologies and products that "pose a particularly acute national security threat because of their potential to significantly advance the military, intelligence, surveillance, or cyber-enabled capabilities of countries of concern."). This particular Executive Order does not fully contemplate a "Reverse-CFIUS" program in that there are no review, approval, and safe-harbor components akin to a traditional CFIUS filing made in connection with foreign direct investment.

Regardless of the final outcomes of the Department of Treasury rulemaking process, the Executive Order marks a foundational and significant legal step to curtail U.S. investment activity in China, and stands to impact a wide range of U.S. companies and investors – including by imposing substantial regulatory compliance and due diligence obligations with respect to future China-related

investments by U.S. parties.

B. Semiconductor, Advanced Computing, and Chipmaking Export Controls

The U.S. investment restrictions described above build upon recent major developments with respect to U.S. export control regulations targeting China, as many of the technologies identified in that Executive Order were previously impacted by sweeping new export control regulations implemented by the Department of Commerce's Bureau of Industry and Security ("BIS") in October 2022.

The updated export controls seek to limit China's access to critical U.S. technologies, targeting advanced computing, integrated circuits, and semiconductor manufacturing items. The key amendments to the EAR from the October 2022 update include the following:

- New Export Control Classification Numbers ("ECCNs") on the EAR's Commerce Control List related to advanced computing integrated circuits and related products, as well as certain semiconductor manufacturing equipment;
- Expansion of end-use-based licensing requirements and controls on items intended for supercomputer and semiconductor manufacturing that target chip-making capabilities of Chinese fabricators;
- New limits on the availability of license exceptions for certain exports and reexports to China;
- Broader and more complex Foreign Direct Product Rules impacting transfers outside the U.S. of advanced computing and supercomputer items that are manufactured abroad; and

- Restrictions on the ability of U.S. persons to support the development or production of integrated circuits at certain semiconductor fabrication facilities located in China.

While the updated controls have only been fully implemented for less than a year, the impact on international supply chains has been profound. Major U.S. and Western suppliers of semiconductor manufacturing equipment have largely cut ties with China, and in 2023 the U.S. has successfully lobbied allies such as the Netherlands and Japan to adopt similar domestic legislation restricting chipmaking technology exports to China. In response, China has recently implemented its own licensing restrictions on the export of gallium and germanium, key elements used in producing chips and fiber optics that are largely produced in China.

Chinese influence on the global semiconductor industry has been and will continue to be in the crosshairs of U.S. regulators, and the combination of U.S. export controls and multilateral partnerships designed to enhance global restrictions deterring China's competitiveness in the semiconductor sector are critical components of those efforts.

At the same time, on August 28, 2023, the U.S. and China agreed to launch an export control enforcement information exchange, along with a new commercial issues working group to seek solutions on trade and investment issues and to advance U.S. commercial interests in China – indicating that additional initiatives are being pursued on both sides to ease recent tensions in the commercial and regulatory spaces.

C. Restricted Parties – BIS Entity List and Chinese Military-Industrial Complex Companies List

U.S. agencies have also greatly increased their use of restricted party designations in recent years to target the Chinese military-industrial complex and limit the outbound flow of U.S. technology to China. This includes Chinese entity designations on the Department of Commerce's BIS Entity List as well as under various economic sanctions programs administered by the Department of Treasury's Office of Foreign Assets Control ("OFAC").

BIS has utilized multiple export control tools at its disposal to restrict technology exports to certain Chinese entities, including amplified use of the BIS Entity List. BIS can designate a company on the Entity List if it determines they are involved in, or risk becoming involved in, activities contrary to the foreign policy and national security interests of the United States. When a foreign company is designated on the BIS Entity List, all exports, reexports, or in-country transfers of items subject to the EAR, including EAR99 items, are generally prohibited to the designated party without first obtaining a license from BIS. Over 600 Chinese entities are currently designated on the Entity List, including for contributing to China's military modernization efforts as well as those deemed to have participated or contributed to human rights abuses in China.

Over 600 Chinese entities are currently designated on the Entity List, including for contributing to China's military

modernization efforts as well as those deemed to have participated or contributed to human rights abuses in China.

OFAC has also actively targeted Chinese military and technology companies through its administration of U.S. economic sanctions programs, not only through the use of its Specially Designated Nationals and Blocked Persons List (”SDN List”), but also through the creation and implementation of the Non-SDN Chinese Military Industrial Complex List (“CMIC List”). The SDN List is the most restrictive OFAC financial sanctions tool, and if a party is designated on the SDN List, persons subject to U.S. jurisdiction are generally prohibited from entering into any type of business transaction with the targeted party anywhere in the world, and the foreign party is cut off from the U.S. financial system. The CMIC List is a less restrictive OFAC sanctions program that prohibits U.S. persons from investing in publicly-traded securities of designated Chinese entities. There are currently over 65 Chinese parties designated on the CMIC List.

ii. Domestic Telecom and Technology Restrictions

In addition to evolving restrictions on the outbound flow of U.S. investment and technology to China, the volume of domestic legislative and regulatory actions targeting Chinese technology utilized in the U.S. has also increased significantly. This includes (i) unprecedented FCC restrictions on Chinese telecommunications companies and equipment/service providers; (ii) federal

government contracting restrictions on the provision and use of equipment and services provided by Chinese telecommunications companies; and (iii) increased legislative efforts targeting Chinese telecom and technology companies.

A. FCC National Security Telecom Restrictions

Congress and the FCC in recent years have grown increasingly concerned about the national security implications posed by Chinese-owned telecommunications companies operating in the United States. For example, in March 2020, the Secure and Trusted Communications Networks Act ("Secure Networks Act") was enacted, which required the FCC to (i) create a list of "covered" telecommunications equipment and services deemed to pose a national security threat to the U.S.; and (ii) create the Secure and Trusted Communications Networks Reimbursement Program ("Reimbursement Program") to fund the replacement of certain covered equipment.

Pursuant to the Secure Networks Act, in March 2021 the FCC released a list of covered telecommunications equipment and services (the "Covered List"), which included telecommunications and video surveillance equipment and services from major Chinese telecom entities such as Huawei Technologies Company ("Huawei"), ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company. The FCC then further expanded the Covered List in March and September 2022, adding the information security products and services of AO Kaspersky Lab (a Russian entity), telecommunications services provided by China Telecom (Americas) Corp., and the international telecommunications services provided by China Mobile International USA Inc., China

Unicom (Americas) Operations Limited, and Pacific Network Corp., as well as its wholly-owned subsidiary ComNet (USA) LLC. The Secure Networks Act prohibits the use of FCC subsidies for the purchase, lease, or maintenance of equipment or services appearing on the Covered List.

In furtherance of these prohibitions, the FCC's Reimbursement Program was subsequently implemented (the so-called "rip and replace" program). The Reimbursement Program authorized federal reimbursement to eligible providers of advanced communication services with 10 million or fewer customers for the cost of removing, replacing, and destroying all Huawei and ZTE equipment and services from their networks. Approximately $1.9 billion was appropriated to carry out the Reimbursement Program, but government funding has been a point of contention – as the FCC has made clear to Congress that current funding for the rip and replace program has been insufficient, particularly for small and rural carriers. In July 2022, the FCC asserted that there was a $3.08 billion shortfall in Reimbursement Program funding, resulting in a pro-rata reimbursement factor allocating for only 39.5% of eligible costs demanded.

More recently, the FCC has used its authority under Section 214 of the Communications Act (which requires FCC authorization for the provision of international telecommunications services) to revoke the international Section 214 authorizations of certain Chinese telecom providers that were deemed to raise national security concerns. Specifically, the FCC recently revoked or denied the international Section 214 authorizations for Chinese entities such as China Mobile International (USA) Inc. (2019), China Telecom (Americas) Corp. (2021), and Pacific Network Corp. and its subsidiary ComNet (USA) LLC (2022). An interesting nuance in these revocations is that they apparently have not forced these

respective Chinese entities to exit the U.S. telecom market in toto. The revocation orders only apply to Section 214 authorizations needed for the provision of “common carrier” services, with at least one of the Chinese entities arguing to the FCC that a number of its services are not common carrier offerings requiring Section 214 authority. While not focused specifically on Chinese providers, in April 2020 an Executive Order was issued formalizing an Executive Branch committee called the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector (which had been informally known as “Team Telecom”). The Committee was tasked to weigh in at the FCC on applications for new license authorizations, as well as on the transfer (and in certain cases) revocation of existing authorizations, related to foreign ownership considerations - with the FCC later adopting specific procedures for such Executive Branch participation in its proceedings. The Team Telecom agencies actively participated in the Chinese entity Section 214 revocation proceedings noted above, and have also been quite active at the FCC on authorizations involving foreign ownership issues, with heightened scrutiny on Chinese ownership and influence.

Separate legislation titled the Secure Equipment Act subsequently took effect in November 2022, directing the FCC to adopt rules to clarify that the Commission will no longer review or approve equipment authorizations for equipment on the Covered List. FCC equipment authorization is required for the import and sale in the U.S. of virtually all electronics equipment, including both (i) “intentional” radiators of radio frequency signals that contain radio transmitters (*e.g.*, Bluetooth and Wi-Fi devices, mobile phones, and the range of radio equipment used by wireless carriers, broadcasters, and enterprise users), and (ii) “unintentional” radiators, such as digital devices and virtually all consumer electronics equipment. Those rules took effect on February 6,

2023, and prevent manufacturers on the Covered List (primarily Chinese manufacturers along with certain Russian companies) from obtaining the FCC equipment authorizations necessary to sell new or updated products in U.S. markets, essentially barring the covered equipment of these entities from the U.S. market. While the new rules do not prevent manufacturers on the Covered List from selling equipment that already has been authorized, the FCC has requested public comment on whether it should revoke all existing equipment authorizations for manufacturers on the Covered List. These public comments are currently under review by the FCC and any additional rules promulgated may become effective before year-end.

B. Government Contracting and Covered Telecommunications Equipment

Many of the entities addressed on the FCC Covered List were also included in the rollout of updated government contracting restrictions under the Federal Acquisition Regulation ("FAR") implemented in August 2020 pursuant to Section 889 of the 2019 National Defense Authorization Act ("NDAA"). At a high level, Section 889 prohibits the federal government and government contractors from procuring or using certain "covered telecommunication equipment or services" that are produced or provided by Huawei, ZTE, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (and their subsidiaries or affiliates) as a "substantial or essential component of any system, or as critical technology as part of any system." Government contractors are now required to certify under the FAR whether they use covered telecommunications equipment or services as part of their annual representations in the System for Award Management. Between

the FCC Covered List restrictions and 2019 NDAA Section 889 government contracting requirements, it is clear that the U.S. is willing to use every legislative and regulatory tool at its disposal to combat perceived national security threats posed by Chinese telecommunications companies operating in the United States and the equipment and services they provide.

Between the FCC Covered List restrictions and 2019 NDAA Section 889 government contracting requirements, it is clear that the U.S. is willing to use every legislative and regulatory tool at its disposal to combat perceived national security threats posed by Chinese telecommunications companies operating in the United States and the equipment and services they provide.

Section 889 has recently been further expanded in the 2023 NDAA's Section 5949, which introduced new prohibitions on U.S.

federal agencies from procuring or contracting with entities to obtain covered semiconductor products or services from certain Chinese entities (including Semiconductor Manufacturing International Corporation, ChangXin Memory Technologies, and Yangtze Memory Technologies). While these restrictions will not go into effect until 5 years after the enactment of the 2023 NDAA, they can be seen as another key example of U.S. efforts to limit Chinese influence on the global semiconductor industry discussed elsewhere in this alert.

C. Evolving Legislation

Numerous pieces of pending domestic legislation have been introduced that seek to build on and expand the regulatory measures discussed herein to target Chinese technology and telecommunications companies, including the following.

- The bipartisan Undersea Cable Control Act passed in the House of Representatives in March 2023, which seeks to prevent China from accessing U.S.-origin goods and technologies capable of supporting undersea cable projects. The Act would direct the Department of Commerce to examine whether an additional array of export controls should be placed on goods, software, and technologies capable of supporting Chinese undersea cable projects. The bill would likely result in an expanded list of items on the EAR subject to a license requirement for export to China, as well as provide additional authority for Commerce to designate Chinese companies associated with undersea cable projects as restricted parties – which would further restrict such companies' ability to acquire U.S.-origin technology without a license approval in place.

- Bipartisan federal legislation targeting U.S. government procurement and use of Chinese-manufactured drones has gained momentum in recent years, including recent bills such as the American Security Drone Act in the Senate and the Countering CCP Drones Act in the House. In addition, several state legislatures have also jumped on the bandwagon with enacted and proposed legislation that generally seeks to bar particular state agencies or local governments from the use or purchase of drones from specific Chinese manufacturers or that are of Chinese origin.

- 2024 National Defense Authorization Act provisions are currently undergoing negotiations in the House and Senate, including a variety of measures targeting China (*e.g.*, expanded annual assessments of China's economic and technological capabilities, reviews and reports on China benefitting from U.S. taxpayer-funded research, modification of public reporting on Chinese military companies operating in the U.S., notification and reporting requirements associated with China's cooperation with Russia, additional procurement prohibitions involving Chinese military companies, *etc*.).

National Law Review, Volume XIII, Number 317