SHEARMAN & STERLING

M&A WATCH

August 13, 2018

NEW CFIUS LAW MOVES TO PROTECT EMERGING TECHNOLOGIES AND PERSONAL INFORMATION, TAKES AIM AT CHINESE INVESTMENT

On August 13, 2018, President Trump signed into law legislation that will sharpen the rules governing U.S. national security reviews by the Committee on Foreign Investment in the United States (CFIUS).[1] The final legislation will intensify scrutiny of foreign investments in U.S. critical infrastructure and critical technology companies and investments by Chinese companies, although some of the more draconian measures included in the original bill have been stripped. Most noticeable among the changes in the final legislation is a retreat from an attempt to extend CFIUS jurisdiction to outbound investments such as joint ventures located abroad. The legislation instead relies on U.S. export control laws to reach a variety of transactions that fall short of acquisitions or significant investments, in an attempt to limit the transfer of U.S. technology to certain foreign countries, especially China.

In many ways, the final legislation gives CFIUS more authority to accomplish what it already has been doing—focusing on technology sectors, China, access to personal information, and investments in companies in proximity to sensitive U.S. Government facilities. Among the more important changes to U.S. law are the following:

[1] The CFIUS legislation, called the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), was integrated into the Defense Authorization Act of 2019, which was signed by the President. The Defense Authorization Act of 2019 also integrated The Export Control Reform Act of 2018. Both sections are cited as "the legislation" in this article.

ADDRESSING OUTBOUND INVESTMENT THROUGH EXPORT CONTROLS

The original bills in both Houses of Congress included a controversial provision that would have extended CFIUS jurisdiction to certain outbound investments, including joint ventures when they include the "contribution by a United States critical technology company of both intellectual property and associated support to a foreign person." A range of U.S. companies lobbied against that provision. As a result, the final legislation instead addresses this issue through U.S. export controls, focusing in part on emerging and foundational technologies that are essential to national security. The legislation, which includes reauthorization of the Export Administration Regulations (EAR), requires the Secretary of Commerce to establish appropriate export controls regarding such technologies that at a minimum require licenses for exporting emerging and foundational technologies to a country "subject to an embargo, including an arms embargo, imposed by the United States." That provision is clearly aimed at China, which has been subject to a U.S. arms embargo dating back to 1989, and also would apply to Russia. The legislation instructs the President to create an interagency process to identify emerging and foundational technologies that "are essential to the national security of the United States" and are not specifically listed as critical technologies elsewhere in the CFIUS legislation. In what could signal a more sweeping crackdown on technology transfer to China, the legislation also instructs the Trump Administration to conduct a review of license requirements for exports, re-exports, or in-country transfers of items to the same list of embargoed countries.

While moving away from asserting extraterritorial jurisdiction, it is clear that Congress wants to have an impact on the transfer of technology and intellectual property in certain sectors and to certain countries. The legislation gives the Administration broad latitude in identifying emerging and foundational technologies. While it will take some time for the U.S. Commerce Department, which administers the EAR, to go through the process of making any changes to existing practice, those changes could affect a wide range of transactions. Congress also tasks the Administration with reviewing the interagency export license review process for deciding whether to classify technology or products as dual-use under the EAR or as munitions under the International Traffic in Arms Regulations administered by the U.S. State Department.

It will be important for U.S. and foreign companies entering joint ventures or similar business arrangements to consider all export control implications, including the likelihood of classification changes, before closing a transaction.

U.S. CRITICAL INFRASTRUCTURE AND CRITICAL TECHNOLOGY COMPANIES

Most investments in technologies and infrastructure that arguably have a connection to national security could be subject to a new jurisdictional analysis. The final legislation continues to focus extensively on foreign investments in U.S. critical technologies and critical infrastructure companies. It extends, with some exceptions for passive investments, CFIUS jurisdiction to all investments by a foreign person in any unaffiliated U.S. critical technology or critical infrastructure company, and in companies that maintain or collect certain personal data of U.S. citizens, regardless of whether the foreign person can control the U.S. business. As under current law, the new legislation continues to define critical technologies very specifically to include items on the U.S. Munitions List, nuclear technology and similarly sensitive products and technology, but also expands this definition to include "emerging and foundational technologies." While the jurisdictional analysis under the new law continues, as before, to focus on whether the foreign person could make important decisions for the U.S. business, it also eliminates the control analysis for all critical infrastructure and critical technology investments that are not passive. This does not mean that all

such non-passive investments must be notified to CFIUS, but it does mean that CFIUS has authority to reach those investments.

CHINA

The new law clearly focuses on Chinese investment, although somewhat more subtly than in earlier versions in Congress. In an obvious reference to the "Made in China 2025" program, designed to increase China's technological self-sufficiency, the legislation urges CFIUS to consider whether a transaction involves "a country of special concern" that has declared the "strategic goal of acquiring a type of critical technology or critical infrastructure that would affect United States leadership in areas related to national security." While the final legislation does not include a specific definition of "countries of special concern," as was included in earlier versions, the original author of the Senate bill has made it clear that the provision was designed to include China. Again focused on China, Congress suggests that CFIUS also consider the "potential national security-related effects of the cumulative control of, or pattern of recent transactions involving, any one type of critical infrastructure, energy asset, critical material, or critical technology by a foreign government or foreign person"—mirroring and expanding the type of policies that have sought to limit China's acquisition of U.S. semiconductor assets under both the Obama and Trump administrations.

The final legislation also directs the U.S. Commerce Department to send to Congress a biennial report on Chinese direct investment in the United States. Congress also recommends that the President reach out to U.S. allies to create their own national security review processes to facilitate coordination of national security threats, which is another provision with potential consequences for China.

This does not mean that no Chinese investments will be approved by CFIUS, but it does mean that Chinese investors will have to look carefully at the sector in which they are investing, and may have to compromise on the extent to which they acquire governance in such investments and consider structures that include U.S. persons as general partners, as discussed below. Investments in critical and emerging technologies will be especially difficult, and Chinese acquisition of U.S. technology could certainly be affected by changes to U.S. export control classifications.

REAL ESTATE TRANSACTIONS

The final legislation retains, with limited exceptions, provisions that would make certain real estate transactions subject to CFIUS jurisdiction, including those involving property located at U.S. ports or those in close proximity to U.S. military installations or sensitive U.S. Government facilities when such proximity could expose national security activities there.

This is another example by which the new law extends CFIUS jurisdiction without a control analysis. Again, CFIUS was already headed in this direction, having at least twice stopped Chinese investments in businesses located near sensitive U.S. Government facilities. Parties to transactions involving real property assets spread across a wide swath of the United States, such as wind farms, apartment complexes, oil and gas assets and retail chains, should as part of due diligence investigate the locations of each of those assets to check for proximity to sensitive U.S. facilities. Certain investors may have to divest any interest in properties located in sensitive locations. The provision does not apply to sale or lease of single housing units or those in urbanized areas as defined by the legislation.

PERSONAL INFORMATION AND CYBER SECURITY

The final legislation expresses the Sense of Congress that the factors to be considered by CFIUS in making a national security determination should be expanded to include the extent to which the covered transaction is likely to expose identifiable information, genetic information, or other sensitive data of United States citizens to foreign investors. Another consideration is whether the covered transaction is likely to have the effect of creating any new cybersecurity vulnerabilities in the United States or exacerbating existing cybersecurity vulnerabilities. It also extends CFIUS jurisdiction to investments in U.S. businesses that maintain or collect sensitive personal data of United States citizens that may be exploited in a manner that threatens national security.

In a clear reference to Russia, Congress recommends that CFIUS consider whether a transaction "is likely to result in a foreign government gaining a significant new capability to engage in malicious cyber-enabled activities against the United States, including such activities designed to affect the outcome of any election for Federal office."

Parties involved in foreign investments in U.S. cloud-computing companies or companies that have access to consumer, health or other personal information of U.S. citizens must consider the CFIUS implications of such investments, which along with emerging and foundational technologies could be the next intense focus of the committee.

PASSIVE INVESTMENTS

Although CFIUS has extraordinary discretion under U.S. law, one bright line has been the regulatory "safe harbor" for ownership interests of 10 percent or less voting interest in a U.S. business as long as the interest is otherwise passive. The new law avoids any definition of passive investment defined by a lower equity limit. It does, however, list those governance rights that will automatically give CFIUS jurisdiction over foreign investments in U.S. critical infrastructure and critical technologies companies and those that collect personal data of U.S. citizens. These include investments through which the foreign investor has access to material, non-public information; has board membership or observer rights; or has any governance beyond voting its shares on issues involving sensitive personal data of U.S. citizens or issues relating to critical technologies or critical infrastructure. Presumably, non-controlling foreign investments in critical infrastructure and technologies that do not include these rights could escape CFIUS jurisdiction. The legislation also specifies a limited jurisdictional exception in such cases for foreign persons making investments as limited partners in investment funds managed exclusively by a U.S. general partner, where the general partner makes all investment decisions, and cannot be removed by the limited partners.

These changes will further limit those situations in which foreign investments are beyond the reach of CFIUS. Businesses should note, however, that foreign investments in many sectors and from private companies from most countries will still be subject to traditional control and national security analyses.

INVESTMENTS INVOLVING FOREIGN GOVERNMENTS

The final legislation requires, for the first time, mandatory short-form CFIUS filings containing basic information for all acquisitions of U.S. critical infrastructure or critical technology companies by foreign companies with substantial foreign-government ownership. CFIUS can require that the parties to such a transaction later submit a full CFIUS notice. The term "substantial" will be further defined through

regulation, although the new law provides that investments in a U.S. business that represent less than 10 percent equity will not be considered substantial.

FILING AND TIMING CHANGES

The legislation permits, but does not require, parties to other types of covered transactions to submit the type of short-form notice mentioned above instead of making a full CFIUS filing. In response to the short-form filing, CFIUS must within 30 days respond by either requesting a full CFIUS notice, telling the parties CFIUS has completed all action under the short-form rules, or indicating that it does not have enough information to do so. This could ease the burden for parties in relatively innocuous transactions.

The legislation requires parties to a covered transaction to include a copy of any partnership agreements, integration agreements, or other side agreements relating to the transaction.

The legislation also changes the time frame for the initial CFIUS review from 30 to 45 days and permits one 15-day extension of the second-stage 45-day CFIUS investigation under extraordinary circumstances. The legislation also requires CFIUS to comment on draft CFIUS notices within 10 days when the parties to that notice stipulate that the investment or acquisition is a covered transaction. This extends from 90 to 120 days the maximum amount of time from date of filing to a presidential decision—a 45-day review; a 45-day investigation; a 15-day extension; and a 15-day presidential decision-making period. The legislation also authorizes CFIUS to send a recommendation to the President at any point during this formal process.

The legislation, for the first time, provides for the potential imposition of substantial fees for companies engaged in a CFIUS review. The fees, which will subsequently be set by regulation, cannot under the new law exceed the lesser of 1 percent of the value of the transaction or $300,000. The legislation also provides various mechanisms to ensure that CFIUS is adequately funded.

INDUSTRIAL POLICY

An earlier version of the House bill included provisions that would have required CFIUS to consider the impact of a transaction on U.S. employment levels and skill retention. While the final legislation does not include this, it does, however, take surprising steps in the direction of industrial policy, with numerous references to the relationship between national security reviews, export controls and U.S. manufacturing and technological leadership. The Trump Administration has clearly made economic impact a national security consideration in the context of investigations on imports of steel, aluminum, autos, and auto parts. Congress is of several minds on this issue, however. Some in Congress are proposing legislative change to narrow the definition of national security in this context, while others are proposing Congressional oversight over this growing trend and still others are proposing to take no action at all.

EFFECTIVE DATE

Some of the new provisions will go into effect on the date of enactment, including those related to side contracts, timing of CFIUS reviews and investigations, authority to suspend pending transactions, and the definitions of critical infrastructure and critical technologies, among others. As such, they would apply to all pending transactions. Other parts of the legislation, including the new short-form declarations, will become effective later, after new regulations have been completed.

CONCLUSION

It has been 11 years since Congress last passed CFIUS legislation. That 2007 law—the Foreign Investment and National Security Act—was a response to the kind of potential physical terrorist threats that seemed imminent in the wake of the World Trade Center bombings. What followed was a focus by CFIUS on critical infrastructure such as energy and telecommunications assets, as CFIUS again adjusted to new perceived threats. As noted at the outset of this article, this latest evolution of U.S. national security reviews represents a codification of a direction in which CFIUS was already headed, with a focus on cyber threats, the acquisition of critical, foundational and emerging technologies, personal information, and businesses in sensitive U.S. locations. The legislation also follows on the heels of a sharply protectionist turn in U.S. international trade policy in another indication of how the United States at this point plans to deal with the impact of globalization. The scope of the changes in the new law will be further revealed when CFIUS and, in the case of export controls, the U.S. Commerce Department, complete the regulatory process implementing the legislation. In the meantime, investors must be cognizant of the impact of the new legislation, including future regulations, on the deals they are negotiating and carefully analyze whether they should elect to file with CFIUS.

ROBERT LARUSSA
Counsel, Litigation
+1 202 508 8180
rlarussa@shearman.com

LISA RAISNER
Head of Government Relations
+1 202 508 8049
lraisner@Shearman.com

GEORGE CASEY
Global Co-Managing Partner
Head of Global M&A
+1 212 848 8787
gcasey@shearman.com

SCOTT PETEPIECE
Head of Americas M&A
+1 212 848 8576
spetepiece@shearman.com

RICHARD FISCHETTI
Partner, M&A
+1 212 848 5179
rfischetti@shearman.com