CARTER/LEDYARD

client advisory

AUTHOR:

Raphael S. Grunfeld / Partner
D: 212-238-8653
grunfeld@clm.com

THE EXPANDING SCOPE OF CFIUS'S JURISDICTION AND MANDATORY REPORTING

INTRODUCTION

Since its establishment by executive order by President Ford in 1975, the Committee on Foreign Investments in the United States, popularly referred to as "CFIUS," has monitored national security reviews of investments in or acquisitions of U.S. companies by non-U.S. persons or businesses and foreign government-controlled persons, purchasing U.S. assets perceived to be critical to the national security of the U.S.

For more than a decade after its establishment, CFIUS monitored foreign investments but had no enforcement capabilities. In 1988, in response to rising concerns over the effects of foreign direct investment on U.S. national security, Congress amended the Defense Production Act of 1950. This "Exon-Florio Amendment" authorized the President to examine and block transactions resulting in foreign "control" (subsequently broadly defined) of any U.S. business when such a transaction could threaten national security. The President then delegated to CFIUS the task of reviewing such transactions.

Over the years, the identity of the countries and the types of assets that CFIUS worries about have changed.

Since 2007, the primary concern has been about the acquisition of and access to technology by foreign entities, especially the Peoples Republic of China. Over time, Historically, CFIUS did not have the authority to review investments in U.S. real estate or to review non-controlling foreign investments in U.S. businesses that give the non-U.S. investor certain governance rights or access to sensitive information.

The increasing use of Chinese joint ventures into which U.S.-origin technology was transferred and the concern that transactions were being structured to circumvent CFIUS, prompted calls for expanding CFIUS's review powers.

FIRRMA AND THE FINAL REGULATIONS

Accordingly, on August 12, 2018, President Trump signed into law the Foreign Investment Risk Review Modernization Act of 2018, known as "FIRRMA" which radically enhanced the powers of CFIUS to review foreign investments in U.S. businesses.

On January 13, 2020, the U.S. Department of the Treasury issued final regulations, effective as of February 13, 2020, that implemented FIRRMA and significantly expanded the authority of CFIUS to conduct national security reviews of foreign investments in U.S. businesses.

On September 15, 2020, the U.S. Department of Treasury published additional final regulations, regarding mandatory notifications required for foreign investors in certain U.S. companies involved in U.S. Critical Technologies.

These regulations introduce three principal changes to the old CFIUS regime.

First, the regulations expand the jurisdiction of CFIUS to review minority, non-passive, non-controlling investments in U.S. businesses developing or producing Critical Technologies, owning or operating U.S. Critical Infrastructure assets, and possessing or collecting sensitive personal data of U.S. citizens, irrespective of the percentage of voting interest acquired.

Second, the regulations mandate CFIUS filings for foreign investments in certain U.S. businesses producing or developing certain Critical Technologies for which a license would be required to export such technology to the foreign buyer or any of its owners and for transactions in which a foreign government-controlled entity acquires control of certain U.S. businesses.

Lastly, the regulations significantly broaden CFIUS's jurisdiction by providing it with authority to review foreign acquisitions of certain U.S. real estate transactions.

The final regulations permanently exempt certain investors from Australia and Canada, and temporarily exempt certain investors from Great Britain and New Zealand from the mandatory filing requirements and from CFIUS's expanded authority to review non-controlling minority investments and acquisitions of certain U.S. real estate interests.

These countries are the only states exempted under the regulations, although the Treasury Department indicated that it may consider adding other foreign states in the future.

To qualify for the exemptions, investors must demonstrate substantial ties to these countries and accept certain restrictions on the nationalities of the individuals serving on their boards of directors and the nationality of some of their equity holders.

EXPANSION OF CFIUS JURISDICTION TO MINORITY, NON-CONTROLLING INVESTMENTS IN CRITICAL TECHNOLOGY, CRITICAL INFRASTRUCTURE AND DATA-INTENSIVE US BUSINESSES

Prior to enactment of FIRRMA, CFIUS's jurisdictional authority was limited to reviewing transactions that resulted in foreign "control" of a U.S. business.

The regulations broadly define "control" to include the power to determine important matters affecting a U.S. business. Thus, for example, the purchase by a non-U.S. purchaser of 7% of a U.S. business with rights to terminate significant contracts or to appoint or dismiss officers, would be a control acquisition subject to CFIUS review, regardless of the small percentage purchased.

As a result of FIRRMA and the final regulations, CFIUS now has the authority to review investments that would not result in control of a U.S. business if two conditions are met.

First, the non-controlling foreign investment must be made in a U.S. business operating in one of three security sensitive business sectors.

Second, the investment must provide the foreign investor with specified rights regarding the U.S. business.

The final regulations extend CFIUS's jurisdiction and powers of review to any non-controlling foreign investment in a U.S. business producing or developing critical **T**echnology, owning or operating critical **I**nfrastructure assets or maintaining or collecting sensitive personal **D**ata of U.S. citizens. The final rules define any such U.S. business as a "TID U.S. Business," (the word TID corresponds to the initial capital letters of the words Technology, Infrastructure and Data.)

For a "non-control investment" to be subject to CFIUS review, the investment must be made in a company that qualifies as a TID U.S. Business and that provides the foreign investor with **one** of the following rights: (i) the ability to access any material non-public technical information in the possession of the TID U.S. Business; (ii) the right to nominate a member or observer to the board of directors of the TID U.S. Business; or (iii) any involvement, other than through voting of shares, in the substantive decision-making of the TID U.S. Business regarding the use of sensitive personal data of U.S. citizens, the operation of U.S. critical infrastructure or the development or release of U.S. Critical Technologies.

It is important to note that, under the final regulations, reporting the transactions to CFIUS will remain voluntary for most non-control investments (except as noted below), providing the transaction parties with the discretion to seek CFIUS review and clearance of a particular investment.

In determining whether to file for CFIUS review of a non-control investment, the parties to the transaction should closely review, among other things, whether the U.S. business is a TID U.S. Business or is similar to a TID U.S. Business, the country of origin of the foreign investor (to see whether the country and investor benefit from certain exemptions from CFIUS described below) and the rights provided to the investor under the investment.

In the event transaction parties decide to seek CFIUS review of a non-control investment, the final regulations allow them to file either the traditional CFIUS joint voluntary notice or, alternatively, a short-form declaration regarding the investment. Declarations are shorter form filings on which CFIUS must act within a shorter time period of 30 days.

THREE CATEGORIES OF TID U.S. BUSINESSES

As mentioned, FIRRMA extended CFIUS's jurisdiction to allow it to review minority, non-passive, non-controlling investments in U.S. businesses that: (i) produce or develop Critical Technologies; (ii) own or operate Critical Infrastructure; or(iii) maintain and collect sensitive personal Data of U.S. citizens.

Critical Technology Businesses

The regulations define a TID U.S. Business as any U.S. company that "produces, designs, tests, manufactures, fabricates, or develops one or more Critical Technologies."

The regulations define "Critical Technologies" as any that are (i) controlled under the International Traffic in Arms Regulations, (ii) included on the Commerce Control List of the Export Administration Regulations, (iii) subject to nuclear-related controls administered by the Nuclear Regulatory Commission and Department of Energy, (iv) select agents or toxins under U.S. regulation or (v) designated as "emerging" and "foundational" technologies pursuant to The Export Control Reform Act of 2018.

What are "emerging" and "foundational" technologies for the purpose of determining whether a business is a TID U.S. Business over which CFIUS has jurisdiction with respect to a non-control investment?

Under the September 2020 Treasury regulations, "emerging" and "foundational" technologies are technologies that would require a license or some other authorization from one of the four main U.S. export control regimes to export such technology to the buyer or its parents in its chain of ownership.

In other words, in looking to see whether CFIUS has jurisdiction to review a non-control investment in a company engaged in a given technology, CFIUS checks if the Department of Commerce has

added that particular technology to its Commerce Control List of technologies for which an export license is required to export such technology to the jurisdiction of the investor or any entity in its chain of ownership. If the particular technology appears on the Commerce Control List, it is deemed to be a Critical Technology and the transaction, which transfers such technology to a foreign non-control investor, is subject to CFIUS review, and as we shall see, also to mandatory CFIUS filing.

The way the Department of Commerce, after participating in an interagency process, adds a particular technology to the Commerce Control List, is by assigning it what is called an Export Control Classification Number ("ECCN") and publishing the addition in the Federal Register. The ECCN is an alpha-numeric code (e.g., 3A981) that describes the item and indicates its licensing requirements, including which destination countries require the exporter to apply for an export license.

Typically, the technologies that the Commerce Department adds to the Commerce Control List are dual purpose technologies that can be used for peaceful purposes or for purposes that threaten national security.

Thus, for example, on October 5, 2021, the Bureau of Industry and Security of the Department of Commerce published a rule updating the Commerce Control List to include software that is capable of designing and building functional genetic elements from digital sequence data, because this software could be exploited for biological weapons purposes. The software is listed under a new given ECCN number 2D352 (where "2" denotes materials processing and "D" denotes software) and therefore requires a license for chemical and biological weapons and anti-terrorism reasons, when it is exported to the destinations indicated in the Commerce Control List under this new ECCN number. The software was added to the Commerce Control List even though it was not designed for biological weapons purposes and, even though the company that developed it was unaware that it could be used in a biological warfare context.

The Department of Commerce has been slow to add emerging and foundational technologies to the Commerce Control List, making it more difficult for parties to a transaction to know whether the transaction is one over which CFIUS has jurisdiction, or one for which mandatory reporting to CFIUS is required. In a recent executive order, the Biden administration announced that it intends to further update the Commerce Control List to include additional items of emerging and foundational technology.

In addition to the Commerce Control List, the executive order requires the Office of Science and Technology Policy ("OSTP") to periodically publish a list of technology sectors that, in its assessment, are fundamental to U.S. technological leadership in areas relevant to national security.

The Office of Science and Technology Policy list foreshadows and is a good guide as to what may ultimately get included in the Commerce Control List when it is updated by publication in the Federal Register.

Accordingly, if a technology is included in a current version of the Office of Science and Technology Policy List, one may want to err on the side of caution and assume it will appear on the Commerce Control List and treat the transaction as if it were subject to CFIUS review and possible mandatory reporting requirements.

Critical Infrastructure Businesses

While CFIUS has reviewed control acquisitions of critical infrastructure assets for many years, FIRRMA directed CFIUS to identify a specific subset of critical infrastructure assets for purposes of its newfound authority to review minority, non-controlling investments in U.S. businesses owning or operating such assets. The final regulations fulfill this legislative mandate by identifying in Exhibit A to the final regulations, 28 categories of critical infrastructure assets.

The list of infrastructure assets includes, among others, certain internet protocol networks, internet exchange points, submarine cable systems, electric generation and transmission assets, oil refineries and pipelines, LNG terminals, exchanges registered under the Securities Exchange Act and air and maritime ports and public water systems.

It is important to note that this narrow list of critical infrastructure assets is relevant only for purposes of the non-controlling investment analysis. CFIUS will continue to operate under a much broader definition of critical infrastructure for purposes of its analysis of controlling acquisitions of U.S. businesses owning or operating such assets. For purposes of control transactions, critical infrastructure is more generally defined as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security.

Under the final regulations relating to non-control investments, only U.S. businesses that perform specified functions with respect to the listed infrastructure assets qualify as TID U.S. Businesses. These functions generally involve owning, operating or producing such assets.

For example, the final regulations list an “interstate natural gas pipeline with an outside diameter of 20 or more inches” as one of the categories of critical infrastructure assets. The rules further require that a U.S. business “own or operate” such a pipeline for it to qualify as a TID U.S. Business. By contrast, an entity that only repairs or services such a pipeline is not a TID U.S. Business under the final regulations.

Data-intensive Businesses

FIRRMA identified any U.S. business that "maintains or collects sensitive personal data of United States citizens that may be exploited in a manner that threatens national security" as the third category of businesses relevant for non-control investment jurisdiction.

The final regulations limit the definition of sensitive personal data to "identifiable data," which is data in 10 specific categories that can be used to distinguish or trace an individual's identity, including, among others, genetic information, health-related data, geo-collection data, biometric enrollment data and state or federal identification data.

A U.S. business that maintains or collects these categories of data will only be considered to have sensitive personal data if it (i) targets or tailors products or services to certain national security-focused agencies or military departments of the U.S. government or their employees, (ii) maintains or collects data on greater than one million individuals at any point over a 12-month period, or (iii) has a "demonstrated business objective" of maintaining or collecting such data on greater than one million individuals and such data is an integral part of the U.S. business's products or services.

NEW CFIUS NATIONAL SECURITY CONCERNS OUTSIDE OF THE DEFENSE AND MILITARY CONTEXT

As a result of FIRRMA, the influence of the Biden Administration and the recently issued first CFIUS executive order, the following additional factors are looked at by CFIUS when reviewing a transaction, and accordingly, should be considered by the parties to an investment in, or acquisition of, a U.S. Business when determining whether or not to notify CFIUS of a transaction before its completion, where no mandatory filing is required:

- A given transaction's effect on the resilience of critical supply chains that may have national security implications, including those outside of the defense and military industries. In assessing a transaction's impact on the supply chain, CFIUS will consider alternative suppliers for the product or service and concentration of ownership or control by a foreign person in a given supply chain will be closely scrutinized.

- A given transaction's effect on U.S. technological leadership in areas affecting U.S. national security including, but not limited to, microelectronics, artificial intelligence, biomanufacturing, quantum computing, advanced clean technologies, and climate adaption technologies. In addition, U.S. technological leadership in any industry can be considered a matter of national security.

- Industry investment trends, meaning that the transaction can be of interest to CFIUS if other acquisitions in the same industries by unrelated foreign acquirers, concentrate one

industry in foreign hands. This gives CFIUS authority to look beyond the four corners of a specific transaction to consider broader investment trends in the industry which may not be apparent to the parties. When viewed in isolation, a single investment may appear to pose only a limited threat to national security, but when viewed in the context of a series of acquisitions in the same or similar related U.S. Business, the threat is greater.

- Cybersecurity where one of the reasons for the purchase is lax cybersecurity controls at the target, which gives the foreign acquirer access to sensitive information. CFIUS will also look at the foreign buyer's own cybersecurity safety and practices.
- Sensitive personal data where the foreign acquirer can de-anonymize the data.
- The foreign purchaser's ties to third parties including foreign governments.
- Protection of new technology innovation by U.S. universities.

In addition, although CFIUS has jurisdiction to review a control transaction involving any U.S. Business, whether or not it is a TID U.S. Business, it should be remembered that CFIUS has a heightened interest in TID U.S. Businesses so that serious consideration should be given to voluntarily reporting a control transaction involving a business engaged in operations similar to a TID U.S. Business.

If the transaction at hand is a non-control transaction, then CFIUS only has jurisdiction to review it if the target is a TID U.S. Business.

MANDATORY CFIUS FILING FOR CERTAIN ACQUISITIONS AND INVESTMENTS

Another expansion of CFIUS's scope under FIRRMA is the imposition of mandatory filings in the following two situations.

- The first is for any transaction in which there is an acquisition of a "substantial interest" in a TID U.S. Business by a foreign person in whom a foreign government also has a "substantial interest."

  For purposes of determining whether a foreign person has a "substantial interest" in a TID U.S. Business, the term means an indirect or direct voting interest of 25 percent or more by the foreign person in the TID U.S. Business.

  For purposes of determining whether a foreign government has a "substantial interest" in a foreign person investing in a TID U.S. Business, the term means a voting interest in that foreign person (whether direct or indirect) of 49 percent or more held by the foreign government.

- The second is where a foreign investor makes a control acquisition of, or a non-control investment with certain governance or information access rights, in a TID U.S. Business that produces, designs, tests, manufactures or develops one or more Critical Technologies for which a license or some other authorization would be required from one of the four main U.S. export control regimes, if such technology would be exported to the foreign buyer or any of its parents in its chain of ownership.

The definition of "Critical Technology" for the purpose of triggering a mandatory CFIUS filing is narrower than the definition of "Critical Technology" for the purpose of determining whether CFIUS has jurisdiction to review a non-control investment and is based on the technology's export control status.

A mandatory filing must be made not later than 30 days before closing.

The four main U.S. export control regimes that regulate export licenses are:

1) the Department of Commerce under the Export Administration Regulations;

2) the Department of State under the U.S. International Traffic in Arms Regulations;

3) the Department of Energy with respect to atomic energy; or

4) the Nuclear Regulatory Commission with respect to` the export of nuclear material.

Most commonly, the central question is whether one or more technologies that the target is involved in are on the Department of Commerce Control List.

In order to determine whether the export of such technology requires an export license and whether a mandatory filing is required, one must know where the principal place of business of each foreign parent in the chain of ownership is located and whether an export license would be required to export such technology to such location.

Usually, the most relevant Export Control Regime is the Department of Commerce under the Export Administration Regulations. The Department of Commerce, Bureau of Industry and Security publishes and periodically updates a list of products that require an export license for export to any given country ("Commerce Control List).

In order to determine whether a given technology requires an export license for export to a certain location, one must identify all of the technologies the target designs, develops, produces or tests, whether for sale or for internal use, regardless of whether the target exports these items, and then check to see if any such technology (which could include goods, services, substances, materials, software programs or items of technical know-how) is listed under an Export Control Classification

Number ("ECCN #") on the Commerce Control List, for export to the particular location in question.

If such technology is so listed, absent a specific exemption from the requirements of an export license, it would require an export license for export to the buyer or to any of the buyer's parents in the chain of ownership, and accordingly a mandatory filing would be required.

By way of example, certain types of software capable of encrypting or decrypting information are listed in the Commerce Control List under ECCN # 5D002. A company that develops an encryption software program together with its source code which is listed in the Commerce Control List under ECCN # 5D002, must apply for a license exemption to the Commerce Department to be able to export such software to any country in the world, except Canada. With respect to some types of 5D002 encryption software, CFIUS regulations require that before concluding that no mandatory CFIUS filing is required, an application for the license exemption must have been filed with the Department of Commerce.

As a result, the parties to a foreign buyer's acquisition of a U.S. Company that develops such encryption software might find themselves having to choose before closing between applying to the Export Authorities for a license exemption, in which case they would be exempt from a mandatory filing, or filing a mandatory declaration with CFIUS.

This need to determine the export license status of a target's products complicates the CFIUS mandatory notification analysis by requiring parties to determine the export control status of all products, software and technology that are produced, designed, tested, manufactured, fabricated or developed by the U.S. Business (whether or not they are in fact exported), the jurisdiction of every entity in the investment chain and the corresponding licensing requirements, potentially introducing significant delays for any target business that has not previously undergone a thorough export review.

Export control analysis is burdensome and time-consuming and requires someone familiar with U.S. export laws working with personnel familiar with the technical aspects of the company's software to wade through potentially applicable export control regimes. This may lead the parties to make a notification to CFIUS in case of doubt.

To sum up, whether or not there is a mandatory filing requirement with respect to a foreign investment in a TID U.S. Business that produces Critical Technology depends on a three-pronged test as follows:

- whether the investment target is a U.S. Business that is involved with Critical Technology;
- whether the foreign investor is receiving rights of control, access to material non-public technical information in the target, voting or observer rights on the board of the target or any

involvement, other than through voting of shares, in substantive decision making with respect to the Critical Technology; and

- whether the Critical Technology requires an export license for export to the foreign buyer and any of its parents.

Certain investors from excepted foreign states, "FOCI" (foreign ownership, control or influence) mitigated entities (subject to special security agreements, voting trust agreements or proxy agreements to offset foreign control) as well as investment funds managed exclusively and ultimately controlled by U.S. nationals, are excluded from the mandatory CFIUS filing requirement.

A mandatory filing can be done either by filing a short form, 5-page declaration to which CFIUS must respond within 30 days or by filing the long form CFIUS notice to which CFIUS must respond within 45 days, subject to an extension of another 45 days.

If one is confident that the target's products and technologies are not ones which would raise national security concerns, one should use the short form declaration.

CFIUS responds to a declaration in one of three ways: (i) it issues a safe harbor letter that it will take no action with respect to the declaration; (ii) it responds that it cannot take a view with respect to whether there are any national security concerns, which is the usual response; or (iii) if CFIUS has reason to believe that the transaction may raise national security concerns, it requests that the filer file the longer form of notice.

The penalty for not making a mandatory filing is the greater of $250,000 and the value of the transaction.

EXEMPTIONS FOR CERTAIN INVESTORS FROM CLOSE US ALLIED COUNTRIES

FIRRMA directed CFIUS to exempt from its expanded jurisdiction over non-controlling investments and acquisitions of certain real estate interests and from its mandatory filing requirements, certain foreign states that have their own robust processes to analyze foreign investment for security risks and certain foreign investors from such states.

The final regulations identify Australia, Canada and Great Britain (including Northern Ireland) as the countries that initially qualify as excepted foreign states.

Designation of these countries was largely anticipated as each operates pursuant to an intelligence-sharing arrangement with the U.S. government.

These countries are deemed excepted foreign states beginning February 13, 2020, for a period of three years.

For each country to remain as an excepted foreign state after this three year period, CFIUS will need to determine that its foreign investment review process is sufficiently robust and otherwise coordinates with CFIUS on national security reviews of transactions.

The final rules exempt investors with substantial ties to these countries ("excepted investors") from several CFIUS requirements.

Specifically, excepted investors will be exempt from CFIUS's expanded jurisdiction to review non-controlling investments in TID U.S. Businesses and certain investments in U.S. real estate. Excepted investors will also be exempt from the mandatory filing requirements in respect of government linked acquisitions of a substantial interest in TID U.S. Businesses and for investments they make in TID U.S. Businesses that produce or develop Critical Technologies for which a license would be required if such technology would be exported to the foreign buyer or to any of its parents in the chain of ownership, though such investments will continue to be subject to voluntary CFIUS reporting.

To qualify for the regulatory exemption, an excepted investor must (i) be organized under the laws of an excepted foreign state or the United States; (ii) have its principal place of business in an excepted foreign state or in the United States; (iii) require that 75 percent or more of its board members or observers be U.S. nationals or nationals of an excepted foreign state (and not any other state); and (iv) ensure that any foreign person who holds more than 10 percent of its voting interests be a national of an excepted foreign state or the United States (and not any other state).

The final rules also identify certain facts that will disqualify an entity, otherwise meeting the above requirements, from being deemed an excepted investor. These include violations of various CFIUS requirements or other U.S. laws and regulations. In addition, if at any time during the three-year period following the completion date of an investment, the non-U.S. person no longer meets all of the above exemption criteria, the non-U.S. person is not an excepted investor with respect to the investment from the completion date onward.

EXEMPTIONS FOR INDIRECT, FOREIGN INVESTMENTS MADE THROUGH INVESTMENT FUNDS

Another exemption given by FIRRMA from CFIUS's expanded jurisdiction involves non-controlling investments made by foreign persons in TID U.S. Businesses through U.S.-managed investment funds.

The final regulations align with the FIRRMA directives by largely exempting from CFIUS's jurisdiction indirect, passive investments made by foreign investors in TID U.S. Businesses through U.S.-managed investment funds.

To qualify for the exemption, the foreign investor (1) may not be the general partner or managing member of the fund; (2) may not have access to material non-public technical information of the TID U.S. Business; or (3) may not have the ability to control the investment fund by: (i) approving or otherwise controlling the investment decisions of the fund; (ii) approving or otherwise controlling the investment decisions made by the fund's general partner or managing member; or (iii) unilaterally dismissing or determining the compensation of the general partner or managing member of the fund.

Any fund meeting these requirements will also be exempt from the mandatory filing requirements for investments in TID U.S. Businesses that produce or develop "Critical Technologies" for which an export license would be required.

Under the regulations, a foreign investor's participation on a limited partner advisory board or similar committee will not, in and of itself, disqualify the investor from the exemption so long as the advisory board does not have the ability to control the investment decisions made by the fund or its general partner.

The regulations also note that routine advisory board actions, including those involving waivers of potential conflicts of interest and fund allocation limitations, will not result in control of the fund.

Under current CFIUS regulations, if an entity's principal place of business is within the United States, it is not considered a "foreign entity" for CFIUS purposes (excluding its U.S. investments from CFIUS jurisdiction). U.S. private equity funds and other U.S. institutional investors have relied on CFIUS's understanding that their principal place of business is within the United States notwithstanding the fact that many of their investment vehicles are incorporated outside of the United States for tax efficiency purposes. Previous CFIUS regulations had not defined principal place of business, which created some ambiguity regarding the facts needed to establish the principal place of business of a U.S.-managed investment fund.

The final regulations attempt to resolve this ambiguity by defining the principal place of business as "the primary location where an entity's management directs, controls, or coordinates the entity's activities, or, in the case of an investment fund, where the fund's activities and investments are primarily directed, controlled, or coordinated by or on behalf of the general partner, managing member, or equivalent..."

The regulations clarify, however, that if an entity has represented in an official filing with the federal, state or any foreign government that its principal place of business is outside of the United States, that location will be deemed the principal place of business of the entity for CFIUS purposes unless it can demonstrate that such location has subsequently changed.

This clarification may have broad ramifications for the U.S. investment fund industry as fund managers may need to review whether they have made any such representations in filings with any government.

MITIGATION

Once CFIUS has reviewed a transaction, it may condition approval on certain steps it requires the target to take to minimize national security risks.

Mitigation, usually through National Security Agreements, can include governance controls, third party oversight, special reporting requirements, operational restrictions, investment standstills divestments, policy and procedure requirements, and often include mitigation agreements.

A violation of a mitigation agreement incurs the same penalties as a failure to file a mandatory declaration.

FOREIGN LENDERS

Loans made by foreign persons to a U.S. Business that include security interests over the securities or assets of the U.S. Business are not in themselves subject to CFIUS review, but may become so if at any stage the foreign lender acquires an equity interest, the right to appoint a board member or other rights characteristic of an equity investment or the right to gain control over the U.S. Business after a default.

Lenders should file a notice or declaration with CFIUS only at the time that, because of imminent or actual default, there is a significant possibility that the foreign lender may obtain control of the U.S. Business or acquire a non-control stake with access rights or involvement in important matters concerning the U.S. Business as a result of the default.

CFIUS regulations provide that CFIUS will take into account, for purposes of deciding whether it has review jurisdiction and for purposes of mandatory filing requirements, whether the foreign lender has transferred day-to-day control over the U.S. Business to U.S. Persons, or to excepted investors.

CFIUS will not have jurisdiction to review and there will be no mandatory reporting requirement in respect of a transaction for the acquisition of a voting interest upon default where the foreign lender is one of a syndicate of banks making the loan and requires the majority consent of the U.S. participants in the syndicate to take action or where the foreign lender does not have a lead role in the syndicate and is subject to a provision limiting its ability to control the debtor or exercise access rights or involvement in the debtor.

ACQUISITION OF CONTINGENT EQUITY INTERESTS

In determining whether acquisition of a contingent equity interest, such as convertible preferred shares or an option to purchase shares, gives CFIUS jurisdiction to review or triggers mandatory filing, CFIUS will take the following factors into consideration:

- the imminence of conversion;
- whether the conversion is at the option of the foreign investor; and
- whether the percentage in interest of the outstanding equity upon conversion can be determined at the time of acquisition.

Based on these considerations, CFIUS has the discretion not to treat the acquisition of a contingency equity interest as an immediately effective acquisition for purposes of CFIUS's jurisdiction to review the transaction and for CFIUS mandatory filing.

NON-NOTIFIED TRANSACTIONS

As a result of FIRRMA and the increased resources it gave CFIUS, there is now a team within CFIUS dedicated to identifying and investigating non-notified transactions. Dozens of case workers review data bases, social media and M&A blogs for non-reported transactions.

The team has identified hundreds of M&A joint ventures, corporate restructurings and investments in a number of strategically important industries.

Parties should consider whether a competitor or other party unhappy with the transaction may contact CFIUS.

When CFIUS comes knocking on the door to investigate a non-reported transaction, it sends a series of questionnaires which will include questions about the foreign investor and its ultimate owners.

Following the Q&A period, CFIUS will review the parties' responses to see whether it has jurisdiction and may confirm that it has none or start an investigation and ask for a notice to be filed.

CFIUS can impose mitigation measures (such as suspending integration of the business) while it conducts its review.

A CFIUS review of a non-notified transaction is more likely to result in mitigation measures than a transaction pro-actively notified to CFIUS.

The number of non-notified transactions for which CFIUS requested a notice has increased exponentially since FIRRMA.

It is important that parties pro-actively analyze the CFIUS requirements of the transaction early and before completion, in order to avoid receiving an email from Treasury a year or so after closing.

CONCLUSION

It is important to note that, today after FIRRMA and its implementing regulations, CFIUS reviews three types of transactions: control transactions, non-control investments, and real estate transactions. CFIUS's jurisdiction over control transactions remains almost unlimited as before. In order to review a control transaction, CFIUS does not have to show that the U.S. business is a TID U.S. business, that the purchaser has access to sensitive information, or that the U.S. business is involved in any Critical Technology for which an export license is required. Rather, CFIUS's jurisdiction over control transactions is based on a smell test. If it smells to CFIUS like a national security risk, they will come in and review. It is only with respect to non-control investments that CFIUS's jurisdiction depends on whether the business is a TID U.S. business, whether the purchaser has access rights to sensitive information and whether a specific Critical Technology requires an export license. In considering whether a particular transaction is subject to CFIUS's more limited review over non-control investments or wider review over control transactions, one should bear in mind the broad definition of "control." Many cases that one might consider to be non-control investments might be considered by CFIUS to be a control transaction.

In considering whether a control or non-control investment in a TID U.S. Business involved in Critical Technology requires a mandatory filing, it will be necessary to determine the export control status of its products, the jurisdiction of every owner of the foreign investor, and the corresponding licensing requirements.

A CFIUS analysis will also need to look at whether a foreign non-excepted government controls the foreign purchaser and whether an excepted investor from an excepted country fulfills all the conditions for an excepted investor, not only at the time of the transaction but also for a period of three years following the transaction.

related professionals

Raphael S. Grunfeld / Partner
D: 212-238-8653
grunfeld@clm.com