COSMOS
Navigate the Compliance Universe

CEP Magazine - January 2019
CFIUS and FIRRMA: Protecting technology and intellectual property

by Michael Rose and Steve Siemborski

Michael Rose (mmichael.rose@us.gt.com) is a Partner and a leader of Grant Thornton LLP's National Governance Risk and Compliance practice in Philadelphia, Pennsylvania, USA.

- grantthornton.com/people/bios/r/rose-michael.aspx
- linkedin.com/in/michael-rose-52382018/
- twitter.com/grantthorntonus
- instagram.com/grantthorntonusa/
- linkedin.com/company/grant-thornton-llp/

Steve Siemborski, CCEP (mssiemborski@calfeesolutions.com) is Managing Director at Calfee Strategic Solutions in Washington, DC.

- calfee.com/professionals/steven-l-siemborski
- linkedin.com/company/calfee-strategic-solutions-llc/

This is the first article in a three-part series on foreign investment regulations.

Heightened US sensitivity to the potential national security ramifications of sales, mergers, or other transactions with foreign parties is a significant potential complication for cross-border deals. Both US companies and foreign entities that are contemplating a transaction must follow a rigorous process to counter any potential threats.

The Committee on Foreign Investment in the US (CFIUS) was formed to evaluate transactions where the acquiring entity is foreign. CFIUS was formed in 1975 to address a fear that technology or funds from an acquired US business might be transferred to a sanctioned country as a result of being acquired by a foreign entity.

CFIUS is focused on deals with US companies that:

- **Produce, design, test, manufacture, fabricate, or develop critical technologies.** Critical technologies are those subject to new export control provisions designed to protect emerging and foundational technologies.
- **Own, operate, manufacture, supply, or service critical infrastructure.** Critical infrastructure companies own, operate, manufacture, supply, or provide services in industries like telecommunications, utilities, transportation, financial services, healthcare, and government services, among others.
- **Sensitive data companies.** These companies maintain or collect sensitive data on US citizens that may be exploited in a manner that could threaten national security.

Updates to CFIUS were made under the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) that went into effect in August 2018.[1] FIRRMA expands CFIUS oversight to include non-passive, minority position investments in critical technology or infrastructure; joint ventures involving technology transfers to a foreign entity; and real estate investments near military or other national security facilities. FIRRMA also includes a provision about acquisition of early stage technologies by unspecified "countries of special concern" that pose a significant national security threat. FIRRMA would nearly double the list of national security factors for CFIUS to consider in its risk reviews and lengthen the review period. As a result, companies considering deals with foreign entities could face and should prepare for a significant CFIUS compliance process.

Safeguarding technology and intellectual property

A key CFIUS focus is technology and its underlying intellectual property, which are assets with both monetary and strategic value. America is an incubator for new technology. Some of our most successful companies — like Apple, Google, Microsoft, Facebook, and Amazon, to name a few — have proprietary technology that started as an idea in their creators' heads. New, potentially lucrative start-ups regularly emerge, and the Holy Grail for a young technology company is to attract private equity investment, which comes in stages as a company develops. Early stage investment is critical for future success and growth. At this point, companies are particularly vulnerable to cash infusions and/or acquisition by foreign entities because of their desire for growth funding.

Foundational technologies are especially attractive to foreign exploitation and are a focus for CFIUS scrutiny. These can be stand-alone products or can serve as a building block that enables progress and applications in multiple areas, including military applications. Some examples that are getting a lot of attention include self-driving cars and trucks, machine learning, artificial intelligence, IT processing and storage, mobile computing and communications, social computing and networking, synthetic biology, wearable technology, robotics, cloud computing, big data, and neuroscience.

The CFIUS compliance process

In a covered transaction, the compliance process generally ranges from 30–90 days and includes:

- An initial 45-day review following CFIUS' receipt of the notice, with an optional 15-day extension.
- An investigation period of up to 45 days for transactions requiring additional scrutiny.
- A 15-day period for transactions referred to the president for review.

At the end of that period, a National Security Agreement (NSA) will be entered into between the acquirer and CFIUS. The NSA will set out the terms on which the covered transaction will be allowed to take place. The NSA can be very broad and cover a wide range of conditions, which depend on the security risk of the transaction. Examples of some provisions that have been included in NSAs are:

- Appointment of a third-party monitor.
- Communications infrastructure must be located largely or exclusively in the US.
- Transaction data related to domestic communications is stored largely or exclusively in the US.
- US customers' records and data are stored largely or exclusively in the US.
- Outsourcing to non-US entities is restricted or prohibited (unless part of an agreement with the Department of Homeland Security).

- Guarantee that any third-party contractor performing a function covered by the NSA will comply with its terms.
- US government inspections of US-based facilities.
- US government interviews of US-based personnel on very short notice.

FIRRMA expanded CFIUS' jurisdiction, plus it included a provision addressing concerns about acquisition of early stage technologies by unspecified countries of special concern that pose a significant national security threat. It nearly doubles the list of national security factors for CFIUS to consider in its risk reviews.

Navigating the CFIUS compliance process

Any foreign company acquiring or investing in a US company with national security concerns is required to get CFIUS approval. For companies that are unsure about whether CFIUS compliance applies to them, here are four important things to consider:

1. Does the target company work with export-controlled technologies?
2. Does its activity include testing, design, production, manufacturing, fabrication, or development of critical technologies?
3. Does it own, operate, manufacture, or supply any critical infrastructure?
4. Does it maintain, collect, or otherwise access sensitive information about US citizens?

Foreign entities contemplating or executing a covered transaction are required to first proactively file a notice with CFIUS. These transactions include mergers, acquisitions, and takeovers by or with any foreign entity that could result in foreign control of a US business. CFIUS has the authority to compel a filing if it determines that a transaction poses a potential risk to national security, so it makes sense to file the notice as soon as possible. The acquirer must agree to an NSA that outlines the restrictions and controls that CFIUS will impose as a condition of consenting to the transaction, and CFIUS must approve the NSA.

For those companies that are already in the process, there are some important things to consider. It goes without saying that responses to any ongoing CFIUS requests must be timely and complete. During the process, CFIUS can make changes that add to or end a deal completely. These include adding deal conditions or adding a mitigation agreement to address security risks. Efficiently working with CFIUS may help avoid or influence the conclusions presented for presidential review, if the process gets that far. The current administration has been more likely to reject deals, so thorough preparation and compliance is crucial.

Readiness measures will help avoid CFIUS findings that an application is incomplete. Typical deficiencies include:

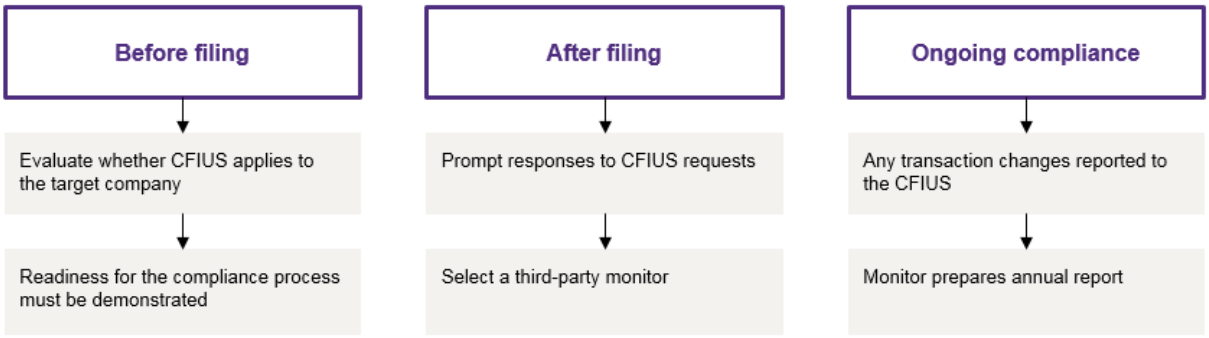
- **Unclear business lines description.** The notice must provide a clear and detailed account of each company's products and services.
- **Unclear transaction description.** The notice must clearly describe all entities involved in the transaction and the nature and structure of the transaction.
- **Not specifically naming geographic location(s) of the US business.** The notice must clearly describe the US business with addresses and/or geographic coordinates for all US properties and facilities.

- **Absence of a certification.** All notices must be certified correctly to be deemed complete.

To avoid deficiencies, many deal participants work with third-party professionals experienced in the CFIUS compliance process.

Another important point is that the compliance process is ongoing. After a deal is approved, a third-party monitor is often required under the terms of the NSA to prepare an annual report of compliance with the terms of the agreement.

Figure 1: Filing steps



Conclusion

For entities that are considering a transaction subject to CFIUS review, getting ahead of CFIUS requirements is essential. Preparation should include understanding both CFIUS and proposed FIRRMA requirements. Preparation will pave the way for a smooth process, if handled proactively.

Takeaways

- Committee on Foreign Investment in the United States (CFIUS) preparation is vital for US or foreign entities considering a transaction subject to CFIUS review.
- Early stage, foundational technology companies are a particular focus for foreign entities looking to exploit their intellectual property.
- The current administration has heightened CFIUS scrutiny.
- Deal participants can be required to have a monitor and provide the annual audit/monitoring report in compliance with the agreed-upon provisions of the National Security Agreement.
- Preparation will pave the way for a smooth process, if handled proactively.

1 "The Committee on Foreign Investment in the U.S. (CFIUS)," U.S. Department of the Treasury, August 2018, http://bit.ly/2PrfYFR