CFIUS Re-enhanced: THE FOREIGN INVESTMENT RISK REVIEW
MODERNIZATION ACT OF 2018 & CHINA

Part I. Introduction

On August 13th, 2018 President Trump signed “The Foreign Investment Risk Review Modernization Act of 2018” (FIRRMA) rebalancing foreign investment in the United States with national security, and firmly aiming its sites on the People’s Republic of China. The passage of FIRRMA was based upon concerns that, “the national security landscape has shifted in recent years, and so has the nature of the investments that pose the greatest potential risk to national security.” As a result, Congress rebalanced the Committee on Foreign Investment in the United States (CFIUS) as a flexible framework of national security measures and a tool in overall national security policy, rather than as a narrow legal structure. The most impactful change to the CFIUS process expanded the authority of CFIUS in reviewing additional transactions, which include real estate transactions, critical and emerging technologies, critical infrastructure and noncontrolling investments. This chapter discusses CFIUS’ re-enhanced role to address evolving trends and national security threats posed by inbound foreign direct investments (FDI), along with the recent rise of China’s economic aggression, which has now prompted calling for greater CFIUS scrutiny of foreign investment transactions.

1 By Michael Kennedy Esq., Kennedy Law & Policy, Washington DC, Homeland Security Institute, Program Vice-Chair, Member (2015-2019). The author thanks Andrew Astuno, Esq. and Michael Cole, Esq. for their helpful comments and edits.


3 The Foreign Investment Risk Review Modernization Act of 2018, §1702(b)(4)

4 CFIUS is an inter-agency committee that reviews the national security implications of foreign investments in U.S. companies or operations. It is chaired by the United States Secretary of the Treasury and includes representatives from 16 U.S. departments and agencies.
The Department of Treasury has promulgated interim regulations through FIRMMA, via a pilot program that began on November 10, 2018, that impact certain decisions and information regarding critical technologies; and (2) the ability of such foreign parties to impact the rapid pace of technological change in certain U.S. industries.

Specifically, the pilot program empowers CFIUS to review non-controlling investments involved in critical technologies related to specific industries. The pilot program also makes effective FIRRMA’s mandatory declarations provision for transactions that fall within the scope of the pilot program – which includes 27 industries involved in critical technologies. This program is in effect until no later than March 5, 2020, at which time final regulations will have been instituted.

A. History of CFIUS: Always Adapting and Now Re-enhanced

Amid growing levels of inbound investment by the Organization of the Petroleum Exporting Countries (OPEC), CFIUS was originally established by President Ford’s Executive Order (EO) in 1975. The Committee members of CFIUS mainly met in secret. Given its limited scope of “national interests,” CFIUS was fairly inactive in its early years, only meeting ten times between 1975 and 1980 and without a clear mandate our strategy as the transactions it should review.

6 Id.
9 Executive Order No. 11858 (b), May 7, 1975, 40 F.R. 20263.
In 1987, CFIUS investigated the Fujitsu-Fairchild merger during a boom in acquisition of U.S. corporations that resulted in a failed acquisition. Fujitsu’s purchase of an 80 percent share of Fairchild, a California semiconductor manufacturer, was criticized by Congress as “selling Mount Vernon to the red coats,” and the Defense Department opposed the acquisition because of Japan’s already significant control over the computer chip industry.

In 1988, following the above concerns of technology, CFIUS’s jurisdiction was codified and significantly expanded. The Exon-Florio amendment gave CFIUS a refocused purpose. Through EO 12661, the amendment stated that CFIUS would conduct reviews and undertake investigations. Thus overnight, CFIUS was transformed from a limited-authority administrative body to a working tool of U.S. foreign investment policy with a firm mandate to advise the President on foreign investment transactions and block them if need be.

On June 13, 2007, Senator Dodd introduced the Foreign Investment and National Security Act of 2007 (FINSA), which President Bush signed and subsequently promulgated EO 13,456 implementing the law. Since FIMSA, there have been narrower proposed amendments to CFIUS, such as Senator Chuck Grassley’s bill placing the Secretary of Agriculture on the

---


14 However, some of the issues raised in the debate still plague CFIUS today. The Exon-Florio proposal debate focused on three issues and a host of opinions: (1) what constitutes foreign control of a U.S. firm; (2) how should national security be defined; and (3) which types of economic activities should be targeted for a CFIUS review.

15 Executive Order 12661 of December 27, 1988, 54 F.R. 779.

16 The law is designated as P.L. 110-49.
Committee over food security. Most of these attempted reforms have been aimed specifically at covered transactions involving Chinese firms. China now tops the list of nations for foreign companies undergoing CFIUS review. Many Chinese companies withdraw from deals before the Committee even reviews them, fearing the blowback from a high-profile rejection.

B. Chinese Economic Aggression – Current Context of FIRMMA’s Passage

Since the 1970s China has embarked on an ambitious program of reform, Made in China 2025, and it has rapidly transformed itself into the second largest economy in the world. However, this growth has been achieved in significant part through aggressive acts, policies, and practices that fall outside of global norms and rules (collectively, “economic aggression”). In 2018, the United States announced a series of trade enforcement actions involving China stemming from three investigations conducted by the U.S. government involving, steel, solar panels, and critical technology. In each instance, China retaliated against U.S. enforcement actions with reciprocal tariffs. In total, over $250 billion worth of U.S. imports from China and $110 billion worth of U.S. exports to China are subject to tariffs initiated in 2018. Concerns


18 The Shuanghui-Smithfield merger and the break between Congress and CFIUS that it caused was the specific trigger of attempted CFIUS reform.


21 (1) Section 201 investigations into a surge of washing machines and solar panel imports, (2) Section 232 investigations into the national security risks posed by imports of steel and aluminum, and (3) the Office of the U.S. Trade Representative’s Section 301 investigation into “whether acts, policies, and practices of the Government of China related to technology transfer, intellectual property, and innovation are unreasonable or discriminatory and burden or restrict U.S. commerce.”

about a wide range of unfair practices of the Chinese government and the Chinese Communist Party related to technology transfer, intellectual property, and innovation are longstanding.

In regard to CFIUS, all deals which have been formally blocked by the President were China-related, most recently the proposed acquisition of a Lattice Semiconductor by Canyon Bridge Capital and Broadcom’s bid for chipmaker Qualcomm. Many other companies either voluntarily pause or cancel their proposed deal or never consider such acquisition in the first place, in light of CFIUS’ mandates.

**Part II. The Foreign Investment Risk Review Modernization Act of 2018**

Although FIRRMA doesn’t specifically identify China, the focus of the bill stems from two urgent and compelling circumstances that are ancillary to China’s robust development of its technology and military economy: (1) the ability and willingness of some foreign parties to obtain equity interests in U.S. businesses in order to affect certain decisions regarding, or to obtain certain information relating to, critical technologies; and (2) the rapid pace of technological change in certain U.S. industries.\(^{23}\) CFIUS was previously authorized to review only transactions (mergers, acquisitions, or takeovers) that resulted in foreign “control”\(^{24}\) over a U.S. business that threatens to impair the national security, or when the foreign entity is controlled by a foreign government, or it would result in control of any “critical infrastructure that could impair the national security.” FIRRMA modified and broadened the authorities by expanding the scope of foreign investments in the U.S. subject to national security review.

---


\(^{24}\) Id at 51328, citing 31 C.F.R. 800.204 Control
Prior to FIRRMA, CFIUS’s authorities did not sufficiently address the new and emerging risks that foreign direct investment can pose to U.S. technological superiority. For example, it overlooked the fact that foreign investors do not need a controlling interest in order to affect certain decisions with respect to the use, development, acquisition, or release of critical technology. CFIUS’s authorities, however, only applied to transactions that could result in foreign control of a U.S. business. Consequently, CFIUS had no authority to prevent a foreign entity from acquiring a non-controlling interest in a U.S. business that produces, designs, tests, manufactures, fabricates, or develops critical technologies. FIRRMA now provides CFIUS new authorities to address the national security concerns that may arise from these investments, but those authorities were not immediately effective upon FIRRMA’s enactment.25

A. Covered Transactions – Expanded Jurisdiction

1. Expansion of Covered Transactions

In response to growing concerns that other types of cross-border transactions could present national security risks, and that parties were increasingly using those other transaction types to avoid CFIUS review, FIRRMA expands “covered transactions” to include foreign non-controlling investments in: (1) U.S. critical technology or infrastructure and (2) real estate near U.S. military or other national security-related sites. As discussed above, the interim regulations now in place covers transactions in 27 defined industries involved in critical technologies. The pilot program also makes effective FIRRMA’s mandatory declarations provision for transactions that fall within the scope of the pilot program which FIRRMA describes as “abbreviated notifications that would not generally exceed 5 pages in length” — for

25 Id at 51324.
all transactions covered by the pilot program. Mandatory declarations, authorized under FIRMA, are a key change to the CFIUS process, which has historically been ostensibly voluntary. Moreover, failure to submit a mandatory declaration when required under the pilot program can result in potentially significant penalties - up to the value of the transaction.

2. Real Estate Transactions - Close Proximity to Military or Sensitive Sites
   Investments in Critical Infrastructure or Critical Technology Companies

CFIUS has raised concerns about a number of transactions in which U.S. businesses had facilities or assets in close proximity to sensitive government installations. Although Chinese companies invest in a broad range of U.S. industries, Chinese deals are mainly focused on high-value acquisitions in technology, agriculture, modern services, and commercial real estate. In 2012, President Obama blocked a Chinese acquisition of Oregon wind farms because they were located too close to a naval weapons station. As a result, CFIUS’s current authority was silent on reviewing real estate transactions such as short-term leases, or transactions that lack a “US business,” even if such transactions pose similar proximity concerns. CFIUS now has the authority to review the purchase or lease by, or concessions to, a foreign person of private or public real estate in the United States that is: (i) located within or will function as part of, an air or maritime port; or (ii) in close proximity to a U.S. military installation or another facility or property of the United States government that is: (a) sensitive for reasons relating to national security; (b) could reasonably provide the foreign person the ability to collect intelligence on activities being conducted at such an installation, facility, or property; or (c) could otherwise

---

28 Rachelle Younglai, Obama blocks Chinese wind farms in Oregon over security, Reuters, September 29, 2012
expose national security activities at such an installation, facility, or property to the risk of foreign surveillance.\(^{29}\)

3. **Non-controlling investments - Critical Infrastructure, Technologies and Sensitive Data**

Additionally, CFIUS now has expressed jurisdiction to review any “other investments” by a foreign person in any unaffiliated U.S. business that: (ii) produces, designs, tests, manufactures, fabricates, or develops critical technologies; or \(^{30}\) such “other investment” will be covered only if it affords the foreign person: (i) access to any material nonpublic technical information possessed by the U.S. business; (ii) membership, observer, or nomination rights for the board (or equivalent body) of the U.S. business; or (iii) any involvement, other than through voting of shares, in substantive decision-making related to sensitive personal data, critical technologies, or critical infrastructure.\(^{31}\)

To adapt to the global applicability of transactions, the definition of “U.S. business” is intentionally broadened to include “a person engaged in interstate commerce in the United States..” This exceeds the current regulatory definition, which includes “but only to the extent of its activities in interstate commerce in the United States.” Now, the bill gives the Committee the authority to review an acquisition of any business anywhere in the world as long as that business provides goods or services into the United States.

4. **Other Provisions**

\(^{29}\) See 3, at §1703

\(^{30}\) The Foreign Investment Risk Review Modernization Act of 2018, §1703(b)(iii)

\(^{31}\) Id at §1719
FIRRMA includes notable CFIUS changes from its predecessor, with a clear focus on China. First, FIRRMA requires a list of countries of ‘special concern” that targeting certain countries\(^{32}\), a biennial report to Congress on FDI transactions by Chinese entities.\(^{33}\) The report must include detailed breakdowns of those foreign direct investments, a list of US companies purchased through Chinese government investment, and an analysis of Chinese investment practices in the United States.\(^{34}\) Additionally, Congress calls for the President to conduct a more robust international outreach effort to urge and help allies to establish processes similar to [CFIUS].”\(^{35}\) FIRRMA also clarified that civil action challenges against the CFIUS actions and findings may only be brought in the United States Court of Appeals for the District of Columbia Circuit.\(^{36}\)

Conclusion: If needed.

\(^{32}\) “The Secretary of Defense shall establish and maintain a list of acquisition programs, technologies, manufacturing capabilities, and research areas that are critical for maintaining the national security technological advantage of the United States over foreign countries of special concern.”

\(^{33}\) Id

\(^{34}\) Id

\(^{35}\) Id at §1706(a)(6)

\(^{36}\) Id at §1715
Export Control Reform Act

- Establishes an interagency process to identify emerging and foundational technologies
- Expected broadly to track “Made in China 2025” plan
- The November 2018 Advanced Notice of Proposed Rulemaking (ANPRM) solicits comments by December 19, 2018
Commerce’s Authority

- The Secretary of Commerce may, in coordination with the Secretary of Defense, the Secretary of State, and the heads of other federal agencies, as appropriate, specify the level of control to apply, including a requirement for a license or other authorization for the export, reexport, or in-country transfer of that technology.

- In determining the level of control appropriate for emerging and foundational technologies, the Secretary shall take into account (i) lists of countries to which exports from the United States are restricted; and (ii) the potential end uses and end users of the technology.
What are Emerging and Foundational Technologies?

- Interagency Process as provided for in the Export Control Reform Act of 2018
- Generally, to capture technologies not currently listed on either the Commerce Control List (CCL) or the U.S. Munitions List (USML)
- CFIUS Chairperson may recommend technologies to be considered “emerging and foundational”
Emerging and Foundational Technologies: Made in China 2025 Industries

- Chinese policies are aimed at advancing specific industrial sectors:

<table>
<thead>
<tr>
<th>New advanced information technology</th>
<th>New-energy vehicles and equipment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated machine tools &amp; robotics</td>
<td>Power equipment</td>
</tr>
<tr>
<td>Aerospace and aeronautical equipment</td>
<td>Agricultural equipment</td>
</tr>
<tr>
<td>Maritime equipment / high-tech shipping</td>
<td>New materials</td>
</tr>
<tr>
<td>Modern rail transport equipment</td>
<td>Biopharma / advanced medical products</td>
</tr>
</tbody>
</table>
Emerging Technologies Under the ANPRM

- The ANPRM seeks public comment on criteria for identifying emerging technologies. BIS plans to issue a separate ANPRM regarding identification of foundational technologies.
- The ANPRM lists the following general categories of technology:

<table>
<thead>
<tr>
<th>Biotechnology</th>
<th>Artificial intelligence (AI) and machine learning technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position, Navigation, and Timing (PNT) technology</td>
<td>Microprocessor technology</td>
</tr>
<tr>
<td>Advanced computing technology</td>
<td>Data analytics technology</td>
</tr>
<tr>
<td>Quantum information and sensing technology</td>
<td>Logistics technology</td>
</tr>
<tr>
<td>Additive manufacturing</td>
<td>Robotics</td>
</tr>
<tr>
<td>Brain-computer interfaces</td>
<td>Hypersonics</td>
</tr>
<tr>
<td>Advanced materials</td>
<td>Advanced surveillance technologies</td>
</tr>
</tbody>
</table>
ANPRM Considerations?

- The ANPRM seeks comments on:
  (1) how to define emerging technology to assist in identification of such technology in the future;
  (2) criteria to apply to determine whether there are specific technologies within the general categories above that are important to U.S. national security;
  (3) sources to identify such technologies;
  (4) other general technology categories that warrant review;
  (5) the status of development of these technologies in the United States and other countries;
  (6) the impact specific emerging technology controls would have on U.S. technological leadership; and
  (7) any other approaches to the issue of identifying emerging technologies important to U.S. national security that would warrant consideration for export control.
Supply Chain Developments

- The 2019 National Defense Authorization Act ("NDAA") imposes new restrictions on procurements for telecommunications equipment or services based on ties to certain Chinese entities.
- A new Executive Order grants the Department of Commerce the authority to prohibit communications providers from using particular products in their networks.
- Commerce’s Bureau of Industry and Security (BIS) added Huawei to its Entity List.
2019 NDAA Supply Chain Restrictions

- Section 889 creates a *general prohibition* on telecommunications or video surveillance equipment or services produced or provided by the following companies (and associated subsidiaries or affiliates):
  - Huawei Technologies Company; or
  - ZTE Corporation
- Also prohibits equipment or services used *specifically for national security purposes*, such as public safety or security of government facilities, provided by the following companies (and associated subsidiaries or affiliates):
  - Hytera Communications Corporation;
  - Hangzhou Hikvision Digital Technology Company; or
  - Dahua Technology Company
- Authorizes the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the FBI, to extend these restrictions to additional companies based on their relationships to the Chinese government.
- Effective August 13, 2019.
EO on Communications Supply Chain

- The order allows the Secretary of Commerce to prohibit any acquisition, importation, transfer, installation, dealing in, or use of any “information and communications technology or service” where Commerce finds that “the transaction involves information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary,” and the transaction:
  - (A) poses an undue risk of sabotage or maintenance of information and communications technology or services in the United States;
  - (B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or
  - (C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

- The term “information and communications technology or services” is not limited to 5G technology and services but is defined broadly to include “any hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including transmission, storage, and display.”

- The order directs Commerce to publish implementing regulations within 150 days.
  - October 12, 2019.
Huawei on the Entity List

- The restrictions prohibit exports, reexports, and transfers of U.S. goods, software, and technology, including common, off-the-shelf electronic components and commercial software to Huawei.

- Users and operators may not receive updates and patches for Huawei network equipment and handsets to the extent such updates or patches are provided from U.S. entities and routed through or customized by Huawei.

- The sweeping prohibitions also extend to the provision of parts, components, software, or other items that would be used to service or repair equipment already owned by Huawei.
  - Commerce took similar action against ZTE back in 2016.