

**ALERT**

# CFIUS to Review More Investments in Technology, Infrastructure, and Data Companies Under Sweeping New Regulations

September 19, 2019

On Tuesday, September 17, 2019, the U.S. Department of the Treasury (Treasury) issued proposed regulations to implement the Foreign Investment Risk Review Modernization Act (FIRRMA), a law that significantly expanded the jurisdiction and operational mandate of the Committee on Foreign Investment in the United States (CFIUS). The proposed rules will amend and restate the current CFIUS regulations at 31 CFR part 800 and will add a new part 802 covering certain real estate transactions. The proposed rules will especially impact certain foreign investments in U.S. businesses involved in technology, infrastructure, and personal data. This alert analyzes the proposed revisions to part 800. Wiley Rein will separately analyze the proposed addition of part 802 in a subsequent alert. Public comments on both sets of rules must be submitted by October 17, 2019. The final regulations will become effective no later than February 13, 2020.

## **Non-Controlling “Covered Investments” in Critical Technology, Critical Infrastructure, and Sensitive Personal Data Businesses**

Prior to the enactment of FIRRMA, CFIUS was limited to reviewing only transactions that could result in “control” of a U.S. business by a foreign person. FIRRMA significantly expanded CFIUS’s jurisdiction to include (among other things) certain non-controlling, non-passive investments in any U.S. business that:

- Produces, designs, tests, manufactures, fabricates, or develops one or more critical technologies;

## Authors

Nova J. Daly  
Senior Public Policy Advisor  
202.719.3282  
ndaly@wiley.law  
Daniel P. Brooks  
Partner  
202.719.4183  
dbrooks@wiley.law

## Practice Areas

Committee on Foreign Investment in the United States (CFIUS)  
Government Contracts  
International Trade  
National Security  
Telecom, Media & Technology

- Owns, operates, manufactures, supplies, or services critical infrastructure; or
- Maintains or collects sensitive personal data of U.S. citizens that may be exploited in a manner that threatens national security.

The proposed rule collectively refers to such businesses as “TID U.S. businesses,” with “TID” being an acronym for “technology, infrastructure, and data.” Subject to certain exceptions and exclusions described below, non-controlling foreign investments in such businesses will be treated as “covered investments” subject to CFIUS review to the extent that the investment would afford the foreign person any of the following:

- Access to any “material nonpublic technical information” in the possession of the TID U.S. business;
- Membership or observer rights on the board of directors or equivalent governing body of the TID U.S. business or the right to nominate an individual to a position on the board of directors or equivalent governing body of the TID U.S. business; or
- Any involvement, other than through voting of shares, in “substantive decisionmaking” of the TID U.S. business regarding (1) the use, development, acquisition, safekeeping, or release of sensitive personal data of U.S. citizens maintained or collected by the TID U.S. business; (2) the use, development, acquisition, or release of critical technologies; or (3) the management, operation, manufacture, or supply of “covered investment critical infrastructure.”

The proposed rule provides the following definitions relevant to determining whether a non-controlling investment is a “covered investment” subject to CFIUS review:

**Critical Technologies.** In accordance with FIRRMA, the proposed rule defines “critical technologies” to include the following:

- Defense articles or defense services included on the United States Munitions List (USML) set forth in the International Traffic in Arms Regulations (ITAR);
- Items included on the Commerce Control List (CCL) set forth in the Export Administration Regulations (EAR) and controlled (1) pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or (2) for reasons relating to regional stability or surreptitious listening;
- Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by 10 CFR part 810 (relating to assistance to foreign atomic energy activities);
- Nuclear facilities, equipment, and material covered by 10 CFR part 110 (relating to export and import of nuclear equipment and material);
- Select agents and toxins covered by 7 CFR part 331, 9 CFR part 121, or 42 CFR part 73; and
- Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (ECRA).

The U.S. Department of Commerce's Bureau of Industry and Security (BIS) published an Advanced Notice of Proposed Rulemaking last year seeking comment on criteria for identifying "emerging technologies" under ECRA. BIS is expected to issue proposed regulations governing emerging technologies this fall and to initiate a separate rulemaking with respect to foundational technologies later this year. Any technologies that BIS identifies as emerging or foundational technologies will be treated as critical technologies for CFIUS purposes.

**Critical Infrastructure.** With respect to covered investments, the proposed rule defines "covered investment critical infrastructure" as the "systems and assets, whether physical or virtual," that are specifically identified in an appendix to the proposed rule. Covered investment critical infrastructure includes, for example, certain IP networks; telecommunications and information services; submarine cable systems and facilities; data centers; satellite systems; facilities that manufacture certain specialty metals, carbon, alloy, or armor steel plate; electricity, oil, and gas facilities; securities exchanges; facilities that serve military installations; technology service providers; airports; maritime ports; and public water systems. Because a U.S. business must "own, operate, manufacture, supply, or service" critical infrastructure in order for an investment in such a business to be treated as a "covered investment," the appendix also identifies the specific functions that the U.S. business must perform in order to qualify as a "TID U.S. business" with respect to the particular covered investment critical infrastructure at issue.

Importantly, this definition only applies in the context of non-controlling "covered investments." With respect to transactions that could result in control of a U.S. business by a foreign person – which the proposed rule refers to as "covered control transactions" – the proposed rule retains the pre-FIRRMA definition of "critical infrastructure" 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."

**Sensitive Personal Data.** The proposed rule defines "sensitive personal data" to include (1) certain "identifiable data" described below, and (2) all genetic information.

"Identifiable data" refers to data that can be used to distinguish or trace an individual's identity, including through the use of a "personal identifier," such as a name, physical address, email address, social security number, phone number, or "other information that identifies a specific individual." The proposed rule clarifies that aggregated data or anonymized data will be treated as identifiable data "if any party to the transaction has, or as a result of the transaction will have, the ability to disaggregate or deanonymize the data, or if the data is otherwise capable of being used to distinguish or trace an individual's identity." Identifiable data does not include encrypted data "unless the U.S. business that maintains or collects the encrypted data has the means to de-encrypt the data so as to distinguish or trace an individual's identity."

Identifiable data will be treated as "sensitive personal data" if:

(1) it is maintained or collected by a U.S. business that (a) targets or tailors products or services to any U.S. executive branch agency or military department with intelligence, national security, or homeland security responsibilities, or to personnel and contractors thereof; (b) has maintained or collected such data on more

than one million individuals at any point over the preceding 12 months; or (c) has a demonstrated business objective to maintain or collect such data on more than one million individuals and such data is an integrated part of the U.S. business's primary products or services; and

(2) it falls within any of the following categories:

- Data that could be used to analyze or determine an individual's financial distress or hardship;
- The set of data in a consumer report, unless such data is obtained from a consumer reporting agency for certain identified purposes and such data is not substantially similar to the full contents of a consumer file;
- The set of data in an application for health insurance, long-term care insurance, professional liability insurance, mortgage insurance, or life insurance;
- Data relating to the physical, mental, or psychological health condition of an individual;
- nonpublic electronic communications, including email, messaging, or chat communications, between or among users of a U.S. business's products or services if a primary purpose of such product or service is to facilitate third-party user communications;
- Geolocation data collected using positioning systems, cell phone towers, or WiFi access points such as via a mobile application, vehicle GPS, other onboard mapping tool, or wearable electronic device;
- Biometric enrollment data, including facial, voice, retina/iris, and palm/fingerprint templates;
- Data stored and processed for generating a state or federal government identification card;
- Data concerning U.S. government personnel security clearance status; or
- The set of data in an application for a U.S. government personnel security clearance or an application for employment in a position of public trust.

In addition to the identifiable data listed above, all genetic information will be treated as sensitive personal data, regardless of whether it meets any of these criteria. The proposed rule clarifies that sensitive personal data does not include (1) data maintained or collected by a U.S. business concerning the employees of that U.S. business, unless the data pertains to employees of U.S. Government contractors who hold U.S. Government personnel security clearances; or (2) data that is a matter of public record, such as court records or other government records that are generally available to the public.

**Access and Involvement Rights.** As noted above, an investment will only be treated as a covered investment to the extent that it affords the foreign person access to "material nonpublic technical information," board membership or observer rights (or the right to nominate a board member), or involvement in certain "substantive decisionmaking" regarding the TID U.S. business. The proposed rule defines "material nonpublic technical information" as information that either (1) provides knowledge, know-how, or understanding not available in the public domain, of the design, location, or operation of critical infrastructure, including, without limitation, vulnerability information such as that related to physical security or cybersecurity; or (2) is not available in the public domain and is necessary to design, fabricate, develop, test, produce, or manufacture a

critical technology, including, without limitation, processes, techniques, or methods. Material nonpublic technical information does not include financial information regarding the performance of an entity.

The proposed rule defines “substantive decisionmaking” as “the process through which decisions regarding significant matters affecting an entity are undertaken,” including, for example, pricing, sales, and specific contracts; supply arrangements; corporate strategy and business development; research and development; manufacturing locations; access to critical technologies, covered investment critical infrastructure, material nonpublic technical information, or sensitive personal data; physical and cybersecurity protocols; practices, policies, and procedures governing the collection, use, or storage of sensitive personal data; and strategic partnerships. The proposed rule clarifies that substantive decisionmaking does not include strictly administrative decisions.

***Exception for Investments by Certain Foreign Investors.*** Covered investments will not include investments made by “excepted investors” that have close ties to “excepted foreign states.” Excepted foreign states will be identified by the Secretary of the Treasury, with the agreement of two-thirds of the voting members of CFIUS, upon a determination that a foreign state “has established and is effectively utilizing a robust process to analyze foreign investments for national security risks and to facilitate coordination with the United States on matters relating to investment security.” Treasury intends to publish an initial list of excepted foreign states with the final rule and may delay certain eligibility requirements for two years “in order to provide the eligible foreign states time to enhance their foreign investment review processes and bilateral cooperation.”

The proposed rule defines an “excepted investor” as a foreign person who is (1) a foreign national who is a national of one or more excepted foreign states (and is not also a national of any foreign state that is not an excepted foreign state); (2) a foreign government of an excepted foreign state; or (3) a foreign entity that meets each of the following conditions with respect to itself and each of its parents:

- The entity is organized under the laws of an excepted foreign state or the United States;
- The entity has its principal place of business in an excepted foreign state or the United States;
- Each member or observer of the board of directors or similar body of the entity is a U.S. national or a national of one or more excepted foreign states (and is not also a national of any foreign state that is not an excepted foreign state);
- Any foreign person that individually holds (or each foreign person that is part of a group of foreign persons that, in the aggregate, holds) a voting or economic interest of 5% or greater in the entity is (1) a foreign national who is a national of one or more excepted foreign states (and is not also a national of any foreign state that is not an excepted foreign state); (2) a foreign government of an excepted foreign state; or (3) a foreign entity that is organized under the laws of an excepted foreign state and has its principal place of business in an excepted foreign state or in the United States; and
- The “minimum excepted ownership” of the entity is held, individually or in the aggregate, by one or more persons each of whom is (1) not a foreign person; (2) a foreign national who is a national of one or more excepted foreign states (and is not also a national of any foreign state that is not an excepted

foreign state); (3) a foreign government of an excepted foreign state; or (4) a foreign entity that is organized under the laws of an excepted foreign state and has its principal place of business in an excepted foreign state or in the United States.

Regarding the last condition, the proposed rule defines the “minimum excepted ownership” with respect to an entity whose equity securities are primarily traded on an exchange in an excepted foreign state or the United States as “a majority of its voting interest, the right to a majority of its profits, and the right in the event of dissolution to a majority of its assets.” For all other entities, the applicable threshold for each of these is 90%.

In the event that an excepted investor fails to meet certain of these criteria in the three years following the completion date of a transaction, CFIUS may file an agency notice with respect to the transaction within one year following the completion date of the transaction, or up to three years afterwards in extraordinary circumstances. Additionally, regardless of whether a foreign person meets each of the conditions listed above, a foreign person will not be treated as an excepted investor if the foreign person or any of its parents or subsidiaries has, in the previous five years, engaged in criminal conduct or violated any U.S. foreign investment, sanctions, or export control laws or is listed on BIS’s Unverified List or Entity List.

**Other Exceptions.** In order to fall within the definition of “covered investment,” the investment must be made in an “unaffiliated TID U.S. business.” Thus, an investment by a foreign person in a TID U.S. business will not be treated as a covered investment subject to CFIUS’s jurisdiction if the foreign person already directly holds more than 50% of the outstanding voting interest in the TID U.S. business or has the right to appoint more than half of the members of the TID U.S. business’s board of directors or equivalent governing body. Investments involving air carriers are also excluded from the definition of “covered investment.”

**Specific Clarification for Investment Funds.** In accordance with FIRRMA, the proposed rule clarifies that an indirect investment by a foreign person in a TID U.S. business through an investment fund that affords the foreign person (or a designee of the foreign person) membership as a limited partner or equivalent on an advisory board or a committee of the fund will not be considered a covered investment with respect to the foreign person if the following criteria are met:

- (1) The fund is managed exclusively by a general partner, a managing member, or an equivalent;
- (2) The foreign person is not the general partner, managing member, or equivalent;
- (3) The advisory board or committee does not have the ability to approve, disapprove, or otherwise control (i) investment decisions of the investment fund; or (ii) decisions made by the general partner, managing member, or equivalent related to entities in which the investment fund is invested;
- (4) The foreign person does not otherwise have the ability to control the investment fund, including, without limitation, the authority (i) to approve, disapprove, or otherwise control investment decisions of the investment fund; (ii) to approve, disapprove, or otherwise control decisions made by the general partner, managing member, or equivalent related to entities in which the investment fund is invested; or (iii) to unilaterally dismiss,

prevent the dismissal of, select, or determine the compensation of the general partner, managing member, or equivalent;

(5) The foreign person does not have access to material nonpublic technical information as a result of its participation on the advisory board or committee; and

(6) The investment does not afford the foreign person any of the access, rights, or involvement specified in the definition of “covered investment.”

### **Declarations**

In addition to the provisions governing non-controlling investments in technology, infrastructure, and data companies, the proposed rule includes new provisions governing voluntary and mandatory declarations.

***Voluntary Declarations.*** FIRRMA allowed parties to a covered transaction to submit short-form “declarations” in lieu of a more detailed written notice. Parties are currently permitted to submit declarations only for pilot program covered transactions as part of CFIUS’s critical technology pilot program. The proposed rule will broaden this to allow parties to submit a declaration for any covered transaction. CFIUS will review declarations within a 30-day assessment period (in contrast to the 45-day review period for notices), and CFIUS may invite the parties to a covered transaction to attend a meeting with CFIUS staff to discuss and clarify any issues pertaining to the transaction as part of its review.

***Mandatory Declarations for Investments by Foreign Governments.*** FIRRMA requires parties to submit a declaration with respect any covered transaction that results in the acquisition, directly or indirectly, of a “substantial interest” in a TID U.S. business by a foreign person in which a foreign government has, directly or indirectly, a “substantial interest.” The proposed rule implements this requirement and defines “substantial interest” as (1) a direct or indirect voting interest of 25% or more by a foreign person in a U.S. business and (2) a direct or indirect voting interest of 49% or more by a foreign government in a foreign person. Parties may comply with this mandatory filing requirement by submitting a notice in lieu of a declaration. The filing must be submitted at least 30 days prior to the completion date of the transaction. This contrasts with the current 45-day requirement for mandatory filings submitted under CFIUS’s critical technology pilot program. Failure to comply with the mandatory filing requirement may subject parties to a civil penalty of \$250,000 per violation or the value of the transaction, whichever is greater.

***Mandatory Declarations Under CFIUS’s Critical Technology Pilot Program.*** The proposed rule does not make any changes to CFIUS’s critical technology pilot program, which imposes a mandatory filing requirement for certain transactions involving investments by foreign persons in U.S. businesses that produce, design, test, manufacture, fabricate, or develop one or more critical technologies. The proposed rule notes that CFIUS is still considering whether to retain the mandatory filing requirement for pilot program covered transactions and that CFIUS expects to address comments filed on the pilot program interim rule when it publishes the final rule for part 800.



## **Other Provisions**

**Filing Fees.** The proposed rule does not address CFIUS's new authority under FIRRMA to assess and collect filing fees for covered transactions that are submitted through a written notice. The proposed rule notes that Treasury is still considering how to implement this authority and that it will publish a separate proposed rule regarding filing fees at a later date. Under FIRRMA, filing fees may not exceed the lesser of \$300,000 or 1% of the value of the transaction.

**Incremental Acquisitions.** The existing regulations provide that "[a]ny transaction in which a foreign person acquires an additional interest in a U.S. business that was previously the subject of a covered transaction for which the Committee concluded all action under section 721 shall not be deemed to be a transaction that could result in foreign control over that U.S. business (*i.e.*, it is not a covered transaction)." The proposed rule clarifies that this incremental acquisition rule only applies to covered control transactions that are submitted through a notice and not to transactions submitted through a declaration or to covered investments (*i.e.*, non-controlling investments).

**Contents of declarations and voluntary notices.** The proposed rule requires that certain additional information be provided with declarations and voluntary notices, including a statement as to whether the foreign person will acquire any special access, rights, or involvement in the U.S. business as well as a description of whether the U.S. business's activities involve any critical technologies, critical infrastructure, or sensitive personal data.

**Finality of Action.** The existing regulations provide that, absent special circumstances, the President and CFIUS may not exercise authority over a covered transaction with respect to which the parties have submitted a written notice and have been advised by CFIUS in writing that CFIUS has concluded all action under section 721 with respect to the transaction. The proposed rule extends this safe harbor to transactions submitted through a declaration.

**Periodic Review and Revision.** Treasury anticipates that it will "periodically review, and as necessary, make changes to the regulations" given "the level of specificity provided in certain provisions of the proposed rule, the pace of technological development, the evolving use of data, and the evolving national security landscape more generally." In particular, Treasury will periodically review and may revise its definition of "sensitive personal data" and may also make changes to its list of covered investment critical infrastructure identified in the appendix to the proposed rule.