ALSTON & BIRD

WWW.ALSTON.COM

International Trade & Regulatory ADVISORY ■

AUGUST 2, 2018

CFIUS Reform Passes Senate Ushering in Expanded U.S. Investment Regime; New Export Controls on the Horizon

On August 1, 2018, nearly one year after Congress first introduced legislation to reform the Committee on Foreign Investment in the United States (CFIUS) review process, the Senate passed the Foreign Investment Risk Review Modernization Act (FIRRMA) by a vote of 87-10. It is expected that President Trump will sign the legislation in the coming days. FIRRMA, which is part of the National Defense Authorization Act for Fiscal Year 2019 (NDAA), was introduced to "modernize and strengthen" the statute authorizing reviews of foreign investment by CFIUS. Also included in the NDAA is the Export Controls Act of 2018 (ECA), which codifies existing export control regulations and promises new controls on "emerging and foundational technologies." In its final form, FIRRMA expands CFIUS's jurisdiction, provides for short-form filings, makes filing mandatory in some cases, authorizes the imposition of filing fees for the first time, and codifies and clarifies many existing CFIUS practices.

FIRRMA

Expanded CFIUS jurisdiction

FIRRMA will expand the jurisdiction of CFIUS to cover additional investments. Current law authorizes CFIUS to review investments that result in foreign "control" of a "U.S. business." FIRRMA expands the scope of "covered transactions" (i.e., transactions subject to CFIUS's jurisdiction) to include new categories of transactions.

- **Certain "other investments" involving critical technologies, critical infrastructure, and sensitive personal data of U.S. persons.** In addition to affirming CFIUS jurisdiction over transactions in which a foreign person acquires control of a U.S. company, FIRRMA subjects a new category of "other investments" to CFIUS jurisdiction. "Other investments" include non-controlling investments in U.S. companies involving critical technologies,[1] critical infrastructure,[2] and the sensitive personal data of U.S. persons that provide a "foreign person": (1) access to nonpublic technical information possessed by the U.S. business; (2) board membership

[1] "Critical technologies" includes "emerging and foundational technologies" identified through the new and enhanced export controls provided for under the ECA.

[2] FIRRMA defines "critical infrastructure" to mean "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."

or observer rights; or (3) any involvement, other than through voting shares, in substantive decision-making related to critical infrastructure, critical technologies, or sensitive personal data of U.S. citizens. CFIUS is directed to define "foreign person" for purposes of these investments to limit the provision's application. In doing so, FIRRMA will require CFIUS to consider "how a foreign person is connected to a foreign country or foreign government, and whether the connection may affect the national security of the United States." FIRRMA also specifically excludes from "other investments" indirect investment by a foreign person through investment funds or limited partnerships notwithstanding the foreign person's membership on the fund's advisory board or a committee fund when the fund is managed by a U.S. person and foreign limited partners have no control over the fund.

- **Real estate investments.** Pursuant to FIRRMA, CFIUS will have jurisdiction to review certain real estate transactions (including sales, leases, and concessions) that involve property located in close proximity to (or otherwise permitting surveillance of) sensitive U.S. government and military facilities, or which involve airports or maritime ports, except for real estate that is a "single housing unit" or located in an "urbanized area." Although CFIUS already reviews some of these transactions, FIRRMA will authorize CFIUS review of short-term leases or greenfield transactions where such transactions raise proximity concerns. The practical effect of this provision is not clear. As with "other investments" involving critical technologies, critical infrastructure, and sensitive personal data of U.S. persons, CFIUS must define the term "foreign person" to limit to the scope of real estate transactions subject to CFIUS review to investments by certain categories of foreign persons.
- **Changes in rights and transactions designed to circumvent CFIUS.** FIRRMA will give CFIUS jurisdiction over any changes in rights of an existing investment that would result in foreign control of the U.S. business.

Additional national security factors

Current law sets forth various factors that CFIUS may consider when conducting its national security analysis. Although FIRRMA does not modify or expand these factors, the "sense of Congress" in the bill's preamble suggests that CFIUS may consider additional factors in its national security analysis of a "covered transaction":

- The involvement of a "country of special concern that has a demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure that would affect" U.S. leadership in areas related to national security.
- The "potential national security-related effects" of the cumulative control of, or a "pattern of recent transactions" involving, any one type of critical infrastructure, energy asset, critical material, or critical technology by a foreign government or foreign person.
- The foreign person's history of complying with U.S. law.
- The control of U.S. industries and commercial activity by foreign persons as it affects the capability and capacity of the United States to protect its national security.
- Whether the transaction is likely to provide a foreign government with access to "personally identifiable information, genetic information, or other sensitive data" of U.S. citizens in a manner that threatens national security.

- The likelihood that the transaction will exacerbate or create new cybersecurity vulnerabilities in the United States or "is likely to result in a foreign government gaining a significant new capability to engage in malicious cyber-enabled activities against the United States."

Many of these factors already play a role in CFIUS assessments. As to the first factor regarding the involvement of "a country of special concern" with a "demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure," many observers believe Congress was primarily concerned with Chinese investment, which is already a focus of CFIUS scrutiny.

Changes to CFIUS review process

The vast majority of CFIUS reviews begin when the parties to a transaction submit a joint voluntary notice (JVN). Under current practice, parties are expected to submit a "draft" notice to CFIUS before the commencement of the official 30-day review period, which provides CFIUS and the parties with an opportunity to resolve any concerns about the draft and finalize the JVN. This informal review process has become a source of unpredictability for parties as the "prefiling" phase can drag on for several weeks. Once the 30-day initial review period ends, CFIUS may clear the transaction or initiate a 45-day investigation period. FIRMAA will alter the current process and practice resulting in reviews that may be shorter or longer.

- **Establishment of abbreviated notifications.** FIRRMA will create a new short-form filing or "declaration" that would allow parties to file an abbreviated notice of five pages or less at least 45 days before the completion of a transaction. CFIUS will be required to respond within 30 days by (1) clearing the transaction; (2) requesting that the parties file a formal notice; (3) informing the parties that CFIUS is unable to complete action based on the information provided and the parties may file a written notice; or (4) initiating a unilateral review of the transaction.

- **Requirement for mandatory filings.** Under current practice, most filings are voluntary. FIRRMA will require at least a declaration for investments involving access to U.S. critical technologies by foreign persons in which a foreign government owns, directly or indirectly, a substantial interest. The bill does not define "substantial interest," and instead directs CFIUS to define the term through regulations.

- **Changes to timeframe for review.** FIRRMA should create more certainty with respect to the pre-filing phase for parties that stipulate that a transaction is a "covered transaction" by requiring that CFIUS either accept a notice within 10 business days of submission or explain why a notice is incomplete. In addition, FIRRMA will lengthen the initial review period from 30 to 45 days, followed by, if necessary, one 15-day extension for "extraordinary circumstances."

- I**mposition of filing fees.** Currently, there is no fee to notify a transaction to CFIUS. FIRRMA will authorize CFIUS to charge a fee not to exceed the lesser of 1 percent of the value of the transaction or $300,000.

- **Judicial review of CFIUS decisions.** FIRRMA will require that a civil action challenging a CFIUS action or finding be brought in the U.S. Court of Appeals for the District of Columbia Circuit.

Increased authority for transactions posing national security concerns

FIRRMA will update current procedures available to CFIUS for dealing with transactions raising national security concerns, though in many instances these updates merely codify existing CFIUS practice.

- **Process for identifying non-notified, non-declared transactions.** FIRRMA will formalize CFIUS's practice of searching for and identifying non-notified transactions and requiring those parties to file a notice.
- **Authorization for mitigation measures for voluntarily abandoned transactions.** FIRRMA will authorize CFIUS to impose mitigation conditions to effectuate abandonment on any party to a covered transaction that has voluntarily abandoned the transaction.
- **Authorization to impose mitigation measures for completed transactions during pendency of review.** FIRRMA will authorize CFIUS to impose interim mitigation measures to address a national security risk pending completion of the review and/or investigation of a completed transaction.
- **Codification of CFIUS authority to suspend transactions and refer transactions to the President.** FIRRMA will authorize CFIUS to suspend a proposed or pending covered transaction that may pose a national security threat while CFIUS review or investigation is ongoing.
- **Increased mitigation oversight.** The use of independent monitors is explicitly authorized under FIRRMA, which is consistent with existing CFIUS practice. In addition, FIRRMA will require CFIUS to maintain a compliance plan for covered transactions that require mitigation.
- **Periodic review of mitigation agreements.** FIRRMA will require CFIUS to periodically review the appropriateness of mitigation agreements and take action to terminate or amend a mitigation agreement if a threat no longer requires mitigation.

ECA

Early versions of FIRRMA would have subjected outbound transfers of intellectual property and associated support to CFIUS review. This approach was strongly opposed by the U.S. technology industry and jettisoned from the final bill. Instead of making such transactions subject to CFIUS review, the NDAA provides for expanded controls for "emerging and foundational technologies" that are "essential" to U.S. national security, pursuant to the Export Controls Act of 2018 ("ECA"). In addition, the ECA repeals and replaces the lapsed Export Administration Act of 1979, which is the basis for U.S. export controls and has been continued since its expiration by the International Emergency Economic Powers Act (IEEPA).[3]

The ECA directs the President, in coordination with the Secretaries of Commerce, Defense, Energy, and State, to establish a "regular, ongoing interagency process to identify" technologies that should be subject to export controls established by the Department of Commerce ("Commerce"). This interagency process appears intended to fill a perceived gap between current export regulations and technologies that the U.S. government considers highly sensitive but that are not yet subject to export restrictions. It is not yet clear how the process contemplated will differ substantively from similar activities already undertaken by the agencies or how the outcome of the newly contemplated interagency process will be projected to the private sector.

The ECA directs the Secretary of Commerce to take into account the potential end uses and end users of the technology as well as countries to which exports from the United States are restricted in determining the

---

[3] The ECA largely codifies the Commerce's current practices regarding controls on "dual-use" items with both civilian and military applications via the EAR as well as existing authorities and procedures by which Commerce regulates the export, re-export, and in-country transfer of items for national security and foreign policy reasons. The law also codifies the civil and criminal penalties for violations of export controls established under the IEEPA.

appropriate level of control. Such considerations are already deeply embedded in the EAR, but the identification of emerging and foundational technologies that are essential to U.S. national security and the definition of such items in regulations will be important to the business community. The history of export regulations and the reform of those regulations teaches that the introduction of proposed new controls can unintentionally capture a wider swath of items and, therefore, impact the business plans and compliance management efforts of companies in multiple sectors. At a minimum, the ECA will require a license before any such technologies are transferred to a country subject to an arms embargo, which would include technology transfers to China.

The ECA will also authorize the Secretary of Commerce to compel various disclosures by certain applicants for licenses or other authorization for the export, re-export, or in-country transfer of emerging and foundational technologies. Applications submitted by or on behalf of a "joint venture, joint development agreement, or similar collaborative arrangement" may be required "to identify, in addition to any foreign person participating in the arrangement, any foreign person with significant ownership interest in a foreign person participating in the arrangement."

The ECA will leave some discretion to the Secretary of Commerce in deciding whether to impose export controls on emerging and foundational technologies. The ECA explicitly states that the Secretary of Commerce is not required to impose controls on the export, re-export, or in-country transfer of emerging and foundational technologies in a number of ordinary-course commercial transactions that would not result in the transfer of technical knowledge to foreign persons:

- The "sale or license of a finished item and the provision of associated technology" if the U.S. person "generally makes the finished item and associated technology available to its customers, distributors, or resellers."
- The "sale or license to a customer of a product and the provision of integration services or similar services" if the U.S. person "generally makes such services available to its customers."
- The "transfer of equipment and the provision of associated technology to operate the equipment if the transfer could not result in the foreign person using the equipment to produce critical technologies."
- The procurement by the U.S. person of "goods or services, including manufacturing services, from a foreign person … if the foreign person has no rights to exploit any technology contributed by the [U.S.] person other than to supply the procured goods or services."
- Any "contribution and associated support" by a U.S. person to "an industry organization related to a standard or specification, whether in development or declared."

The ECA will require Commerce to consider the impact of a proposed export on the U.S. "defense industrial base" in issuing export licenses and deny any request that would have "a significant negative impact" on the defense industrial base. License applicants will be required to provide information on the impact of the proposed export on the defense industrial base in their applications.

You can subscribe to future ***International Trade & Regulatory*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Jason M. Waite
202.239.3455
jason.waite@alston.com

Kenneth G. Weigel
202.239.3431
ken.weigel@alston.com

Thomas E. Crocker
202.239.3318
thomas.crocker@alston.com

Jon M. Fee
202.239.3387
jon.fee@alston.com

Anthony M. Balloon
404.881.7262
tony.balloon@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Helen Su
650.838.2032
helen.su@alston.com

Uni Li
202.239.3236
+86.10.85927501
uni.li@alston.com

James Burnett
202.239.3364
james.burnett@alston.com

Anna Karass
202.239.3515
anna.karass@alston.com

M. Jason Rhoades
202.239.3090
jason.rhoades@alston.com

Chunlian Yang
202.239.3490
lian.yang@alston.com

Derek Zotto
202.239.3017
derek.zotto@alston.com

ALSTON & BIRD

WWW.ALSTON.COM