Skadden

CFIUS' First Full Year Under FIRRMA

Partners

Michael E. Leiter / Washington, D.C.

Ivan A. Schlager / Washington, D.C.

Counsel

Daniel J. Gerkin / Washington, D.C.

Associates

Katie Clarke / Washington, D.C.

Nathan L. Mitchell / Washington, D.C.

Michelle A. Weinbaum / Washington, D.C.

This article is from Skadden's *2020 Insights*.

Four Times Square
New York, NY 10036
212.735.3000

The achievement of legislative consensus in 2018 around a preferred approach to safeguarding U.S. technology and information from national security threats via foreign investment resulted in passage of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA). Following the legislation and the associated adoption of two sets of rules by the Committee on Foreign Investment in the United States (CFIUS) to begin implementing the legislative vision, the focus shifted from the legislators to the activity of CFIUS itself.

In its first full year under FIRRMA, CFIUS has learned what works and does not work under its interim rules, clarified its increased jurisdiction and focus on transactions involving critical technology and infrastructure and sensitive personal data, and demonstrated a growing appetite for reviewing non-notified transactions (*i.e.*, transactions that are not voluntarily filed with the Committee) and enforcing mitigation agreements. In 2020, we expect general continuity of CFIUS practices, with an increased focus on China-related non-notified transactions; implementation of the final FIRRMA regulations (effective February 13, 2020) that will fill some regulatory gaps, including civil penalties, use of voluntary declarations and white-listed countries; and, likely most significantly, expanded mandatory CFIUS coverage via continuing export control reform.

Although CFIUS is a crucial and often-used tool in the U.S. government's broader efforts to protect U.S. technology, information, infrastructure and security from foreign actors, it is far from the only tool available. More specifically, as the U.S. government has pursued a "decoupling" of the U.S. and China — particularly as it relates to sensitive U.S. technology — Congress and the executive branch have pursued numerous related but distinct initiatives. Export control reform, greater scrutiny of export control licenses, executive orders related to specific Chinese actors and broader review of foreign technology in U.S. information and communications technology, limits on the U.S. government's use of technology from certain foreign providers and aggressive use of more traditional trade instruments all combine to significantly complicate cross-border business, investments and supply chains. In this light, CFIUS and other developing initiatives likely will remain central to investors and businesses through 2020 and beyond.

Safeguarding Critical Technology: FIRRMA's Pilot Program and Mandatory Filings

In October 2018, CFIUS implemented FIRRMA's Pilot Program for critical technology transactions, which effectuated both the Committee's expanded jurisdiction to review certain noncontrolling investments that involve information rights for minority investors and its new authority to direct that certain filings — for the first time ever — be mandatory. (See "US Finalizes CFIUS Reform: What It Means for Dealmakers and Foreign Investment" and "CFIUS Pilot Program Expands Jurisdiction to Certain Noncontrolling Investments, Requires Mandatory Declarations for Some Critical Technology Investments.") With the release of the final regulations, CFIUS clarified that the Pilot Program in its current form remains in effect through February 12, 2020. Beginning February 13, 2020, the Pilot Program will, in substance, remain in effect, but will be fully integrated within the CFIUS final regulations. Thus, mandatory filings for controlling and certain noncontrolling investments in critical technology remain,

and they have in fact been expanded to certain foreign government-related transactions in businesses involving critical infrastructure and sensitive data. What remains uncertain — although CFIUS' general intent is clear — is exactly how CFIUS will modify the current NAICS-code based mandatory filing requirements and implement a filing requirement based solely on export control considerations. (According to the preamble to the final rule, Treasury anticipates issuing a separate notice of proposed rulemaking that would effectively eliminate the association between "critical technologies" and the 27 industries previously identified as sensitive. Rather, the mandatory filing requirement would be triggered by export licensing requirements alone.)

Thus far, the mandatory filing requirement has impacted both deal diligence and timing for many implicated transactions. In particular, technology-focused funds and early-stage investors have confronted a disconnect between a fast-moving investment environment in the early-stage technology sector and the delays inherent to a CFIUS review. CFIUS sought to address delays by creating a short-form declaration and providing alternative results to approve or block a transaction, but investors encountered mixed results in terms of both timing and certainty. CFIUS has yet to publish statistics on the declaration process but has made informal comments to the effect that, although a significant number of declarations have been submitted, they often do not provide investors with the "safe harbor" that results from formal CFIUS approval of a transaction. In other cases, filing a short-form declaration has resulted in CFIUS requesting that the parties file a full notice, extending the length of the CFIUS process. Accordingly, parties should consider filing a full notice for a Pilot Program transaction at the outset, in lieu of a short-form declaration, or should carefully structure the transaction (*e.g.*, by limiting governance or information rights) such that a mandatory filing is not required. In 2020, short-form declarations may prove much more helpful once CFIUS implements rules permitting parties to use them for voluntary filings for less sensitive transactions, and not just for mandatory critical technology filings.

Emerging and Foundational Technologies: Ongoing Reform Means Continued Uncertainty

The Pilot Program compelled U.S. companies to pay closer attention to, and often to become more educated about, the export control classifications of their products, services and technology — a task made more difficult by ongoing export control reform. (See "Tightened Restrictions on Technology Transfer Under the Export Control Reform Act.") In November 2018, the Department of Commerce (Commerce)

Key Takeaways for 2020 and Beyond

- The vast majority of CFIUS filings will remain voluntary, and important considerations remain for voluntarily filing, including CFIUS' expanded jurisdiction and increased attention to non-notified transactions.
- CFIUS' jurisdiction and sensitivity will remain aligned with export control laws, and both foreign investors and U.S. companies considering business combinations should develop or maintain fundamental competency in the subject area.
- CFIUS is expected to have greater resources and appetite for enforcing mitigation agreements; therefore, companies must prioritize understanding and complying with both new and existing agreements.
- CFIUS' increasing interest in companies that collect U.S. citizen information is likely to result in increased mitigation to shield foreign investors from accessing that information.
- Parties contemplating covered transactions in the information and communications technology sector should expect more focus on supply chain restrictions and vendor review in potential mitigation agreements.
- The Committee remains primarily concerned with the national security threats posed by China, and thus both Chinese investors and non-Chinese investors with significant Chinese connections are likely to be subject to increased scrutiny.
- The majority of CFIUS' requirements will continue to apply to "excepted investors" from "excepted countries" even if CFIUS establishes, as expected, a "white list" of such investors and countries.

published an advance notice of proposed rulemaking to solicit comments on the criteria it will use to identify "emerging" technologies. Emerging technologies fall into representative categories that include artificial intelligence and machine learning, quantum computing, robotics, nanotechnology and biotechnology, among others. Commerce has yet to publish specific proposed rules for emerging technologies — newly developed technologies such as artificial intelligence, machine learning, autonomous vehicle technology or robotics that are not already captured by existing export controls — or an advanced notice of proposed rulemaking regarding "foundational" technologies — meaning technologies currently subject to existing export controls that are only controlled for anti-terrorism reasons, and which are therefore generally freely exportable to all but U.S.-embargoed destinations. However, we expect gradual rulemaking on this front throughout 2020. (See "Commerce Department Will Move Forward With More Stringent Export Controls for Certain Emerging Technologies" for additional insight into the proposed emerging technologies rules.) Both technologies are explicitly included in CFIUS' definition of "critical technology" and thus potentially implicate mandatory filing requirements and impact CFIUS' view of the risk associated with affected transactions.

Non-Notified Transactions: Increasing Scrutiny

Before FIRRMA, CFIUS had the authority to review non-notified transactions; however, its resources were limited. The number of voluntarily filed transaction notices continues to increase, with over 200 filed in 2017, over 230 in 2018 and over 240 in 2019 (not including additional short-form declarations filed in the past year). FIRRMA granted CFIUS increased hiring authority, permitting it to build up its capacity and allowing certain staff members to spend more time strictly focused on non-notified transactions. Over the past year CFIUS demonstrated an increased emphasis on this category, which tends to generate dramatic outcomes, including its authority to unwind transactions. This was demonstrated in Beijing Kunlun Wanwei Technology's acquisition of a stake in Grindr — a company that collects personal user data including sexual orientation, HIV status and photos — in which CFIUS initiated and ultimately ordered Kunlun to divest its interest; and PatientsLikeMe's acquisition by iCarbonX — a Chinese digital health company — in which CFIUS similarly forced iCarbonX to divest its interest. These divestments demonstrate both CFIUS' willingness to review completed transactions and force divestiture when it finds a national security concern and its increasing focus on deals that involve sensitive data about U.S. persons, such as health, genetic and other general information. Given CFIUS' increased focus on non-notified transactions, and its willingness to force divestitures of completed transactions to address its concerns, companies should carefully weigh the effects a voluntary filing will have on deal certainty and timing against the sensitivity of the transaction and the likelihood CFIUS may take an interest. This becomes most important when investments have a nexus — either direct or indirect — to China or Russia, or involve especially sensitive technology or information. As both above-cited cases illustrate, CFIUS' definition of what makes a transaction sensitive goes far beyond traditional government-related technologies and information.

National Security Agreements: Evolving CFIUS Practices

FIRRMA granted CFIUS broader powers to mitigate threats to national security. For example, CFIUS can suspend a transaction during its review or call for interim mitigation before completing review, and CFIUS may unilaterally open a review for any breach — even if unintentional — of a mitigation agreement. In April 2019, for the first time ever, CFIUS imposed a $1 million civil penalty for repeated breaches of a 2016 CFIUS mitigation agreement, citing its "commitment to enforcement." Later in 2019, CFIUS imposed a $750,000 civil penalty for violations of a CFIUS interim order related to data access and monitoring. CFIUS' increased hiring authority is likely to correspond to greater attention to negotiating and enforcing mitigation agreements in 2020; such agreements may involve — among other measures — limitations on governance and information rights, supply chain assurances, cyber and data security requirements, supply assurances to the U.S. government, security monitoring and annual audits. Given CFIUS' growing appetite for enforcement, companies must carefully consider their future ability to comply when entering into a new agreement. Companies operating under mitigation should consider allocating resources to prioritize and ensure ongoing compliance.

China-Related Investments: No Relief in Sight

Despite tense ongoing trade negotiations, most notably with China, the U.S. government has strictly maintained that the country remains open to foreign investment — a sentiment CFIUS representatives have echoed publicly. But CFIUS and a number of federal agencies also have continued to articulate strong concerns about both the legal and illegal transfer of U.S. technology and data to China — a worry that was the principal motivating factor behind FIRRMA's enactment. A number of recent public enforcement actions have targeted Chinese companies, such as CFIUS' forced divestments of Grindr and PatientsLikeMe, and in other contexts, such as with the $1 billion fine ZTE was required to pay under its

settlement agreement in connection with export violations. Although CFIUS approved some deals involving China in 2019, the harsh scrutiny and increased likelihood of either heavily mitigated or blocked transactions coincided with a noticeable downturn in Chinese foreign direct investment. CFIUS' concerns about China extend to joint ventures as well. Even before FIRRMA, CFIUS had the jurisdiction to review technology transfers to China through joint ventures, and CFIUS' focus on and skepticism of these arrangements has continued. Accordingly, non-Chinese investors should continue to carefully consider the terms of their existing joint venture agreements, as well as the ultimate sources of any co-investment funds they may use when entering into a transaction.

Final Rules: Greater Definitiveness and Possible Changes in 2020

In September 2019, CFIUS issued two sets of proposed regulations seeking to further implement FIRRMA, and, on January 13, 2020, CFIUS issued final FIRRMA regulations effective February 13, 2020. (See "Draft CFIUS Regulations Portend Evolution, Not Revolution.") Among other things, these rules codified CFIUS' expanded jurisdiction over noncontrolling investments in, and increasing attention to, businesses involving critical technology, infrastructure or bulk U.S. personal data — "TID U.S. Businesses." The final rules address most of FIRRMA's mandated changes, including the following key highlights:

- **Technology U.S. Businesses.** As noted above, the final rules clarify that CFIUS will maintain the mandatory filing regime for entities in this category. The most significant changes yet to come in this realm will be Commerce's release of defined "emerging and foundational technologies" and future rulemaking to replace the industry-based filing criteria with one focused on export control licensing requirements.
- I**nfrastructure U.S. Businesses.** The final rules clarify CFIUS' focus on Infrastructure U.S. Businesses, which will be defined through the functions a U.S. business performs in relation to critical infrastructure. For example, covered critical infrastructure includes telecommunications services, a particular focus of the U.S. government over the past year, and the final rules implicate U.S. businesses that supply or service telecommunications infrastructure. (See "Commerce Department Takes Steps To Thwart Use of Information and Communications Technology and Services Associated With Foreign Adversaries.") Parties contemplating covered transactions in the telecommunications industry should expect more focus on supply chain restrictions and vendor review in potential mitigation agreements.
- **Data U.S. Businesses.** Motivated by concerns that foreign governments may influence foreign parent companies to directly access U.S. personal data, the final regulations define Data U.S. Businesses in a way that affects a wide range of companies that likely would not have considered themselves to be of interest to CFIUS. This is in part because CFIUS has prospectively defined personally "identifiable data" to include all data that "can be used to distinguish or trace an individual's identity" when it is not aggregated or otherwise anonymized. While CFIUS has limited the definition to apply to businesses that have collected or maintained data on over 1 million individuals (or have demonstrated an objective to do so), in practice this requirement does little to narrow CFIUS' scope. Examples added to the final regulations confirm CFIUS' expansive scope, for example, stating that the time period for demonstrating a business objective to maintain or collect sensitive data from 1 million individuals could extend out to at least two years. Foreign investors will want to expand their diligence regarding how a U.S. business collects, stores and protects its U.S. personal data when considering a new transaction. Conversely, sellers will be interested in a potential purchaser's history of data-related compliance and practices. Importantly, CFIUS has shown an interest in all data, not just identifiable data that meets the definition for a TID U.S. Business, and this sensitivity to data can provide a hook for jurisdiction where CFIUS may have other concerns about a foreign investor.
- In addition to the primary set of rules that addresses TID U.S. Businesses, CFIUS issued a second set of rules to codify its expanded jurisdiction over real estate. Under FIRRMA, the Committee's jurisdiction includes certain stand-alone real estate deals that would not traditionally have been covered transactions. The final regulations focus primarily on real estate transactions that could provide a foreign person with proximity to airports and maritime ports or to military installations or other sensitive facilities or properties of the U.S. government. Like with Infrastructure U.S. Businesses, the final rules lack specificity, and investors will be looking to see how CFIUS asserts its jurisdiction in practice once the rules are published. The Committee anticipates providing a web-based tool for the public to better understand the geographic coverage of the final regulations. Investors should remain cognizant, however, that CFIUS' expanded jurisdiction over real estate transactions does not preclude the Committee from exercising jurisdiction over transactions that involve could result in foreign control or certain non-controlling investments by a foreign person in an entity engaged in interstate commerce that also owns or leases real estate.

CFIUS 'White List'

One of the more widely anticipated changes under the final rules was clarification of whether and how CFIUS would establish the "white list" to exempt certain foreign investors from filing requirements for their noncontrolling investments in TID U.S. businesses. Under FIRRMA, CFIUS was directed to specify criteria to limit its application of expanded jurisdiction to certain categories of foreign persons. In its final rules, CFIUS addressed this by creating a set of "excepted foreign states" to receive special treatment; excepted investors, in turn, must be from "excepted foreign states." CFIUS' initial list includes Australia, Canada and the United Kingdom — three countries that share extremely close intelligence and foreign investment review relationships with the United States.

Perhaps most importantly, the expected benefit to these "excepted investors" is likely to be small because the white list will not exempt foreign investors from CFIUS' jurisdiction in controlling transactions. In essence, meeting the "excepted investor" criteria exempts certain Australian, Canadian and U.K. investors from CFIUS' expanded jurisdiction, but does nothing to remove their investments from the Committee's traditional jurisdiction over transactions in which the foreign person obtains a controlling interest in a U.S. business. Further, although inclusion as an excepted investor can suggest that CFIUS views a foreign investor as a relatively lower-threat acquirer, a filing may be warranted if the acquired asset is particularly sensitive to U.S. national security. Given these limitations, we expect the white list likely will have limited practical effect for investors.