LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Deal Maker's Guide To The New CFIUS Framework

By **Charles Comey, Charles Capito and Jim Ryan**

(February 13, 2020, 4:37 PM EST) -- It seems there's never a dull moment in the U.S.-China bilateral relationship. Public markets relaxed following easing tensions in the trade war with China with the announcement of the parties' Phase I trade agreement, signed on Jan. 15.

Charles Comey

But continued strategic decoupling in the wake of the U.S. Department of Justice indictments of Chinese People's Liberation Army members for the 2017 Equifax hack, and the proliferation of confirmed coronavirus cases worldwide, has re-tightened macroeconomic concerns across the U.S. and other global markets.

Against this fraught backdrop, at the policy level, the U.S. government continues to focus on foreign investment into, and the prevention of transfer of sensitive technology and resources out of, the United States.

Charles Capito

The latest suite of U.S. national security regulations on cross-border investment and acquisitions signals policymakers' ongoing efforts to balance the need to address the strategic challenges presented by China's global expansionism and by other threat actors, on the one hand, with maintaining an open and vibrant international investment environment, on the other.

On Jan. 13, the Committee on Foreign Investment in the United States published final regulations to implement the Foreign Investment Risk Review Modernization Act, or FIRRMA. The regulations took effect on Thursday.

Jim Ryan

Here's an overview of the key questions deal makers should be asking to assess whether CFIUS must, or should be, notified of a transaction under the new rules.

Who are the parties?

A seemingly simple but critical question highlighted by the new CFIUS regulations is — are both a foreign investor and a U.S. business involved?

On the sell side, the test for whether there is a U.S. business for CFIUS purposes is simply whether the target entity is engaged in interstate commerce in the United States, meaning, in most cases, does the business have U.S.-based revenues or assets? The business, for these purposes, includes both U.S. subsidiaries and branches of non-U.S.-based companies.

Where the target is incorporated, the nationality of its management and owners, and the relative magnitude of its U.S. business, however, aren't relevant for this prong of the CFIUS jurisdiction test. The U.S.-business test here means that even targets that may not regard themselves as U.S. companies could trigger a CFIUS review when put up for sale.

Assuming the target is or has a U.S. business, the focus then shifts to the buy side, where the investor's/buyer's country of origin is key, since not all countries are treated alike under the new regulations. The inquiry runs as follows:

Is the buyer a foreign person for CFIUS purposes?

For CFIUS, foreign persons include any foreign national, government, or entity or entities over which a foreign national, government, or entity exercises or could exercise control. This means that a Delaware-registered investment fund would be foreign if controlled by foreign parties, while a Cayman vehicle controlled by U.S. citizens would not be, unless foreign owners/limited partners hold special management or other rights.

Since the question is one of ultimate beneficial ownership and control, transaction parties need to look through layers of corporate ownership to analyze who actually owns and controls the investor/buyer entity.

Once the entity or entities that control the investor/buyer are identified, the next step is to determine if the entity is a foreign entity. Parties need to look beyond the jurisdiction of formation or registration and instead undertake a more in-depth analysis based on the entity's principal place of business, and, for publicly-traded companies, the exchange on which its shares are traded.

The final regulations look at where the investor's/buyer's management directs, controls or coordinates its activities.

What about specific countries?

For years, practitioners and the investment community have generally understood that, in practice, not all countries are treated the same by CFIUS, but CFIUS' jurisdiction has not, until now, been expressly affected by an investor's nationality. The new rule includes a short list of friendly allied nations — Australia, Canada and the United Kingdom.

Certain investors from these excepted foreign states are exempt from CFIUS review for minority noncontrol investments. CFIUS has indicated it will review and periodically update this list over time, and that the currently excluded countries will also be assessed for continuing eligibility after two years.

What is the nature of the target's technology and business?

As with an investor's nationality, not all technologies and businesses are treated the same for CFIUS purposes. The final regulations emphasize the strategic importance of U.S. businesses that involve critical technologies, critical infrastructure, sensitive personal data (the so-called TID U.S. businesses), and certain real estate transactions.

Consequently, transaction parties should closely review the target's business, technologies and operations, including the amount and nature of personally identifiable data of U.S. citizens that the business aggregates, if any, to assess the transaction's CFIUS risk profile.

Are critical technologies involved?

The definition of critical technologies remains unchanged from the CFIUS pilot program, which the new rules supersede.

The analysis remains focused principally on how the U.S. business' technologies are classified for export control purposes, including the yet-undefined category of emerging and foundational technologies. The U.S. Department of Commerce has been working on defining emerging and foundational technologies since the passage of FIRRMA, but has not yet announced when the new regulations will be issued.

One change announced in the final regulations is that CFIUS anticipates a new rule that will shift from defining critical technology U.S. businesses based on their North American Industry Classification System, or NAICS, codes, and instead base the analysis solely on export licensing requirements. This expected change is designed to make deal parties' risk analysis easier (since export control codes are generally perceived as more precise than currently used NAICS codes).

In the meantime, parties should consider whether the target's business falls within any of the broad categories of emerging technologies. The most-talked about technology on this front is artificial intelligence, but the scope is broad and includes certain types of biotechnology, microprocessor technologies (e.g. systems-on-chip and stacked memory on chips), data analytics, quantum information and sensing technology, additive manufacturing (e.g. 3D Printing), and advanced materials (e.g. advanced fiber and fabric technology, and biomaterials).

Does the target operate critical infrastructure?

The new rules also regulate certain noncontrolling investments in critical infrastructure, that is, U.S. businesses that perform critical infrastructure functions including internet protocol networks and exchange points, data centers and core processing services for federal financial institutions. Such investments are covered transactions and, therefore, notifiable to CFIUS.

Does the target aggregate and store sensitive personal data?

The questions to confirm here are whether the target tailors its 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; and whether the target has collected or has an objective to collect personally identifiable data on more than one million individuals.

The type of information CFIUS is concerned with here ranges from financial data to physical, mental, or psychological health information, to geolocation data. Prior to the new rules, CFIUS' concerns over transactions that resulted in foreign control of personally identifiable data were evident in the Grindr LLC and PatientsLikeMe divestiture orders. These are but two recent public examples of the committee's increasingly activist approach to reviewing and rectifying nonnotified transactions where it perceives risks to U.S. national security.

Is sensitive real estate involved?

The new regulations expand CFIUS' jurisdiction over real estate transactions, including leases as a new category of potentially covered transactions. Covered real estate is determined by a property's proximity to sensitive government sites, including certain airports, maritime ports and military installations.

The rule includes numerous exceptions, so parties should review not only the nature and location of the property involved, but also the intended uses of the property (residential, retail sales, heavy industry, etc.), whether the property is single or multi-tenant, and facts about the profile of the buyer.

Helpfully, CFIUS has announced it will make available a web-based tool to better illustrate the coverage of the new rule. For now, parties should consult sources such as TIGERweb, U.S. Department of Transportation lists of airports and maritime ports, and the U.S. Bureau of Ocean Energy Management to determine whether a property is covered under this new category.

What rights is the investor getting?

A common misconception of deal parties is what constitutes control for CFIUS purposes. Here, the threshold is very low in practice. Even investments for as little as 10% of a company's voting securities can constitute control.

Other than certain permitted passive minority investor rights (like blocking a sale of the company or amendments to a shareholder agreement), any right over matters like the disposition of a target's assets, changes to production, operational, or research and development, or selection of new business lines can result in a finding of control for CFIUS purposes.

Is the investment a covered investment?

Covered investments afford the foreign investor access to material nonpublic technical information of the target, membership or observer rights on the target's board of directors (or equivalent governing body), or any involvement in substantive decision-making of the U.S. business — for example in the form of influence or involvement related to critical technology, critical infrastructure or sensitive data.

How are contingent interests treated?

One helpful clarification in the final regulations is that contingent equity interests (such as purchase options) do not trigger a filing requirement until their exercise, assuming there isn't other earlier acquisition of control or the kinds of access, rights or involvement described in the regulations. Experienced acquirers were already operating on this basis prior to the final regulations, but the formal recognition gives additional helpful clarity.

Key Takeaways

Subject to certain exceptions, a mandatory filing is required for:

- Investments in a TID U.S. business or covered real estate transaction that give a foreign investor control of the U.S. business (as discussed above), board membership or observer rights, access to material nonpublic technical information, or involvement in substantive decision-making with respect to critical technologies; and

- Transactions where the foreign party is acquiring 25% of the U.S. target and where a foreign government has a direct or indirect voting interest of 49% or more in the foreign party.

Of course, a proposed transaction can still entail national security considerations even without a mandatory filing requirement, and parties should be careful to assess CFIUS risk in cases where, for

example, the target possesses personally identifiable data of U.S. citizens or may constitute a TID U.S. business.

In such cases, parties may wish to consider whether to take advantage of the new rules permitting the submission of short-form declarations in nonmandatory cases. This can add certainty to the decision about whether a filing is necessary (although at the expense of a 30-day delay in closing while CFIUS reviews the declaration).

The determination can be particularly meaningful for serial foreign acquirers of U.S. technology or life sciences businesses that entail national security sensitivities. We are in an era where not filing and assuming CFIUS risk is not recommended for acquirers wishing to demonstrate transparency and goodwill to the U.S. government as they continue to invest in the American market.

Although the published regulations are final, we expect that practices relating to CFIUS will continue to evolve and the U.S. government will continue to refine the CFIUS rules and regulations over time. Careful planning, accounting for further developments as they arise (including in connection with export control rule changes) and consulting with experienced counsel remain as crucial as ever for successful cross-border transactions.

Charles C. Comey and Charles L. Capito III are partners and Jim Ryan is an associate at Morrison & Foerster LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.