

CFIUS Jurisdiction Continues to Expand



Paul Marquardt
Partner
Washington, D.C.
pmarquardt@cgsh.com



John McGill, Jr.
Senior Attorney
Washington, D.C.
jmcgill@cgsh.com



Samuel Chang
Associate
Washington, D.C.
sachang@cgsh.com

In 2020, boards of directors will continue to face an evolving landscape in reviews of foreign investment by the Committee on Foreign Investment in the United States (CFIUS), particularly with respect to issues relating to technology, infrastructure and personal data. Boards, and Technology Committees in particular, should be aware of these developments for their possible ramifications for foreign investment.

On September 17, 2019, the US Department of the Treasury proposed regulations¹ implementing most of the remaining provisions of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which updated the statute authorizing CFIUS reviews of foreign investment. FIRRMA mandates that the final regulations enter into force by February 13, 2020.

Although the proposed regulations primarily codify CFIUS practice over the past decade, they underline CFIUS’s focus on foreign investment in businesses that develop critical technology, perform specified functions with respect to critical infrastructure and handle sensitive personal data of specified types and volumes (defined collectively in the proposed regulations as “TID US Businesses”):

- **Critical Technologies.** Unchanged from the 2018 critical technologies pilot program, “critical technologies” includes a wide range of export-controlled technologies, as well as “emerging and foundational technologies” to be controlled under the Export Control Reform Act of 2018 (which remain to be defined).

¹ For additional details on the Proposed Regulations, see our September Alert Memo [here](#).

- **Critical Infrastructure.** A business qualifies as a “critical infrastructure” TID US Business if it performs specified functions corresponding to particular types of infrastructure (including assets in the telecommunications, energy, financial services, transportation, manufacturing and defense sectors), as detailed in an appendix to the proposed regulations.
- **Sensitive Personal Data.** The regulations focus on data of US persons that is “identifiable” to an individual’s personal identity and that falls within one of 10 enumerated categories (including genetic, biometric, geolocation and certain health- and financial-related data). The relevant businesses are those that (i) “target or tailor” their products or services to US national security agencies or their personnel (including, for example, military discounts), (ii) maintain or collect covered data on greater than 1 million individuals, or (iii) integrate such data with the US business’ primary products or services and intend to serve more than 1 million US persons.

Under the proposed regulations, TID US Businesses are subject to a mandatory filing regime for entities linked to foreign governments (at least 49% owned by a foreign state, directly or indirectly) acquiring at least a 25% voting interest in the US business, subject to an exception for some passive investments through US funds. CFIUS’s already broad jurisdiction over any investment with substantial governance rights is even further expanded to cover observer rights and access to technical data or decisions (e.g., with joint R&D). Whether or not the new rules technically apply, TID US Businesses will continue to be an area of CFIUS focus.

The proposed regulations also expand CFIUS’s jurisdiction over real estate transactions involving certain property rights at airports, maritime ports or near a list of identified government locations.

Although the proposed regulations primarily codify CFIUS practice over the past decade, they underline CFIUS’s focus on foreign investment in businesses that develop critical technology, perform specified functions with respect to critical infrastructure and handle sensitive personal data of specified types and volumes.

Key Takeaways

In 2020, boards should:

- Identify the advisability or requirement to file a notification with CFIUS early in a transaction, assess the benefits and risks of voluntarily filing with CFIUS and consider structuring investments and acquisitions so as to mitigate CFIUS scrutiny.
- Be aware that CFIUS is now devoting significant resources to identifying and investigating transactions that are not voluntarily notified, particularly in early-stage technology companies.
- Bear in mind CFIUS risk as a potential constraint on strategic exits for both existing and new investments.