CFIUS: Three Trends to Know

MAY 2022

Scott Boylan
Partner, StoneTurn
sboylan@stoneturn.com
+1 202 349 1130

Nathan Fisher
Managing Director, StoneTurn
nfisher@stoneturn.com
+1 415 848 7613

by Scott Boylan & Nathan Fisher

The Committee on Foreign Investment in the United States (CFIUS) is a multi-agency arm of the US Government responsible for reviewing foreign investment into the US and assessing the potential risk or threat a given investment may pose to national security.

Given the inherent complexity of that charter, one should not be surprised to learn that CFIUS' powers and authorities have been redefined many times over the years – most recently in 2018 with the passage of the Foreign Investment Risk Review Modernization Act (FIRRMA), which further extended the reach of CFIUS' authorities across a greater number of industries and transaction types.

StoneTurn

CFIUS representatives and industry experts recently convened for the 8th annual ACI Conference on CFIUS to discuss recent trends and future forecasts. From those discussions, three critical takeaways stood out that must be understood by anyone facing a transaction with foreign partners or investment (and thus potentially a CFIUS review).

1 National Security Is....?

National security is purposefully undefined to provide CFIUS flexibility in addressing threats. When CFIUS was first formed in the mid-1970s, there were concerns about Arab investments in the US using their tremendous profits in the oil trade. Concerns later shifted to the emerging economic powerhouse of Japan which started investing heavily in the US. In the early years of CFIUS' existence, China and Russia were not even participants in the global economic system, but today they represent CFIUS' largest and most significant focus.

The first deal killed by a President under CFIUS authority was a Japanese attempt to purchase a silicon chip manufacturer. Foreign acquisition of chip manufacturers has been a consistent concern of CFIUS throughout its existence. Today, CFIUS has identified new technologies, assets, and nationalities as threats to US National Security, and the limitations of its reach are not explicitly defined. Per FIRRMA, CFIUS' authority expanded to include reviews of non-controlling investments, as well as certain real estate transactions. Further, FIRRMA put special focus on reviewing transactions involving US critical technology businesses – that is by CFIUS standards a US business involved in: critical Technology; critical Infrastructure; or sensitive personal Data (collectively known as "TID" US businesses). Some of these technologies are more easily identified as sensitive as they may already be tied to existing US export controls. But CFIUS is equally concerned with "emerging technologies," and that is a list continually growing as new products and capabilities are evaluated. Even if a transaction does not directly include a critical piece of technology, the target company's connection to such technologies, infrastructure, or even supply chain may subject it to CFIUS restrictions.

Similarly, transactions may also be judged according to the friends of your friends. That is to say, perhaps the foreign party of your transaction does not represent an adversarial foreign nation – but if they have their own close economic relationship with such, that third party connection could jeopardize your transaction.

It's Not Just Tech.

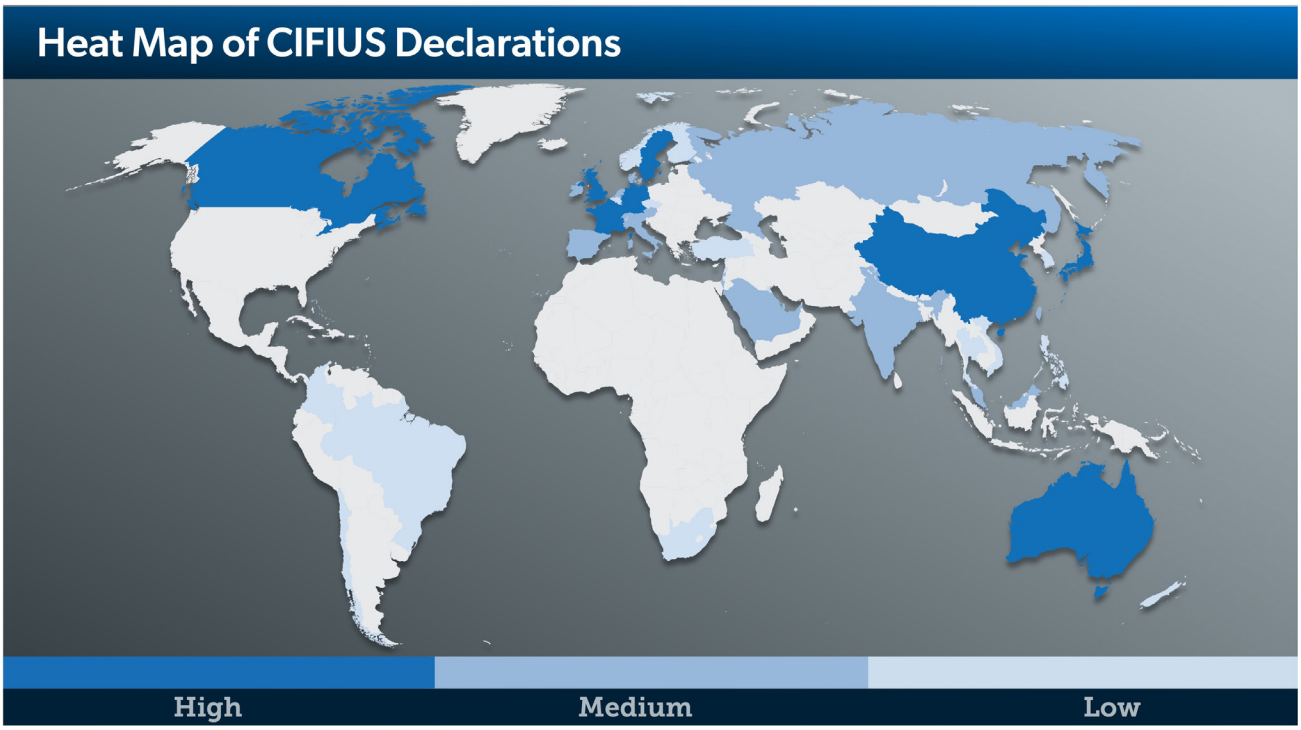
While **CFIUS** reviews of tech transactions have received considerable publicity, **any sector can be subject to notice, including:**

- Hospitality
- Social Media
- Food Production
- Real Estate
- Energy
- Aerospace
- Financial Services
- Utilities
- Manufacturing
- and More

2 Personal Data

Of all the assets a transaction may involve, CFIUS is increasingly concerned with access to personal data – especially that of US citizens and government employees. Regardless of the transaction company's industry, products, or operations, if the proposed transaction has the potential to empower a foreign entity with direct access to sensitive US person information, CFIUS will likely perform a review of the proposed transaction and may impose mitigation requirements or reject the transaction entirely. Though CFIUS has not published a definition of sensitive personal data, CFIUS has in some transaction reviews determined sensitive personal data to include names, addresses, email addresses, telephone numbers, dates of birth, and more obvious identifiers, such as social security numbers, medical records, and financial records. US companies involved in the collection, storage, or sharing of personal data may be designated by CFIUS as a TID US Business dependent on the nature of the personal data and the volume set with which they deal.

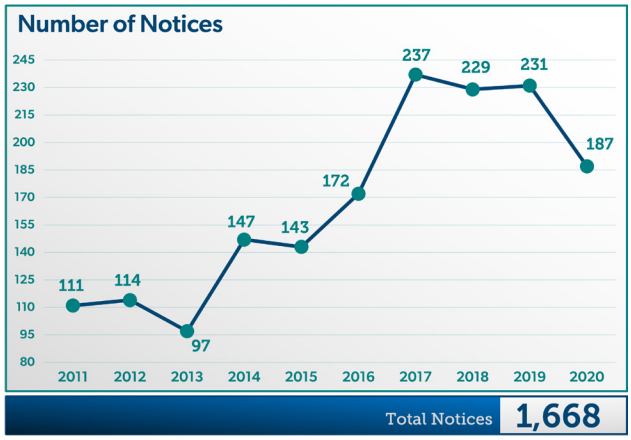
In many cases, transactions involving sensitive personal data have been successfully negotiated and approved with CFIUS by accepting certain mitigating controls. These controls can include separated US IT systems, enhanced security of data, and limiting access to only US-based US citizens.



StoneTurn

3 Non-notified Transactions

FIRRMA not only increased CFIUS's powers and reach, but also increased its resources. Many of those resources are increasingly being devoted to identifying non-notified transactions in which investors did not file an application with CFIUS but CFIUS believes that a national security risk is indeed presented by the transaction and thus requires that the parties file. Most often this occurs after the deal has already closed. CFIUS always had this power but heretofore has lacked resources to initiate these investigations at a large scale. Per the most recent available report, in 2020, CFIUS identified 117 non-notified transactions for mandatory filing.



CFIUS officials present at the conference acknowledged they are deliberately expanding this effort and allocating additional resources to source business intelligence and review an increased number of transactions. In fact, the Department of the Treasury Strategic Plan for 2022 – 2026 establishes one measure of success to be "Accelerated timelines for identification and processing of covered transactions that have not been voluntarily filed with CFIUS ("non-notified" transactions)."

It is never advantageous for a foreign investor to be asked to file by CFIUS. First, CFIUS believes that you were likely trying to circumvent the national security review process and their suspicions of malicious intent are significantly raised. There is a good likelihood that the investors will be required to unwind the transaction and if approved will likely result in a mitigation agreement with terms that are significantly more restrictive than if the investors had filed prior to completing the transaction.

It is far better to assess the potential need to file with CFIUS in the early stages of the transaction process, primarily through a thorough CFIUS-minded due diligence effort. There are many expert resources in this industry who can effectively help navigate this process and ensure you have a robust understanding of the following:

1. What constitutes a national security concern today? This changes constantly and can be influenced by daily events across the world.
2. What components of your deal (assets, parties, technologies) may give CFIUS reason to further review your proposal?
3. Mitigation terms are likely in many transactions. Anticipate what specific mitigations CFIUS may impose on your transaction and evaluate the transaction in that context.

StoneTurn

About the Author

Scott Boylan, a Partner with StoneTurn, has more than 30 years of experience in advising public- and private-sector organizations on a broad range of international legal and business issues, including trade compliance, investment security and government contracting. He has been involved in all aspects of the Committee on Foreign Investment in the United States (CFIUS), from negotiating mitigation agreements for the government, sellers and buyers to establishing and leading compliance protocols for mitigated companies.

Nathan Fisher, a Managing Director with StoneTurn, brings over a decade of experience investigating national security threats to the U.S. government. As a Special Agent with the Federal Bureau of Investigation (FBI), Nathan conducted a vast array of complex intelligence, counterintelligence, and cyber-focused investigations and operations. In his current role, Nathan advises clients across the national security, CFIUS, and cyber spectrums.