Corporate

CFIUS updates reflect changing world

By Alice Tchernookova January 10, 2023

The recent White House executive order mirrors the rapidly evolving environment of inbound investments in the US and related threats

As the world evolves, the laws and rules regimenting it need to keep up. This logic also applies to inbound foreign investment into the US, and its associated risks.

To that end, the White House recently published an executive order on ensuring robust consideration of evolving national security risks by the Committee on Foreign Investment in the United States(CFIUS). The first of its kind, it will provide formal presidential direction on factors CFIUS should consider when reviewing transactions.

"National security risks do evolve, and the Biden administration is guiding CFIUS not only to look at more traditional factors, but also at news ones, such as technological leadership and competitiveness, or supply chain resilience," said Michael Gershberg, partner at Fried, Frank, Harris, Shriver & Jacobson. “The world is perhaps more complicated, and transactions are more complex from a commercial standpoint, so there are more aspects to consider for each transaction. The reality of today’s international politics and economics also adds complexity.”

The executive order defines five specific sets of factors CFIUS should take into account. These include the transaction’s effect on the resilience of critical US supply chains, its impact on US technological leadership in areas affecting national security, industry investment trends, cybersecurity risks, and risks to US citizens’ sensitive data.

“Because of the changing nature of national security risks, there are now some industry sectors, investors and countries that make a CFIUS filing more likely,” said Gershberg. “The government is interested in a whole range of factors – more than anyone would have considered 15 or 20 years ago.”

Microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation were all singled out as areas of technological leadership particularly relevant to matters of national security.

“The executive order makes repeated references to relevant third-party ties, which means CFIUS will be considering not just the foreign investors themselves, but also any other ties they may have to foreign countries or persons – perhaps foreign suppliers or customers, or joint venture partners,” said Gershberg. “Another factor is aggregate industry investment trends, which implies not simply looking at the effects of a particular transaction, but putting them in the context of other investments in the same sector or by the same country of origin, to see the broader picture.”

Coupled with the near-simultaneous release of CFIUS enforcement and penalty guidelines,the measures could modify the regime significantly.

“It is the first time since CFIUS’s establishment 50 years ago that a president has exercised his direct authority to modify how and when the agency is to assess specific risks to US national security posed by inbound foreign investment,” said Harry Broadman, partner and managing director at Berkeley Research Group, and a former member of CFIUS. “The timing of the back-to-back release of CFIUS’s annual report and the executive order can hardly be a coincidence and was clearly well-planned. Changes to how the committee operates could well be sweeping.”

Keeping enemies at bay

Contents of the executive order were also likely influenced by the wider geopolitical context, including the US’s ongoing head-to-head with China in the technological sphere.

“The executive order refers to ‘countries of special concern’, which is generally understood to include China and Russia,” said Gershberg. “It was intended to highlight certain issues that the Biden administration perceives as relevant factors for national security, and activities in which those countries may be engaging.”

As such, Gershberg argued, the executive order could be interpreted as a warning to those countries that the US is cognisant of such activities and intends to place a particular focus on them.

"With the macro and geopolitical environment having become so different so quickly, the government realised that certain instruments of statecraft were particularly crucial to advance its interests," said Mario Mancuso, international trade and national security partner at Kirkland & Ellis. "As it relates to CFIUS, the downsides of missing a risky transaction nowadays could be so great in that the overall legal regime had to be upgraded."

An initial step in this direction was the 2018 Foreign Investment Risk Review Modernisation Act (FIRRMA), which aimed to broaden and modernise CFIUS's legal authority to address national security concerns arising from transactions more effectively. The new penalty and enforcement guidelines are a second step in this process, Mancuso argued.

"Those pieces working together are part of the same effort to make the foreign investment review system more effective," he said. "All of this focused activity is meant to support the national security mission of eliminating or mitigating national risk in inbound transactions. Given the state of US-China strategic competition, the US's margin of error today is much smaller than it was just a generation ago."

The CHIPS and Science Act of 2022, which over the next 10 years will direct $280 billion into US semiconductor production and R&D and the creation of regional high-tech hubs, is also part of the effort to keep up with Chinese competition. According to government research, the US currently only accounts for 12% of the world's semiconductor production, compared to 37% in the 1990s.

"Years ago, the US's qualitative overmatch against potential adversaries was so great that if it missed a sensitive technology here or there, it wouldn't really make a difference: the country was much stronger and much more capable than its competitors," said Mancuso. "However, that is not true with respect to China – today, the gap is shrinking, and so the US has to be more mindful of certain types of technologies and where they go."

The CHIPS act has also introduced further export controls, this time on semiconductors, and prohibits companies from making further investments in China and producing certain types of chips in China and Russia if they are awarded subsidies under the act.

"CFIUS as a regime is not exclusively focused on a single country, but given its importance, China is in a category of one," Mancuso explained. "Although Russia is also a threat actor for the US – in cybersecurity, for example – its economy is pretty small. CFIUS regularly reviews prospective transactions for any nexus to Russia or to sanctioned entities and individuals. But as a practical matter, it is secondary to China, as Russia doesn't play as big a role in the global economy."

Although Russia's invasion of Ukraine has made the US more cognisant of the threat it represents, the war has had little impact on the evolution of CFIUS, and both the executive order and the penalties and enforcement guidelines would have likely come out in the same form.

“China has been front and centre of US security concerns for a long time, and so this renewed focus shouldn’t come as a surprise, but the war between Russia and Ukraine isn’t a part of this in the first instance,” said Broadman. “The war has certainly made people more aware of the dangerous world we live in, but there is no strong correlation with the CFIUS review.”

A top concern in matters of US national security is the role played by governments in state-dominated economies such as China, which domestically controls personal data and information about its citizenry.

“The argument is that the US needs to protect its own citizens in international transactions,” Broadman added. “That is a natural evolution that has very little to do with Russia and the war in Ukraine.”

Alice Tchernookova
AMERICAS EDITOR

Alice is Americas Editor for IFLR, with a responsibility for the US markets, particularly covering how they interact with the UK and Europe. She regularly touches base with market participants positioned both on the buy and sell side, but also with a large number of advisors and consultants across all parts of the market. Previously, she focused on benchmark reform and Brexit.

Established in 1975, Washington’s interagency executive branch foreign investment screening entity – the Committee on Foreign Investment in the United States (CFIUS) – not only pioneered national security regulation of inbound investment transactions, but for decades also marked the US as virtually the only country possessing such a regime.

The irony of the juxtaposition of the world's most ardent champion of liberalised investment and trade flows being such a pioneer was – oddly – rarely voiced by America's international economic partners. In fact, it became seen as business as usual.

Today, half a century later, many other countries – indeed mostly other advanced democracies – are in the process of either creating their own foreign investment regulatory regimes or strengthening nascent frameworks on this score. State-dominated nations, too, are now further intensifying such regulatory practices, which are, of course, part and parcel of the fundamental policy tenets that define their economic systems.

As national security regulation of inbound foreign investment matures across the globe, will the next phase of such regulation focus on outbound foreign investment transactions?

CFIUS: the global beacon

Much of the recent proliferation around the globe of initiatives to regulate national security risks of inbound foreign investment has been driven by the accelerated rise of China in the world economy over the last few decades and its staying power. Compounding this was US enactment in 2018 of the nation's first wholly CFIUS-dedicated statute, FIRRMA (the Foreign Investment Risk Review Modernization Act), and unusual for lawmaking by Washington, was its passage by Congress almost unanimously and on an overwhelmingly bipartisan basis.

In contrast, much of the impetus behind CFIUS' creation was Japan's increasing global economic strength – a phenomenon that, over time, has waned. Moreover, the initial legislation was a relatively obscure amendment to a core law of US defense policy.

FIRRMA and its subsequent implementing regulations set out systematically, and in great detail, CFIUS' operating principles, procedures, and sectoral classifications where national security oversight of cross-border transactions, including those that were already consummated, would be most rigorous.

Around the time of passage of FIRRMA or soon thereafter, more than 25 countries either now have in place dedicated inbound investment review processes or are well on the way of doing so. Mostly this includes democracies, such as Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Hungary, Iceland, India, Ireland, Japan, Latvia, Lithuania, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Romania, South Korea, Slovakia, South Africa, Spain, the UK.

In addition, at the regional level, the European Union (EU) has established a bloc-wide information-sharing framework regarding inbound foreign investments by non-member countries. This provides a process for *all* EU members to raise issues about the national security implications of a prospective transaction in one member's market even if it does not directly involve capital flows across other members' borders.

State-dominated countries have also established or strengthened regimes to regulated foreign investment, most notably China, Russia, and Saudi Arabia.

At the same time, while some countries have not put in place unified or self-contained foreign investment regulatory statutory frameworks, they do screen such investment through other instruments and channels, including (i) limits or prohibitions on foreign ownership of land; (ii) restricting foreign investment through licensing requirements; and (iii) specifying sector-specific percentage limits for foreign investment.

Sectoral creep for defining sensitive sectors

The definition of what constitutes sensitive sectors in which foreign investment could pose a threat to national security has accelerated significantly in the past few years. Arguably more than any other democracy, the US has been the most aggressive on this front, although other jurisdictions have now closely followed the US lead.

For several decades, the traditional focus was on regulating/banning foreign transactions in domestic firms or activities in bona fide defense and security operations. By the early 2000s, that was enlarged to include infrastructure facilities, some of which, on the face of it, seemingly had tenuous national security risks.

Arguably the most well-known case was the proposed transfer of contractual rights for port management services in several US ports from one foreign entity to another in 2006. The purchaser was to be DP World (DPW), a state-owned company in the UAE. The port services contracts were already owned by a British firm (Peninsular and Oriental Steam Navigation Company – P&O). Yet after DPW acquired P&O, the contracts were to fall under DPW control. Although the transfer already had been approved by CFIUS, US Congress passed legislation to block the deal.

A contrasting example was the 2013 sale of the pork products company Smithfield Foods to the Chinese firm Shuanghui. At the time, it was the largest Chinese purchase of a US company in history. As CFIUS was in the throes of its process of deciding whether or not to approve the sale, the US Senate Committee on Agriculture, in an unprecedented move, held hearings on the threat the proposed transaction would pose to the safety of the US food supply chain. It was truly a poignant moment in the politicisation of the CFIUS process – for two reasons.

First, the acquisition had little, if anything, to do with China's interest in sales of pork *within* the US market; rather Shuanghui's objective was to actually increase US exports of pork to China, which it has subsequently done.

Second, Smithfield Foods and its US advisors seemingly had blinders on as to their fundamental understanding of the perceived political ramifications of the deal as seen through the eyes of US politicians (whether or not such perceptions were rational). Indeed, Smithfield was stunned that a deal combining the elements "China" and "US food" would even merit *voluntary* notification to CFIUS. Given all that has transpired in the political realm of Chinese investment in the US over the past couple of decades, to say this reaction was naïve would be an understatement. Nonetheless, the transaction was consummated.

Over the past few years, the concept of national security within the CFIUS process has broadened beyond defense and security assets; infrastructure; and real estate, and now includes personal data. This is increasingly true in other countries as well. Nothing personifies this more than the Trump administration's machinations over the proposed divestiture of the Chinese firm ByteDance's TikTok app. The mishandling of the case served only to undermine the stature of the US as the global beacon for certainty and clarity of nations' policies toward foreign investment.

Coordination and disclosure on the investor side: no longer just a bilateral process

The jurisdictional proliferation of national security regulation of foreign investment has ushered in a dramatic change in the way in which investors – especially multinational corporations – engaged in cross-border transactions must now navigate the screening process. Not surprising, taking a bilateral approach is increasingly unlikely to get very far. The fact is that many governments regularly share data.

In the case of the US, FIRRMA mandates CFIUS to engage in such practices. The goal is to facilitate harmonisation across countries wherever there is a coincidence of interests. The result is that even where multiple jurisdictions have similar foreign investment screening frameworks, parties to a transaction will need to plan carefully to succeed through multi-jurisdictional review processes, bearing in mind that the review process undertaken by CFIUS is arguably the most challenging of its kind in the world.

Will the US establish national security regulation for outbound foreign investment?

A new chapter in US regulation of foreign investment may well be in the offing: national security screening of *outbound* investment by US firms.

Urged on by the Biden White House, legislation in the final stages currently pending in the US Congress – still subject to reconciliation between Congress' two houses, their final vote and then signature by the President – contains provisions that could subject certain investments made abroad by US firms to regulatory approval.

Propagated by concerns about US entities "offshoring" advanced technology development, production capabilities, and supply chain operations that are deemed vital to US manufacturing, the legislation seeks to establish a US Committee on National Critical Capabilities (CNCC) that would operate similarly to CFIUS.

Several sectors are being highlighted in the pending statute: (i) medical supplies, medicines, and personal protective equipment; (ii) components essential to the operation, manufacture, supply, service, or maintenance of critical infrastructure, including that required following natural or manmade disasters; and (iii) components determined to be critical to military and intelligence systems and operations.

Given the votes taken to date on various sections of the legislation, it would be surprising if, in some form, such a law is not ultimately enacted. If that comes to pass, one would be hard pressed not to believe that other countries would follow suit – both democracies and state-dominated economies alike.

Harry G. Broadman is managing director at Berkeley Research Group LLC, where he chairs BRG's emerging markets practice and its CFIUS practice, and is also a faculty member at Johns Hopkins University.