Published on *The National Law Review* https://natlawreview.com

Foreign Investment and National Security: Navigating Heightened Scrutiny of US, EU and UK Cross-Border Deals

Article By:

Mark T. Ciani

Ciara McBrien

Jonathan Rotenberg

Alex Taylor

Edward A. Tran

Oliver Williams

As geopolitical tensions ratchet higher across the globe – fueled by the ongoing conflict in Ukraine, turbulent relations between China, the United States (US), and Europe, escalating conflict in the Middle East, and increased governmental efforts to promote industrial resilience through 'onshoring' and 'friendshoring' of supply chains – countries are increasingly placing national security concerns at the forefront of their trade and investment policymaking endeavors. For cross-border dealmakers, the result has been a proliferation of new and enhanced regimes for reviewing foreign direct investment (FDI) on national security grounds, with the range of strategically important sectors and transactions subject to heightened scrutiny expanding exponentially. The regulatory environment for FDI has thus become increasingly complex in key investment destinations such as the US, the European Union (EU) and the United Kingdom (UK) – a trend that appears likely to accelerate in the near to medium term.

Background on National Security and Investment Regimes

Although the scope of national security and investment regimes varies substantially across jurisdictions, the regimes generally facilitate government scrutiny of and intervention in foreign acquisitions and investments in domestic businesses for the purposes of safeguarding national security. In addition to assessing potential national security concerns associated with inbound FDI, governments are increasingly scrutinizing outbound FDI into certain advanced technologies and

products (such as artificial intelligence (AI), quantum information technologies, semiconductors and microelectronics).[1] Governments are also dedicating greater resources to identifying and monitoring investments in domestic companies by parties associated with perceived certain jurisdictions (such as China and Russia), resulting in heightened scrutiny of transactions with direct or indirect links to those jurisdictions.

While the regulatory landscape for cross-border investment is becoming ever more challenging, it can be navigated successfully through careful transaction structuring and engaging with potential national security issues at the earliest possible opportunity. In addition to evaluating potential filing and approval requirements and adjusting expected transaction timelines accordingly, the transacting parties may need to consider a broad range of potential mitigation measures and the effect those measures – and any attendant implementation costs – may have on the continued viability of the transaction.

In this advisory, we provide a high-level overview of the FDI review frameworks applicable to US, EU and UK targets and discuss a few illustrative examples of transactions that have recently been subject to review.

The US Landscape

CFIUS Review of Inbound FDI

The Committee on Foreign Investment in the United States (CFIUS) is an inter-agency committee of the US government responsible for screening acquisitions by foreign persons of US businesses and real estate to determine whether they raise national security concerns. While most sensitive transactions are brought to CFIUS's attention through the filing of pre-closing notifications, CFIUS maintains an active surveillance group to monitor ongoing and completed transactions for potential review and investigation.

If CFIUS determines that a transaction poses national security concerns, it may propose mitigation measures to resolve the matter. However, if the parties and CFIUS cannot agree on the scope of the mitigation measures, or if adequate mitigation measures are infeasible or unavailable due to the sensitive nature of the US business, CFIUS will request that the parties abandon or unwind the transaction. If they refuse, CFIUS can refer the transaction to the president, who has the authority to suspend or prohibit the transaction or require divestment post-closing.

The scope of CFIUS's jurisdiction was significantly expanded after the enactment of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) and the promulgation of subsequent regulations. Prior to FIRRMA, CFIUS jurisdiction was limited to transactions in which a foreign person was acquiring, or could acquire, control of a US business, and CFIUS filings were made exclusively on a voluntary basis. FIRRMA extended CFIUS's jurisdiction to cover certain non-controlling foreign investments in US businesses involving critical technology, critical infrastructure or sensitive personal data (TID US businesses)[2] where the investments grant the foreign person access to material nonpublic technical information, board membership or observer rights, or involvement in the business's substantive decision-making.[3] Furthermore, FIRRMA provided CFIUS with jurisdiction over acquisitions by foreign persons of real estate located in or near certain US ports, military installations and other sensitive areas.

FIRRMA also created a mandatory CFIUS filing regime for three types of transactions. The first category consists of acquisitions of control by foreign persons over US businesses that produce,

design, test, manufacture, fabricate or develop critical technologies where a US regulatory authorization would be required for the export, reexport, transfer (in-country) or retransfer of the technology to the foreign persons (US Critical Technology Businesses). The second category covers non-controlling investments by foreign persons in US Critical Technology Businesses where the foreign person is also acquiring certain access rights, board rights or substantial decision-making rights with respect to the critical technology. The final category involves the direct or indirect acquisitions of voting interests of 25 percent or more in TID US businesses by foreign persons in which a foreign government has, directly or indirectly, a 49 percent or more voting interest.[4] Failure to submit a mandatory filing could subject the transacting parties to a civil penalty not to exceed US$250,000 or the value of the transaction, whichever is greater. Given these requirements, deal parties contemplating FDI into any TID US business should ensure that a CFIUS analysis, including due diligence on prospective foreign investors, their beneficial owners and controlling persons, is conducted at the earliest potential opportunity.

Treasury Review of Outbound FDI

In addition to CFIUS's scrutiny of inbound FDI, the US Treasury Department has issued proposed rules to prohibit or require notification of certain types of outbound investments by US persons into entities located in or subject to the jurisdiction of a designated "country of concern" (currently China and the special administrative regions of Hong Kong and Macau), or owned by persons of a country of concern, where the entities are involved in specific categories of advanced technologies and products.[5] Certain AI systems, quantum information technologies, semiconductors and microelectronics are the initial technologies and products subject to the proposed rules.

The proposed rules would apply to certain transactions entered into by US persons, including equity or contingent equity investments; certain convertible debt financings and contingent equity investments; a greenfield investment or other corporate expansion; a joint venture; and certain investments as a limited partner or equivalent in a foreign pooled investment fund. In each case, the US person's obligations would be subject to an actual and constructive knowledge standard, with the latter effectively requiring a US person to conduct a reasonable and diligent inquiry prior to undertaking a covered transaction. Exceptions are provided for a host of transaction types, provided they don't afford a US person rights beyond the typical minority shareholder protections. These include investments in publicly traded securities; certain small or minority investments in a venture capital fund, private equity fund or other foreign pooled investment fund; full company buyouts; intracompany transactions between a US parent and its majority-controlled subsidiary; and certain transactions determined by the Treasury Secretary as likely to have any associated national security concerns adequately addressed by the actions of a foreign country or territory. Violations of the proposed rules could subject a US person to civil and criminal penalties under the International Economic Emergency Powers Act (IEEPA), with the Treasury Secretary empowered to take any action authorized under IEEPA to nullify, void or otherwise require divestment of any prohibited transaction.

The EU Landscape

FDI screening in the EU is done pursuant to Regulation 2019/452 (the FDI Regulation). The FDI Regulation sets forth a list of factors that EU Member States may wish to consider when assessing whether an investment affects their national security. It does not, however, introduce an EU-level FDI screening regime, nor does it require EU Member States that do not currently have an FDI regime to introduce such a regime. Therefore, EU Member States retain full power to legislate for and control FDI in their jurisdiction. The FDI Regulation is under review, however, and certain limitations are

likely to change.

In January 2024, the European Commission published its proposed reforms to the FDI Regulation. These proposals are intended to harmonize the application of FDI regimes across EU Member States by, amongst other things, requiring all Member States to introduce an FDI regime and to screen investments in certain sectors. The proposals also seek to widen the scope of the existing regime to capture indirect acquisitions by foreign investors (i.e., through the use of an existing EU company) and to streamline filing processes and timelines across Member States.

The UK Landscape

The UK's National Security and Investment Act (NSI Act) enables scrutiny and intervention in acquisitions and investments made by and in UK-based entities or assets in order to protect national security, much like CFIUS does in the US. The NSI Act provides the UK government with wide powers to block or apply conditions to certain investments on national security grounds and to impose any remedies it deems necessary.

The NSI Act imposes mandatory filing obligations for qualifying investments in target companies with specified activities in the UK in 17 sensitive sectors (including AI, computing hardware and military or dual-use technologies). The proposed acquirer(s) of shares or voting rights (exceeding defined thresholds) must obtain government clearance for their transaction before it takes place.

All other qualifying investments are subject to a voluntary filing regime and if the UK government considers it appropriate, it reserves the power to call in unnotified transactions for a national security assessment. Transactions in any sector can, therefore, be reviewed under the voluntary regime, but there is a higher risk of a national security intervention if the target has activities that are within, or closely linked to, one of the 17 sensitive sectors. Land and certain fixed assets, including transfers of intellectual property, may also be in scope.

Please see our previous publications (available here and here) for a more detailed analysis of the NSI Act's operative provisions.

Illustrative Case Studies

US CFIUS Case Study

On 13 May 2024, President Biden issued an executive order requiring MineOne Wyoming Data Center LLC, a company ultimately majority-owned by Chinese nationals, and certain related entities (collectively, MineOne) to divest legal and beneficial ownership and other rights in certain real estate in Cheyenne, Wyoming located within one mile of Francis E. Warren Air Force Base. MineOne purchased the property in June 2022 to use in connection with a cryptocurrency mining operation and proceeded to install equipment and related infrastructure to facilitate the mining of cryptocurrency and other digital assets. Under the order, MineOne was also required to remove all property, installations and equipment from the property and immediately cease and prohibit access to the property except as needed to comply with the order. Ultimately, the US authorities considered that the "proximity of the foreign-owned Real Estate to a strategic missile base and key element of America's nuclear triad, and the presence of specialized and foreign-sourced equipment potentially capable of facilitating surveillance and espionage activities, present[ed] a national security risk to the United States[.]"[6]

The order is notable insofar as it is the first time a president has taken action to block or unwind a

foreign investor's real estate transaction on national security grounds since CFIUS's jurisdiction was expanded in 2018 to permit the review of such transactions near or military installations and other sensitive US government sites. Also noteworthy is that CFIUS was alerted to the transaction based on a public tip, rather than a voluntary submission by the transacting parties. Although CFIUS's mandatory filing requirements do not extend to real estate transactions, the MineOne case illustrates the extent to which CFIUS has recently enhanced its investigatory capabilities through additional funding as well as publicly available "hotline" mechanism through which third parties – including spurned M&A bidders – can alert CFIUS to non-notified transactions that may pose a threat to US national security. Transacting parties considering FDI in real estate near sensitive US government sites, in businesses involved in cryptocurrency or other advanced technologies, or from foreign persons with a connection to China or other US countries of concern, should take particular care to assess potential CFIUS risks at an early stage. Upon review, a voluntary filing may be advisable under the circumstances so that potential national security concerns can be identified and addressed prior to closing or on a going-forward basis pursuant to a negotiated mitigation agreement.

UK NSI Act Case Study

On 16 November 2022, the Secretary of State made a final order pursuant to the NSI Act with respect to the acquisition of the UK's largest semiconductor manufacturer, Newport Wafer Fab (NWF), by Nexperia B.V. (Nexperia). Nexperia is ultimately owned by Wingtech Technology Co., Ltd., a Shanghai-listed company reportedly backed by the Chinese Communist Party. The final order required Nexperia to sell at least 86 percent of NWF.

The transaction was one of the first examples where the Secretary of State extended its initial review period by an additional 45 working days by retrospectively calling in the transaction for a full national security assessment. By exercising its power under the NSI Act to "stop the clock" for information gathering purposes, the transaction was ultimately under review for six months, from 25 May 2022 to 16 November 2022.

The Secretary of State's conclusions were that (i) technology and know-how that could result from a potential reintroduction of compound semiconductor activities at NWF's Newport site could undermine UK capabilities, and (ii) the location of the Newport site could facilitate access to technological expertise and know-how in the South Wales Cluster, and the links between the site and the Cluster may prevent the Cluster being engaged in future projects relevant to national security.

This decision illustrates the importance of new and emerging technology and, in particular, the semiconductor industry to the UK's national security. The decision also demonstrates the growing nervousness with respect to China's global efforts to obtain control of semiconductor manufacturers, as the production of semiconductors becomes ever-more integral to the UK's industrial and defense capabilities, and the orderly functioning of the global economy more broadly.

Of particular interest in this case is that initially, the UK government concluded there were insufficient reasons to block the transaction on national security grounds, as NWF's technology was considered primarily legacy and low-tech. However, after "*political and industry concerns grew about the broader resilience of semiconductor supply chains amid international geopolitical uncertainty*,"[7] the government reversed its position and retrospectively called in the transaction for a full national security assessment. This further demonstrates the growing sensitivity to areas of technology in the current global landscape and how politicized FDI schemes are becoming in practice.

In March 2024, the UK Secretary of State gave clearance for Siliconix Inc and Vishay Intertechnology

Inc, two US-based corporations, to complete an acquisition of NWF from Nexperia. However, the final order only allowed the acquisition to complete subject to the condition that Vishay and Siliconix (or their subsidiaries) must inform the Secretary of State in advance of completing any agreement to sell, transfer, grant a lease or licence to any third party which would allow that third party to use any part of the Newport site. This perhaps evidences that, while the NSI Act is broad in scope, the identity of the investor is one of the key considerations in the UK.

EU Case Studies

As in the UK, deals involving technology that can be used for both civilian and military purposes – so-called "dual-use technology" – has been a particular focus of FDI regulators in the EU. For example, in 2020, German regulators blocked the proposed acquisition of IMST GmbH (IMST), a German communications technology company, by Addsino Co. Ltd, a subsidiary of China Aerospace and Industry Group Co. Ltd (CASIC). CASIC is a defense corporation controlled by the Chinese government. IMST operates in satellite and radar communications and has technology that is relevant for military applications. The German regulator found, therefore, that the acquisition would have potentially endangered supply to the German armed forces. In addition, IMST possessed significant 5G technology, which the German regulator found to be a part of Germany's critical infrastructure.

Deals involving semiconductors have also failed following regulatory scrutiny. In 2022, after an extended period of regulatory scrutiny, the bid by GlobalWafers, a Taiwanese company, for Siltronic AG, a German producer of silicon wafers was forced to lapse because the German regulator failed to issue a clearance decision prior to GlobalWafers' bid expiring. Silicon wafers are an essential component of the semi-conductor industry, and the proposed deal would have resulted in GlobalWafers becoming one of the world's largest producers.

Finally, regulators in the EU have not just been hostile towards acquisitions by corporations from China and the Far East. In October 2023, the French Ministry of the Economy prohibited the acquisition of two French subsidiaries of Velan Inc, by Flowserve Inc, a US corporation (Flowserve). The French subsidiaries manufactured and supplied certain parts for French nuclear submarines and nuclear reactors. Flowserve is a US multinational providing fluid motion and control products and services. Here, the regulator's concern seemed to be the possible negative impact on the French defense sector. The decision by the French regulator is particularly notable because acquisitions by US corporations are not typically blocked by EU regulators.

Key Takeaways for Deal Participants

Our brief dive into FDI regimes makes clear that understanding and early engagement with such regimes are paramount to successfully completing your transaction through the regulatory process.

It is recommended that investors:

- Engage with their lawyers at the outset of a transaction to help them understand the background and key objectives, the identities of key participants, and any potential national security considerations that may be implicated.
- Map out a comprehensive deal timetable that includes the sequencing of potential filings that may need to be made so that all parties are aware of potential delays from the outset of discussions. Investors should be aware that the assessment and screening process may vary widely from transaction to transaction and may not be as predictable as statutory provisions

would suggest.
- If you are co-investing, consider the risk profile of all investors involved in the transaction.
- Consider allocating national security risks among the parties through appropriate transaction terms, including:
    - representations or warranties as to the presence or absence of any mandatory filing requirements;
    - limitations on foreign investor rights so as to avoid triggering specific review thresholds or criteria; and
    - allocation of costs associated with any pre- or post-closing filings or required mitigation measures.

Concluding Remarks

The scope of FDI regimes across the US, EU and UK are broad, and governments in all three jurisdictions are willing to step in to block or amend a transaction where they consider that it represents a risk to national security. A perceived risk can arise directly because of the assets involved or indirectly because of the potential impact on supply chains for products deemed critical to national security. At present, all three jurisdictions appear to apply a great deal of scrutiny to acquisitions by Chinese investors; whether this view will continue is likely to depend on geopolitics and the global economy. Whether investment from additional jurisdictions is welcomed or rejected is likely to involve similar considerations, albeit perhaps to a lesser extent. What is clear, however, is that anyone thinking of doing a cross-border deal needs to think at an early stage about FDI, to figure out whether and to what extent it will apply to a proposed transaction. These considerations apply equally to buyers and sellers, both of whom need to assess the potential FDI risk, together with any possible remedies or mitigating actions, alongside the other commercial terms of the deal.

---

1 *See*, e.g., Provisions Pertaining to US Investments in Certain National Security Technologies and Products in Countries of Concern, 89 Fed. Reg. 55,846 (proposed July 5, 2024) (to be codified at 31 C.F.R. pt. 850), *available* at https://www.federalregister.gov/d/2024-13923 (imposing notification requirements and prohibitions on US persons transacting with covered foreign persons engaged in activities involving specified advanced technologies and products that pose significant national security risks).

2 *See* § 800.248 TID U.S. business, available at https://www.ecfr.gov/current/title-31/subtitle-B/chapter-VIII/part-800/subpart-B/section-800.248 (defining a TID US business as any US business that (i) produces, designs, tests, manufactures, fabricates or develops one or more critical technologies; (ii) owns, operates or supports US critical infrastructure; or (iii) maintains or collects, directly or indirectly, sensitive personal data of US citizens).

3 *See* § 800.215 Critical technologies, available at https://www.ecfr.gov/current/title-31/part-800/section-800.215 (defining the term "critical technologies" with reference to US export control regulations). Critical technologies are generally those subject to export restrictions on the basis that they are considered essential to maintaining US technological superiority and national security. Examples include certain advanced arms and defense technology, AI, quantum computing, semiconductors and microelectronics, biotechnology and biomanufacturing, nuclear facilities, equipment and material, advanced clean energy, climate adaptation or critical materials. Critical infrastructure includes systems and assets, whether physical or virtual, so vital to the US that their incapacity or destruction would have a debilitating impact on national security.

4 Exemptions apply to interests held by or on behalf of the governments of certain "excepted foreign states", which currently consist of the UK, Canada, Australia and New Zealand.

5 *See* note 1 above.

6 *See* Order Regarding the Acquisition of Certain Real Property of Cheyenne Leads by MineOne Cloud Computing Investment I L.P., available at https://www.whitehouse.gov/briefing-room/presidential-actions/2024/05/13/order-regarding-the-acquisition-of-certain-real-property-of-cheyenne-leads-by-mineone-cloud-computing-investment-i-l-p/.

7 *See* Nexperia sells Newport Wafer Fab to US chip company for $177mn, available at https://www.ft.com/content/cf295f39-4be8-4ecb-a8f1-963c94d9b1c2.

National Law Review, Volume XIV, Number 290