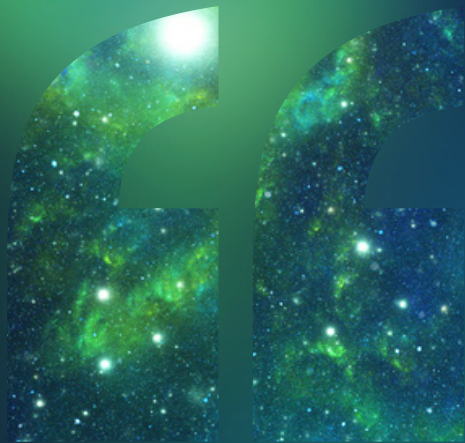
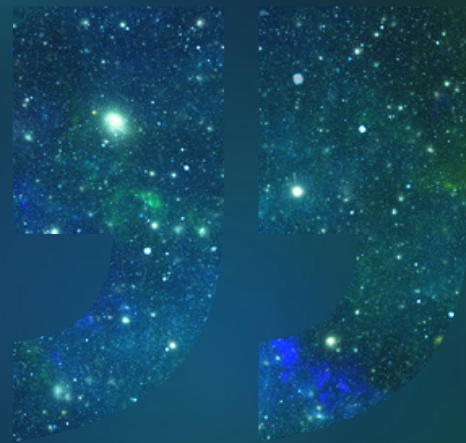


C L I F F O R D

C H A N C E



**THE EVOLVING
CONCEPT OF
NATIONAL SECURITY**



— THOUGHT LEADERSHIP

FEBRUARY 2022



THE EVOLVING CONCEPT OF NATIONAL SECURITY

In a recent yet unmistakable trend, the regulation of foreign investments under national security and foreign investment regimes has been growing ever more comprehensive, with sectoral coverage expanding to unprecedented levels. In this article originally published in the Foreign Direct Investment Regulation Guide – First Edition, Clifford Chance experts examine the shift by looking at the evolution of Foreign Direct Investment (FDI) regimes in Australia, the European Union, the United Kingdom and the United States.

In terms of mergers and acquisitions, foreign direct investment (FDI) regimes broadly fall into two categories: (1) those that apply only to investments made directly in domestic companies and aim to give domestic businesses in certain sectors a degree of protection from foreign competition (e.g., Indonesia, Malaysia and the United Arab Emirates), and (2) those that apply also to indirect investments (e.g., the acquisition of a foreign parent company that has a subsidiary in the jurisdiction in question).

The second type of regime, which is the focus of this article, tends to concentrate on the national security implications of foreign investments, and has historically recognised defence and critical infrastructure (such as energy and transport) as being fundamental to national security.

In a striking turn of events, a new viewpoint has been gaining traction globally during the past decade; in short, that national security should be seen to include everything from defence and critical infrastructure to artificial intelligence, healthcare, nanotechnology and the media, to name but a few examples. As a result, national FDI regimes have gradually expanded to the communications and advanced technology sectors and, subsequently, have been further extended to new areas such as healthcare, food security and water. It is clear that the concept of national security has begun to drift into national interest and may be blurred still further.

Changes in the scope of FDI regimes

Through legislative changes to existing regimes and the creation of entirely new national screening regimes, the number and scope of FDI regimes have changed significantly in the past few years, transforming the concept of national security.

Legislative changes in Australia and the United States

Australia: Introduction of a stand-alone national security review

Prior to 1 January 2021, national security concerns were not considered on a stand-alone basis and would be assessed only when an underlying transaction was considered a notifiable or significant action in its own right. Under the assessment regime for these transactions, national security considerations were a factor applied in determining whether a transaction was not in the national interest. The underlying focus of these policies was extended over time from defence and critical infrastructure to broader industry sectors and activities, such as those involving Australian businesses that stored or had access to sensitive personal information (particularly in relation to defence or intelligence personnel) or that may have had access to government information systems through contractual arrangements or otherwise. As such, transactions involving the healthcare industry, data centres or other information

technology providers, and the construction and commercial real estate sectors, came under increased scrutiny during the assessment process.

Significant amendments to the Foreign Acquisitions and Takeovers Act 1975 (Cth) (FATA) came into effect on 1 January 2021, introducing the stand-alone concepts of a notifiable national security action and a reviewable national security action. Unlike other transactions regulated by the FATA, these concepts are not subject to any monetary threshold or other limitation.

A transaction or other activity undertaken by a foreign investor will constitute a 'notifiable national security action', for which approval is compulsory and suspensory when it involves (1) the commencement of a 'national security business', (2) the acquisition of a 'direct interest' (i.e., 10 per cent or greater) in a national security business or in an entity that carries on a national security business, or (3) the acquisition of an interest in 'national security land'.

The assessment of transactions is delegated by the Treasurer of the Commonwealth Government to the Foreign Investment Review Board (FIRB) which assesses transactions against a national interest test. When that national interest test is met, the Treasurer or his or her delegate will issue a letter confirming there is no objection to the underlying transaction. When the industry sector in which a target operates is considered sensitive or has a security concern, no-objection letters are often granted, subject to conditions. The Treasurer is given a broad call-in right in respect of 'reviewable national security actions', which grants the Treasurer a range of powers when such actions are considered to have a national security concern.

The introduction of this concept has ultimately resulted in foreign investors being required to undertake an assessment of potential national security concerns in any merger or acquisition transaction conducted in Australia, as reviewable national security actions capture any transaction, regardless of

size, that result in a foreign investor acquiring or obtaining (1) an interest of 10 per cent or more in an Australian entity, (2) a position that allows the investor to influence or participate in the central management or control of an Australian entity, or (3) a position that allows the investor to influence, participate in or determine the policy of an Australian entity.

United States: transformation of the CFIUS regime

During the past five decades, the evolution of the concept of 'national security' has resulted in a significant transformation of the US government's foreign investment regime. Although reviews of foreign investment in the United States, either direct or indirect, remain the domain of the Committee for Foreign Investment in the United States (CFIUS or the Committee), the Committee's role in these reviews has continuously evolved, expanded and shifted to reflect the changes in US national security priorities.

The basic structure of the Committee was established in 1975 by Executive Order 11858. The founding premise of CFIUS remains the same, as it was initially designed as a mechanism within the US government's executive branch to monitor the effects of foreign investment in the United States. The Committee adopted a more active role in 1988 with the passing of the Exon-Florio amendment to the Defense Production Act of 1950 (Exon-Florio). Exon-Florio granted the President the authority to block foreign mergers, acquisitions and takeovers that threatened national security. At this point, national security was focused on the potential effect on defence activity, with assessments of the 'threat' posed by the foreign investor, the 'vulnerability' of the US business and the consequences for national security – an assessment framework fundamentally still used today. The 1993 Byrd Amendment further expanded CFIUS's scope to include a specific focus on the threat from foreign government investment, including state-owned and controlled entities.

The CFIUS regime underwent another major overhaul and expansion in the wake of Dubai Ports World's (DP World) attempted purchase of certain US commercial port operations in 2006. As a UAE state-owned enterprise, DP World's attempted acquisition faced significant opposition from the US Congress, as well as the public, partly because of the heightened national security environment prevailing at the time. Although, ultimately, DP World sold its operations to a US owner, the event's aftermath, and clear indication of heightened national security concerns regarding foreign investment in the United States, led to the enactment of the Foreign Investment and National Security Act of 2007 (FINSA). FINSA overhauled the existing CFIUS regime and significantly expanded CFIUS's authority and presence. In particular, the passage of FINSA increased CFIUS's reporting requirements, enabled greater Congressional oversight, and mandated mitigation agreements be implemented and monitored for continued compliance. FINSA also explicitly expanded the list of national security concerns relevant to a CFIUS review beyond the traditional defence and military activities, to include, for example, potential foreign government control, non-proliferation, counterterrorism cooperation, transshipment or diversion risk, and energy security.

After the enactment of FINSA, the focus of the national security discourse gradually shifted to the question of China and, specifically, the question of 'technology transfer' – the process of acquiring advanced technologies to enhance civilian economy and military capabilities. These methods include FDI, venture capital investment, joint ventures, licensing agreements, cyber espionage and talent acquisition programmes – with at least one report by the Defense Innovation Unit Experimental (DIUx) concluding that the US's existing tools (CFIUS and export controls) were inadequate. Further, the intensity of the CFIUS process during this period began to shift, with the Committee seemingly subjecting deals involving Chinese investors to increased scrutiny. This increased scrutiny was evidenced by CFIUS reviews resulting in the President

blocking trans-actions involving Chinese investors in 2012, 2016 and 2017 (with the latter transactions involving the semiconductor industry), all of which received significant media attention. These trends culminated in the passage of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which brought yet another expansion in CFIUS's authority, as well significant changes to the regulatory process itself. Among other changes, FIRRMA formally expanded CFIUS's jurisdiction and implemented mandatory filing requirements, as well as penalties for failure to file. The new mandatory filing requirements constituted a significant departure from the historically voluntary CFIUS notification process.

FIRRMA's implementation further reflected the evolved and expanded scope of national security in the context of foreign investment in the United States. Specifically, FIRRMA included a temporary programme (the pilot programme), dedicated to reviewing foreign investments, including non-controlling investments, into critical technology entities. The pilot programme included 27 specifically enumerated industries deemed to be 'critical technologies' and required mandatory CFIUS filings for foreign investments into these industries. The pilot programme and its mandatory filing requirement were incorporated into the mainline CFIUS regulations in 2020, although 'critical technology' was redefined to be based on export control licensing requirements.

Legislative implementation of new UK national security regulation

The UK government, like many others, has been focusing on the perceived dangers of investment in key sectors and critical infrastructure. The UK's previous regime gave the government the power to review certain transactions on national security grounds. In principle, it could intervene in investments made by domestic investors (so, in fact, was a national security screening regime not an FDI regime), although all the formal interventions to date under the regime have involved foreign investment.

A new, more expansive regime entered into force on 4 January 2022, in the guise of the National Security and Investment Act 2020 (the NSI Act). The NSI Act gives the UK government wide powers to call in and review investments on national security grounds and to impose any remedies it deems necessary.

The UK's previous regime was voluntary and non-suspensory. However, if no clearance was sought, the government could intervene and impose remedies on national security grounds, including unwinding the transaction, provided the transaction met the thresholds under the merger control regime or involved defence-sector contractors.

For transactions that close on or after 4 January 2022, the NSI Act imposes mandatory filing obligations for qualifying investments in target companies with certain activities in any of the following 17 sensitive sectors: civil nuclear; communications; data infrastructure; defence; energy; transport; artificial intelligence; autonomous robotics; computing hardware; cryptographic authentication; advanced materials; quantum technologies; engineering biology; critical suppliers to government; critical suppliers to the emergency services; military or dual-use technologies; and satellite and space technologies.

All other qualifying investments are subject to a voluntary filing regime, including investments that completed on or after 12 November 2020. Transactions in any sector can be reviewed under the voluntary regime, but there is a higher risk of a national security intervention if the target has activities in, or closely linked to, one of the 17 sensitive sectors listed above. Investments in real estate that is used for sensitive activities, or that is proximate to such a site, also carry a higher risk of investigation by the government.

In recent years, even before the entry into force of the NSI Act, the concept of national security has significantly expanded in the United Kingdom, from a focus on defence sector deals to investments in targets with various technologies, such as civilian satellites

(Inmarsat), radio equipment (Hytera), computer processing units (ARM) and graphene products (Perpetuus). Moreover, a range of international investors have been caught, including those from China, the United States and Canada.

Coordination and evolution of national security in the European Union

Regulation (EU) 2019/452 (the FDI Screening Regulation or the Regulation) entered into force on 10 April 2019 and applies to transactions taking place after 11 October 2020. The FDI Screening Regulation is not a replacement for the national screening regimes of EU Member States, which retain ultimate control over investments in their territory. Rather, it acts as an important supplement to the national regimes by introducing a cooperation mechanism between Member States. It also allows the European Commission (the Commission) to review and opine on investments that are likely to affect security or public order in more than one Member State or that could undermine projects of interest to the whole Union (for example, EU programmes for energy, transport and telecommunications networks).

Under the Regulation, Member States are required to notify the Commission and the other Member States of any FDI in their territory that is undergoing screening by providing certain information (such as details of the investor, investment vehicle and the Member States in which the investor or investment vehicle conduct business, among other things) and may include a list of Member States whose security or public order is deemed likely to be affected. In addition, the Commission and Member States may request information and provide comments on investments for which screening is not being undertaken by the relevant Member State but which the Commission or other Member States consider likely to affect security or public order.

Scope of the FDI Screening Regulation

No monetary thresholds are applicable under the FDI Screening Regulation. Further, only a non-exhaustive list of factors, which can be applied by EU Member States or the Commission when determining whether an investment is likely to affect security or public order, is set out in Article 4 of the Regulation. This list of factors includes the effects of the investment on:

- critical infrastructure, whether physical or virtual, including energy, transport, water, health, communications, media, data processing or storage, aerospace, defence, electoral or financial infrastructure, and sensitive facilities, as well as land and real estate crucial for the use of such infrastructure;
- critical technologies and dual-use items as defined in point 1 of Article 2 of Council Regulation (EC) No. 428/2009, including artificial intelligence, robotics, semiconductors, cybersecurity, aerospace, defence, energy storage, quantum and nuclear technologies as well as nanotechnologies and biotechnologies;
- supply of critical inputs, including energy or raw materials, as well as food security;
- access to sensitive information, including personal data, or the ability to control such information; and
- the freedom and pluralism of the media.

From such a list, it is evident that a wide array of sectors now fall within the ambit of national security concerns, with scope for further expansion in future.

Interaction with national screening regimes aimed at guiding the concept of national security

Prior to the introduction of the FDI Screening Regulation, the primary mechanism for foreign investment screening lay firmly at the feet of national authorities. Although national regimes continue to take precedence over the powers of the Commission and other Member States under the Regulation (the host Member State for the investment

has the ultimate say in deciding to allow or block the investment), they vary across Member States in the scope and severity of scrutiny of foreign investments.

At the time of writing, 18 EU Member States have some level of investment screening mechanism in place, while a further four Member States are considering implementing such measures. Only four Member States do not have, and do not have any plans to implement, an FDI screening regime. Nevertheless, all Member States will be able to participate in some level of investment screening across the Union under the banner of the Regulation.

Following the post-covid-19 pandemic policy-making trend towards domestic protection of a growing list of key sectors, such as healthcare, energy and transport, a number of national investment screening regimes across Member States are in the process of being revisited and strengthened. Many governments have viewed the pandemic as an opportunity to shield strategic industries from the opportunistic reach of foreign investors, allowing the notion of national security to be interpreted more broadly.

In addition, some EU Member States, such as France, Germany, Italy and Spain, introduced more stringent controls on foreign investment in the wake of the pandemic, many initially as a temporary measure. In France, the government lowered the threshold for screening non-EU investments in listed French companies to 10 per cent, whereas Italy introduced new notification requirements for EU investors in sensitive sectors and non-EU investors acquiring 10 per cent or more of entities considered as strategic. Spain requires authorisation for certain investments to be obtained by residents of Member States of the European Union and the European Free Trade Association (EFTA), in addition to the requirement for authorisation for non-EU/EFTA residents. At the time of writing, the foregoing restrictions had been extended to apply until at least 31 December 2021. As part of a more permanent amendment, Germany added 16 industries and certain types of transactions to the scope of its national FDI screening regime.

The outlook for such stringent national regulation of FDI beyond the end of 2021 is unclear, though given recent trends and the lasting effects of the pandemic, it is unlikely that governments will wish to relinquish their grip on certain key sectors of the economy to protect national interests.

Concept of national security under institutional guidance

In conjunction with revised or new legislation, national screening authorities and the European Commission have released detailed guidance to provide market participants with a description of the industry sectors and activities that they consider relevant to their national security assessments.

For example, the Commission, in anticipation of the full implementation of the FDI Screening Regulation and following the outbreak of the pandemic, adopted Guidance for Member States concerning FDI in March 2020. The main purpose of the Guidance was to streamline a pan-European response to the monitoring of FDI, particularly within the context of the public health crisis and to safeguard essential capital, technology and assets from any prospective hostile takeovers by companies from third countries. In its Guidance, the Commission recommended the adoption of extensive national FDI screening legislation.

In the United Kingdom, the government published a draft Statement of Policy Intent in summer 2021, setting out how it intended to use its new call-in powers for investments. The risk factors identified in the statement include whether (1) the target entity or assets could be used in a way that poses a risk to national security ('target risk'), (2) the acquirer has characteristics that suggest there may be a risk to national security as a result of the transaction ('acquirer risk') and (3) the acquirer will obtain a level of control that could allow it to pose a risk to national security ('control risk').

In Australia, FIRB released a detailed guidance note that provides market participants with a clear description of the

industry sectors and activities that FIRB considers relevant to any national security assessment. This guidance provided a sectoral breakdown detailing particular subsectors and activities within sectors where FIRB considers approval would be mandatory or recommended. These industry sectors capture:

- financial services, including large-scale financial institutions and providers of payments and clearing infrastructure;
- communications providers and network operators;
- broadcasting services and media;
- commercial construction contractors – which may be involved in the construction of government or other sensitive premises;
- commercial real estate investors – particularly properties housing government tenants or sensitive industries;
- businesses that are considered critical service providers or those involved in critical technologies or the extraction or processing of critical minerals;
- defence contractors and providers;
- energy, including electricity, gas, liquid fuels and nuclear, and operators of energy markets and infrastructure;
- healthcare and medical sectors – particularly those that hold sensitive patient information;
- tertiary education providers;
- information technology and data storage providers;
- transport, including ports, public transport providers and aviation; and
- operators of water and sewage infrastructure.

Finally, the evolving and expanding concept of national security is clearly reflected in the evolved and expanded role of CFIUS, as the monitor of foreign investment in the United States. In the past 20 years alone, CFIUS has expanded and been empowered. Critical technologies, critical infrastructure, personal data and real estate have been formally acknowledged as potential national security concerns. Further, the formerly wholly voluntary process now



has a significant mandatory element, and penalties may be assessed for failure to comply. Non-controlling investments now fall within CFIUS's jurisdiction and can even trigger a mandatory review. The role of CFIUS, and its power, will likely only continue to grow as national security concerns evolve further.

Conclusion

It is clear that the past five years alone have brought about significant changes in the approach to national security globally. A number of geopolitical concerns have arisen, in particular between China and the West, which have prompted several major Western economies to rethink the level of protection for domestically important industries. These concerns have been exacerbated by the effects of the covid-19 pandemic, which prompted fears about the supply of essential goods and services while large parts of the economy ground to a halt in the wake of far-reaching lockdowns and restrictions on movement.

Given the additional anticipated stresses of climate change and related geopolitical changes, there is no doubt that governments are laying the foundations for an economy that is cushioned as far as possible against the effects of global pandemics and financial or environmental shocks. The effects of these actions on global investment is yet to fully take shape and deserves close monitoring. Although parallels can be drawn with certain other regulatory activities (such as merger control), FDI regimes are notoriously less transparent, with governments enjoying a greater degree of discretion, less stringent time limits for decision-making and less regard for following precedents. It may be that the shift towards a chameleon-like concept of national security has only just begun.

An extract from GCR's Foreign Direct Investment Regulation Guide - First Edition. The whole publication is available at <https://globalcompetitionreview.com/guide/foreign-direct-investment-regulation-guide/first-edition>

CONTACTS



Emily Xueref-Poviac
Counsel
Paris

T: +33 1 4405 5343
E: emily.xuerefpoviac@cliffordchance.com



Jennifer Storey
Partner
London

T: +44 207006 8482
E: jennifer.storey@cliffordchance.com



Mark Currell
Partner
Sydney

T: +61 2 8922 8035
E: mark.currell@cliffordchance.com



Renée Latour
Partner
Washington DC

T: +1 202 912 5509
E: renee.latour@cliffordchance.com

CLIFFORD CHANCE

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2022

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.