REPRINT FINANCIER WORLDWIDE

AUGUST 2018

FINANCIER WORLDWIDE corporatefinanceintelligence

FINANCE & INVESTMENT

National security investment reviews go global: key policy themes and recommendations

MARIO MANCUSO, LUCI HAGUE AND SAM MOSS

KIRKLAND & ELLIS LLP

The historic Western consensus that foreign direct investment (FDI) is an unalloyed good is beginning to crack. In the past year, Australia, Canada, the United Kingdom, the US and the EU have taken meaningful steps to adopt, upgrade and implement more stringent measures to review inbound investments. In large part, these measures reflect a shared concern with the long-range impact of Chinese industrial policies, including Made in China 2025, that have been implemented in part through acquisitions of US and EU companies in sectors traditionally considered sensitive as well as economically significant (e.g., semiconductors, robotics).

Because every transaction has a unique national security risk profile – and views about a nation's macro security environment may evolve rapidly inside governments – national security reviews inject an element of uncertainty in transactions that is often difficult to avoid. That said, concerns inside Western capitals have generally crystallised around certain key themes.

KIRKLAND & ELLIS LLP

Mario Mancuso is a partner and Luci Hague and Sam Moss are associates at Kirkland & Ellis LLP. Mr Mancuso can be contacted on +1 (202) 879 5070 or by email: mario.mancuso@kirkland.com. Ms Hague can be contacted on +1 (202) 879 5195 or by email: lucille.hague@kirkland.com. Mr Moss can be contacted on +1 (202) 879 5254 or by email: sam.moss@kirkland.com.

Listed below are four of these, with some general recommendations to mitigate associated transaction risks.

Protection of 'foundational' technologies

Much of the current discourse regarding striking the right balance between the economic benefits of an open investment policy and national security priorities are reflected in proposals that key domestic technologies ought to be preserved from acquisition, appropriation or exploitation by foreign parties. In the US, Germany and elsewhere, government stakeholders have called for the preservation of such 'critical' technologies to be codified as a key element of a country's broader national security policies.

For example, in the US, proponents of legislation to reform the Committee on Foreign Investment in the United States (CFIUS) have highlighted the lack of coverage in the CFIUS regulations of new technologies that have not yet been classified for export control purposes but are essential for US national security. These 'foundational' technologies are widely seen as critical to preserving US military 'overmatch' capabilities. Germany strengthened its national security review infrastructure in July 2017 in reaction to a perceived wave of Chinese takeovers of German technology companies considered to be the 'crown jewels' of German industry, explicitly empowering the German government to intervene in more technology transactions.

As part of a broader effort to strengthen its national security review mechanisms, the UK has adopted new measures to expand the UK government's ability to review transactions implicating certain advanced technologies and export-controlled products, which became effective on 11 June 2018. Just one week later, the UK Competition and Mergers Authority announced that it would intervene under the new regime in the $58m acquisition of a UK aerospace company by a Chinese investor.

Infrastructure

While infrastructure transactions have long been of interest to national security review regulators, they have taken on new sensitivity in recent years, in part due to shared recognition that investments in infrastructure provide increased access to population centres and facilities, and thus expanded opportunities for parties with malign intent to engage in sabotage or surveillance.

Australia's Foreign Investment Review Board (FIRB) has been especially active in reviewing these investments, rejecting bids from State Grid Corporation (China) and CKI Holdings (Hong Kong) for the long-term lease of a 50.4 percent interest in electricity distribution network Ausgrid. The UK government has stated that, of the sectors that attract FDI in the UK, it is 'most focused on' infrastructure investments. Germany and Belgium have raised concerns about proposed minority investments by China's State Grid Corporation in their respective countries' electrical grids and power networks. A pending European Commission proposal to introduce an EU-wide investment screening mechanism for transactions that may implicate the national security interests of multiple EU member states would likely increase potential scrutiny of infrastructure, energy and transportation transactions.

Big Data

There is increasing recognition that vulnerabilities arising from access to data are fundamentally different, and more challenging to mitigate. Risk presented by foreign acquisition of a manufacturing facility producing a key material for a country's government can potentially be mitigated through traditional mitigation measures (e.g., visitation restrictions, physical access controls and export restrictions, etc.). In contrast, traditional mitigation measures are less likely to be effective in protecting data. For example, a target company's data could be scraped and transferred virtually instantly anywhere in the world – with no way to undo the harm. In the US, the assistant secretary of the treasury for international markets and investment policy stated that 'the digital, data-driven economy has created national security vulnerabilities never before seen'. Concerns about exploitation of large sets of otherwise benign commercial data have prompted the delay or abandonment of several high-profile public transactions.

In June 2018, the French Ministry for the Economy and Finance introduced proposed legislation to expand the jurisdiction and powers of its national security review regime. The draft legislation would require notifications of certain foreign investments in industries deemed 'strategic', including Big Data storage businesses, and would expand French authorities to impose measures to mitigate identified national security risks, including divestment of assets.

Supply chain integrity

Certain recent transactions have made clear that governments increasingly pay attention to investment in third-party companies that do not sell a finished product directly to government customers, but instead provide parts, components, technologies or services that are integrated into or used for finished products. On 23 May 2018, Canada blocked a proposed $1.5bn takeover of construction firm Aecon Group by China Communications Construction Co. In December 2017, the German Ministry of Economics initiated a national security review of the proposed acquisition of Cotesa, an aerospace supplier, by China-based Advanced Technology & Materials, in part due to concerns about Cotesa's supply of products to aerospace and defence customers. The transaction was ultimately approved. And in September 2017, President Trump blocked the takeover of Lattice Semiconductor Corp. by Canyon Bridge, citing 'the importance of semiconductor supply chain integrity to the US government'. The action followed Department of Defense (DOD) concerns about Chinese investments in US startups – which remain a top priority for DOD, as well as President Obama's December 2016 executive order prohibiting the takeover of Aixtron Corp. by a consortium of Chinese investors on similar grounds.

Recommendations

Think holistically, applying national security expertise and insight to the facts. The above list of areas of interest is not exclusive. National security considerations can arise in unexpected and counterintuitive ways, and each prospective cross-border transaction should undergo a bespoke review of its national security profile with the assistance of qualified advisers.

Be thorough, thoughtful and consistent. Transaction parties should assume that information submitted in connection with national security reviews will be checked against public and non-public information (e.g., derived through intelligence activities), and potentially (subject to applicable laws) shared with third-country regulators.

Consider the timing and content of public announcements. Transaction parties should carefully consider whether and when to publicly announce transactions that may undergo national security review or raise questions from regulators.

Red-team alternative deal structures to assess degrees of risk. Most national security regulators perceive China to be in a 'category of one' for risk. Transaction parties should carefully evaluate what deal structures and commercial arrangements, if any, may be available to help mitigate concerns.

With early strategic assessments and careful planning, buyers and sellers can often accurately assess deal feasibility, and take steps to enhance deal certainty, minimise delays and complications, and avoid embarrassment. ■