Australian Institute of Company Directors

ORGANISATION

National security compliance for directors

Australia has a complex and relatively new national security framework. There are criminal offences and regulatory controls directed at protecting critical infrastructure, intellectual property, and political process from foreign influence and interference. These laws can have an important impact on company dealings and, in some cases, regulate the conduct of directors. Failure to comply can result in heavy penalties and, in some cases, remedial directions.

This director tool examines key areas of national security compliance for directors, including broadly stated criminal offences, requirements to register when engaging in political and public communications with or for certain foreign companies and persons, disclosure and control rules that apply to critical infrastructure and restrictions on foreign-owned companies investing in Australia.

Criminal offences for being reckless as to the national interest

In 2018, the Australian government introduced a range of **new criminal offences relating to national security**. It is an offence to:

a. Deal with information or an article, while reckless as to whether or not it will prejudice Australia's national security, if this results in the information or article being made available to a foreign principal (*Criminal Code Act 1995* s 91.2(2), penalty is imprisonment for 20 years);

b. Provide resources, or material support, to a foreign intelligence agency or a person acting for a foreign intelligence agency (*Criminal Code Act 1995* s 92.8, penalty is imprisonment for 10 years);

c. Directly or indirectly receive funds from, or make funds available to, a foreign intelligence agency organisation (*Criminal Code Act 1995* s 92.10, penalty is imprisonment for 10 years)

d. Communicate or deal with information from a Commonwealth officer when:

   a. the information has a security classification of secret or top secret;

   b. the communication or dealing damages the security or defence of Australia;

   c. the communication or dealing interferes with a Commonwealth criminal offence, including any act that prejudices, prevents detection, investigation, prosecution or punishment of an offence against a Commonwealth law;

   d. the communication or dealing harms the health or safety of the Australian public.

   (*Criminal Code Act 1995* ss 122.4A (1) and (2), penalties are imprisonment for five years for communicating and imprisonment for two years for dealing).

Meaning of foreign government principal

The term 'foreign principal' is defined broadly. The meaning includes foreign government (which includes foreign regional or local government authorities), a foreign political organisation, a public international organisation, a terrorist organisation, or an organisation owned, directed or controlled by one or more foreign principals.

Governance impact

These criminal offences, and other related offences, can create a risk for directors where:

- A director does not know and has not tried to establish the country of origin or ownership structure of companies involved in business transactions;
- A director does not know and has not tried to establish the background of foreign individuals that may have employed or with whom they may transact;
- A director, or his or her organisation, is entrusted with valuable Australian intellectual property and/or sensitive Commonwealth information; and
- A director, or his or her organisaiton, is asked to share valuable Australian intellectual property or sensitive Commonwealth information with a joint venture partner and/or financier.

Recommendations

Directors should ensure they know with a reasonable degree of confidence, the background of people and companies with whom they do business. Asking the right questions is the first step. It may also be prudent to conduct thorough background checks. The checking should aim to establish whether they constitute a foreign principle and/or have links to a foreign national security agency.

Do not obtain, provide, or collect funds from any organisation or individual that might be associated with a foreign intelligence agency.

Do not share valuable intellectual property or sensitive information with any person or organisation until a properly diligent investigation establishes that they are not a foreign principal or related to a foreign national security agency or you are satisfied that the communication would not:

- prejudice Australia's national security;
- have a security classification of secret or top secret;
- damage the security or defence of Australia;
- interfere with or prejudice the prevention, detection, investigation, prosecution, or punishment of a criminal offence against a Commonwealth law; or
- harm or prejudice the health or safety of the Australian public or a section of the Australian public.

The Foreign Influence Transparency Scheme

The Foreign Influence Transparency Scheme requires organisations to register if they propose to undertake certain activities on behalf of a foreign principal. The regulated activities are parliamentary lobbying, general political lobbying, communication activities, and payment of money or giving things of value (such as donating). Marketing and/or sale of a product or service is not a regulated activity.

Under this scheme a foreign principal is a foreign government, a foreign political organisation, a foreign-government-related entity or a foreign-government-related individual. A foreign-government-related entity includes any part of a foreign government, including a government authority and regional and local entities. A foreign-government-related individual is a person who is not an Australian citizen or permanent resident, and who is employed by or otherwise under an obligation to a foreign government. Also, a foreign-government-related entity includes any entity that is controlled by a foreign principal.

The test for control is quite technical but sets a low bar. For example, a foreign principal is defined to include a foreign-governement-related entity, and a foreign-government-related entity can be any entity where more than 15 per cent of the share capital is owned by a foreign principal. Accordingly, there may be a chain of control where a foreign-government-related entity owns 15.1 per cent of a company (thereby the company is deemed a foreign principal) and that company owns 15.1 per cent of a second company (thereby deeming the second to be a foreign principle) and that company has more than 15 per cent of the share capital of the entity with which the Australian organisation is dealing. In this case, the company with which the Australian organisation is dealing is deemed to be a foreign principal despite the very distant related foreign government shareholding.

The Foreign Influence Transparency Scheme does not require foreign principals or their employees to register when acting on their own behalf. Also, the mere fact that a company is incorporated in a foreign jurisdiction does not, of itself, make the company a foreign principal.

Governance impact

The Foreign Influence Transparency Scheme creates a particular risk for directors where:

- a venture or project requires political lobbying, public advocacy and/or the giving of donations or support to a third a third party; and
- the venture partner is either clearly owned in whole or in part by a foreign government or political organisation (including a sovereign wealth fund) and or government-owned enterprise; or
- the ownership and/or control relationship is unclear.

Recommendations

Directors should regard political lobbying, public advocacy and/or the giving of donations or support for the benefit in whole or part of a venture partner as a red flag. Do not proceed until and unless, you have completed due diligence on your client or venture partner and have evidence that they are not a foreign principal within the meaning of the Foreign Influence Transparency Scheme or, if you establish that the venture partner is a foreign principle, register under the Foreign Influence Transparency Scheme with the Commonwealth Attorney- General's Department before proceeding.

The Security of Critical Infrastructure framework

The Security of Critical Infrastructure Act 2018 (Act) nominates strategically important ports, electricity generation, gas and water assets of significant scale (roughly those serving 100,000 people or more) as critical infrastructure. The Act gives the Minister a power to declare other assets critical infrastructure in secret.

It is not public what other parts of the Australian economy may have been declared critical infrastructure, but obvious candidates include airports, railway systems, major data centres and fuel processing and storage facilities. In August 2020, the Department of Home Affairs published **a consultation paper** seeking submissions on proposed reforms to the critical infrastructure regulatory framework.

Under the current framework, critical infrastructure assets are placed on a register maintained by the Department of Home Affairs. Owners and operators of designated access are required to provide the registrar with detailed ownership and operation information indicating the extension extent and characteristics of any foreign ownership and/or operational control. Regulated parties are required to update information provided to the registrar within one month of any change taking place. The Minister has a power to direct owners and operators of critical infrastructure to mitigate against a national security risk.

As a result of this framework, significant commercial assets within the Australian economy are required to consider the national security implications associated with changes in ownership, control, and operations. For example, the Minister could issue a direction requiring a transfer of ownership to a foreign entity, or an outsourcing of operation or control systems offshore, to be undone if he or she considers that it creates a national security risk.

Governance impact

This regime directly regulates nominated critical infrastructure assets. Directors of these entities must now consider national security implications associated with any changes of ownership, control or operations or risk being subject to a ministerial direction, potentially undoing or redoing business transactions.

The regime is also relevant to suppliers and investors in critical infrastructure assets. The possibility that the Minister might reject an investment or sale reduces the cohorts that might successfully acquire an interest in the business. Some suppliers to critical infrastructure assets might be rejected as unsuitable, particularly if their service offering or system involves connection to or controlled by offshore infrastructure. The national security implications of operational arrangements for critical infrastructure assets (including infrastructure assets where the designation as critical infrastructure is likely but not certain) must now be a material consideration for suppliers.

Recommendations

Directors of critical infrastructure assets need to understand and maintain an awareness of national security implications associated with their ownership structure and their operational arrangements. It is now more important than ever for the chair and directors to ensure the constraints and requirements arising from the national security obligations are understood within their organisations.

Service and system suppliers also need to understand the compliance framework controlling customers who are or may be critical infrastructure. Systems and services that give offshore access and control are likely to disadvantage a tender. Alternatively, solutions that bolster and reinforce national security will have an advantage.

Foreign Investment Review Board policy on national security

Since 29 March 2020, all foreign investments into Australia must be approved by the Foreign Investment Review Board. On that date the previous monetary threshold was set to zero. This measure was introduced to ensure "appropriate oversight" during the COVID-19 pandemic and made in anticipation of the introduction of a new framework to enhance the national security review of sensitive acquisitions and to create extra powers and resources to ensure foreign investors comply with the terms of any approval.

On 31 July 2020, the Treasurer announced the release of the exposure draft of the Foreign Investment Reform (Protecting Australia's National Security) Bill 2020 for **public consultation**. Key elements include:

- a national security test that enables the Treasurer to:
  - impose conditions or block any investment by a foreign person on national security grounds regardless of the value of investment;
  - require notification of any proposed investment by a foreign person in a sensitive national security business;
  - require notification where a business or entity owned by a foreign person starts to carry on the activities of a sensitive national security business;
  - allow any investment that would not ordinarily require notification to be 'called in' for screening on national security grounds;
  - allow investors to voluntarily notify to receive investor certainty from 'call in' for a particular investment or apply for an investor-specific exemption certificate; and
  - allow the Treasurer to impose conditions, vary existing conditions, or require the divestment of any realised investment if national security risks emerge;
- foreign persons will be required to seek further foreign investment approval for any increase in actual or proportional holdings above what has been previously approved, including because of creep acquisitions and proportional increases through share buybacks and selective capital reductions; and
- narrowing of the scope of the moneylending exemption so that it does not apply where foreign money lenders are obtaining interests in a sensitive national security business under a moneylending agreement.

These changes come with increased investigation powers, enforcement powers and penalties.

A key element of the new scheme is the concept of a 'national security business'. Under the proposed reform, this concept will include all critical infrastructure owners and operators designated under the *Security of Critical Infrastructure Act 2018*, all carriers and carriage service providers regulated the *Telecommunications Act 1997*, organisations dealing with information that has a security classification and supplier of defence related goods, technology and services.

Governance impact

All foreign investment into Australia requires Foreign Investment Review Board (FIRB) approval even if it is in a non-sensitive area. Foreign-owned businesses that start operations in national security business, and/or expand their investment in Australia related to national security business, will be required to deal with the FIRB. The proposed 'call-in' power may have implications for existing operations. The power of the Treasurer to order divestment to address a perceived national security risk represents an element of sovereign risk not previously present.

Recommendations

Directors of foreign entities should consider and assess the possible perception of national security risk associated with new or increased investment. Ensure that your organisation is aware of the relevant notification obligations and is aware of the likely view of the FIRB arising from your notification.

For directors of an Australian entity, consider the business risk associated with transactions with foreign owned counterparties (including borrowing) arising from the need to obtain FIRB approval no matter the value of the transaction.

National security, law enforcement and secrecy

In addition to the regulatory frameworks described above, an Australian business may receive a request or order from a law enforcement or national security agency requesting or requiring covert assistance. The relevant powers are varied but often require that the recipient maintain absolute secrecy in relation to the fact of the request or order and in relation to its subject matter. For example, there is a penalty of five years imprisonment for mentioning certain matters relating to a warrant issue by ASIO.

Responding to a lawful request, warrant or order can be problematic for a director or officer, particularly when performance of the order or request requires activities relating to the information, assets, or personnel of his or her organisation.

Directors that receive information warrants or access orders and/or internal reports regarding the receipt or implementation of such orders, should seek to clarify the extent to which a secrecy obligation applies and what can and cannot be communicated. If the nature of the business is such that the receipt and processing of a warrants or access order occurs or is likely to occur, the director should ensure she or he has advice regarding the extent to which appropriate governance procedures are in place, including regarding the extent to which associated information can be recorded and communicated.

Conclusion

National security regulation now forms and integral part of the Australian business environment. National security laws regulate individuals, entities, and conduct. They can also have an impact on how others deal with the regulated individuals and entities. Maintaining an awareness of these new laws can help guide decision making to avoid regulation, review and, in an extreme case, prosecution.

The rules described in this director tool are being enhanced and developed by the federal government continuously. They are likely to have increasing importance and more profound consequences as they are developed and expanded and accordingly, awareness of national security obligations is an important governance obligation for directors and their boards.

Related AICD Director Tools

- *Managing a data breach: Ten oversight questions for directors*
- *The consumer data right framework*
- *Data and privacy governance*

About the author

Patrick Fair GAICD BEc LLB CIPM FAISA, is the principal of Patrick Fair Associates; an Adjunct Professor at the School of Information Technology, Faculty of Science, Engineering and Built Environmental, Deakin University; the Chairman of the Communications Security Reference Panel at the Communications Alliance; and General Adviser for LexisNexis Practical Guidance Cybersecurity, Data Protection and Privacy.

About us

The Australian Institute of Company Directors is committed to strengthening society through world-class governance. We aim to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. Our membership includes directors and senior leaders from business, government and the not-for-profit sectors.

For more information t: 1300 739 119 w: aicd.com.au

0723b-6-32_20