17 August 2020

UPDATE

CYBER SECURITY STRATEGY, FOREIGN INVESTMENT RULES AND UPCOMING AND OUTSTANDING PJCIS REPORTS

This update covers recent developments related to Australian's national security framework.

Significant changes to the role of the Foreign Investment review board will increase national security oversight of foreign owned businesses. Australia's Cyber Security Strategy 2020 (**Strategy**) proposes a rage of new legislated controls and industry guidelines. We also mention a consultation on new rules for the protection of critical infrastructure of national significance and outstanding and upcoming reports by the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**)

1. Changes to Foreign investment rules

On 29 March 2020, changes were made to the threshold for review of foreign investments. The previous monetary threshold for foreign investment in (generally $275million) was set to zero. The revised threshold was said to provide "appropriate oversight" during the Covid-19 pandemic and to anticipation a new framework to enhance the national security review of sensitive acquisitions. Details of the new framework for national security review of foreign acquisitions were released for consultation on 31 July 2020.
The proposed changes 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.
- Narrowing 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; and
- A new Register of Foreign Ownership that will merge and expand the existing agricultural land, water, and residential registers, to increase the Government's visibility of foreign investments made in Australia; and
- New information-sharing provisions to allow foreign investment information to be shared with the ATO and across national security agencies.

A key element of the new scheme is the concept of "National Security Business". It has been proposed in draft legislation open for comment that 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.*

These changes come with increased investigation powers, enforcement powers and penalties. Submissions remain open until 31 August 2020. The consultation page is here.

2. Australian's Cyber Security Strategy

The Strategy was released on 6 August 2020. The Strategy renews the federal governments previously stated intention to enhance, educate and improve the security of Australia's IT infrastructure and allocates significant funding to counter cybercrime, centralise management, operation and security of It systems used by government agencies and support the Australian Cyber Security Centre.

It also outlines significant changes upcoming changes to cyber security related law and regulation, including:

- New laws to "make sure" Australia can recover quickly in a cyber emergency including a power to make directions to business and take direct action to protect systems.
- "Fit-for-purpose" powers and capabilities to discover, target, investigate and disrupt cybercrime.
- Possible legislative changes to clarify the obligations for businesses that are not critical infrastructure to protect themselves and their customers from cyber threats.
- Minimum cybersecurity requirements for operators of critical infrastructure and systems of national significance and "refine" incident reporting for compromises and near -misses that meet a certain threshold. (See the item following)
- "legislative certainty" to telecommunications providers implementing threat blocking technology.

These proposals are outlined in only general terms. Notably, it is unclear what new "powers and capabilities to target and investigate" are required, the proposed form and extent the proposed new security obligations for business that are not critical infrastructure and manner in which threat blocking might be authorised and encouraged.

Other new regulatory guidelines are proposed:

- A voluntary Code of Practice on the security of the Internet of Things.
- Support for business to implement threat blocking technology that can automatically protect citizens from known malicious cyber threats.
- Increased information for consumers about cyber security features to look for when buying a product and, longer term, consideration given to cyber security labelling.

A copy of the Strategy is available here.

3. Consultation on Protecting Critical Infrastructure and Systems of National Significance.

On 13 August 2020, the government issued a discussion paper seeking views on the planned introduction of an "enhanced regulatory framework" for critical infrastructure and systems of nation Significance. The discussion paper calls for views regarding:

- a positive security obligation for critical infrastructure entities, supported by sector-specific requirements;
- enhanced cyber security obligations for those entities most important to the nation; and

- Government assistance to entities in response to significant cyberattacks on Australian systems.

A copy of the discussion paper is available here. Submissions close on 16 September 2020.

4. Upcoming and overdue PJCIS reports

The PJCIS is required to review and report on the mandatory data retention scheme by section 187N of the *Telecommunications (Interception and Access) Act 1979*. That report was due on 13 April 2020 but has not been released.

The PJCIS is reviewing the *Telecommunications and Other legislation Amendment (Assistance and Access) Act 2018*. The subject of this inquiry was referred to the National Security Legislation Monitor whose report is available here. The INSLM report recommends that the government create independent oversight of the power introduced by TOLA. The INSLM's recommendations are in line with industry submissions but it is not certain that they will be adopted by the PJCIS. The PJCIS is due to report on 20 September 2020.

Please contact me if you have any questions regarding these developments

patrick@patrickfair.com 0411361534

Level 26 1 Bligh Street
Sydney NSW 2000 Australia
L +61 2 8226 8584
M +61 (0) 411 361 534
F +61 2 8226 8899
E patrick@patrickfair.com
W www.patrickfair.com
Technology Law Pty Ltd.
ABN: 44 003 792 809