Australian Government

Department of Home Affairs

Department of Home Affairs submission to the Inquiry into the Foreign Investment Reform (Protecting Australia's National Security) Bill 2020 and the Foreign Acquisitions and Takeovers Fees Imposition Amendment Bill 2020

Senate Economics Legislation Committee

10 November 2020

Table of Contents

Foreign investment and national security

Since the establishment of the Critical Infrastructure Centre in 2017 and its subsequent integration into the portfolio, the Department of Home Affairs has contributed its advice and understanding of national security risks to inform the Treasurer's consideration of proposed foreign investments in Australia's critical infrastructure.

As the geopolitical environment continues to evolve, and as our national economy and critical infrastructure become ever more complex and interconnected, it is essential that the foreign investment framework set out in the *Foreign Investments and Takeovers Act 1975* also adapts to meet these challenges. In the Department's view, the *Foreign Investment Reform (Protecting Australia's National Security) Bill 2020* and *the Foreign Acquisitions and Takeovers Fees Imposition Amendment Bill 2020*, deliver important updates to the framework to support the effective management of emerging national security risks.

Home Affairs' role in the foreign investment review process

Home Affairs is one of several national security partners the Treasury consults in preparing advice for the decision-maker on foreign investment applications, alongside the Australian Security Intelligence Organisation and the Department of Defence. Home Affairs' Critical Infrastructure Centre undertakes risk assessments on a case by case basis where an acquisition may involve foreign investment in one of Australia's eight critical infrastructure sectors: energy, water, transport, food & grocery, health, banking & finance, telecommunications and government. Home Affairs' referral criteria are regularly updated, and are being reviewed in light of proposed amendments to the sectors identified by the *Security of Critical Infrastructure Act 2018*[1].

The Critical Infrastructure Centre works closely with Home Affairs' Counter-Foreign Interference Coordination Centre, the Treasury and other national security partners to assess national security risk in each case, relating to:

- Sabotage
- Espionage, and
- Coercion / foreign interference.

Where national security risks are identified, the Critical Infrastructure Centre may recommend imposing mitigations, which include a spectrum of binding conditions on the acquisition or, in the most extreme cases, rejection. These recommendations form part of the broader package of advice prepared by the Treasury to inform consideration by the Foreign Investment Review Board, and ultimately the Treasurer.

On 29 March 2020, the Treasurer announced temporary changes to Australia's foreign investment framework in response to the COVID-19 pandemic, setting a $0 threshold for all foreign investment in Australian businesses and land. The change resulted in a significant spike in the volume of applications referred to Home Affairs for scrutiny, which it would not normally see under the regular monetary thresholds. However, it did not significantly change the proportion of cases that Home Affairs assessed as consequential. This may suggest that monetary thresholds are a poor predictor of whether an asset could be used to facilitate sabotage, espionage or coercion against Australia's national interest.

Additionally, in the increasingly complex economic environment, government and the private sector—including operators of critical infrastructure—are increasingly relying on smaller businesses to provide critical equipment or outsourced services. These smaller businesses are not themselves critical infrastructure providers and may not be subject to scrutiny under the monetary thresholds, but may have trusted access to

[1] Further information available at https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf

physical sites or IT networks, or may be entrusted with large sensitive data sets. This level of trust may place them in a position where they could be exploited to conduct activities prejudicial to national security.

The single touch nature of the foreign investment framework also cannot easily take into account how the national security risk associated with a business may change over time.

A robust compliance regime, supported by the appropriate powers, is required to ensure compliance with the conditions that have been imposed to manage national security risk. National security conditions play a critical role in managing foreign control of or access to critical systems and assets and sensitive data. However, these conditions are only effective where ongoing compliance is monitored.

The Bills carve out national security-related businesses, and allow for call-in where other national security concerns may emerge. At the same time, they place limitations around what is subject to national security review, and retain existing monetary thresholds for the majority of foreign investment. They also allow for investors—if in doubt—to create certainty by self-notifying for national security review to pre-emptively consider potential risk.

The ability to call in investments and impose conditions, or even to force divestment after the fact in the most extreme of cases, addresses the point in time nature of the foreign investment review process by allowing the Treasurer to scrutinise foreign ownership after the fact where the national security significance of an asset changes over time, or where national security concerns are only identified after the fact.

Finally, the additional compliance and enforcement tools and capabilities are an additional step to ensure that once national security conditions are imposed, foreign investors are compliant and conditions are effective in mitigating the risk.

Complementary reforms

The Bills, as proposed, will complement work underway by Home Affairs to further address threats to Australia's national security. The Minister for Home Affairs released a consultation paper in August 2020, proposing amendments to the *Security of Critical Infrastructure Act 2018* to expand the scope of that legislation to cover additional sectors and introduce new regulatory requirements for critical infrastructure operators. Specifically the legislation will comprise the following elements:

1. A Positive Security Obligation, requiring the responsible entity of a critical infrastructure assets to adopt and maintain an all-hazards critical infrastructure risk management program, mandatorily report serious cyber security incidents to the Australian Cyber Security Centre; and where required, provide ownership and operational information to the Register of Critical Infrastructure Assets.
2. Enhanced cyber security obligations that establish:
    - the ability for Government to request information to contribute to a near real-time national threat picture;
    - owner and operator participation in preparatory activities with Government; and
    - the co-development of a scenario based 'playbook' that sets out response arrangements.
3. A Government assistance regime that applies to all critical infrastructure sector assets, reflecting the fact that Government maintains ultimate responsibility for protecting Australia's national interests. As a last resort, the reforms provide for Government assistance to protect assets during or following a significant cyber attack.

These proposed reforms address the increasing threats to our critical infrastructure sectors by placing obligations on critical infrastructure owners and operators to protect their assets against all hazards. Over time this may relieve some of the pressure on the foreign investment review process, by allowing sector-wide obligations to take the place of case-by-case national security conditions. Sector-wide obligations will also ensure that foreign-owned and Australian-owned businesses are held to the same security standards.

Reforms to the *Security of Critical Infrastructure Act 2018*, however, will have limited effectiveness in mitigating risks where a foreign-owned entity is deliberately and deceptively acting to undermine Australia's national security. The reforms contemplated in the Bills before the committee will provide a complement to critical infrastructure security reform by effectively managing national security risk arising from ownership.

The proposed reforms also complement Australia's approach to countering foreign interference, which seeks to raise awareness and increase resilience in areas of society most at-risk of such activity.

The Bill before the committee proposes a new national security test which requires the mandatory notification of any proposed direct interest in a sensitive 'national security business' (including starting such a business). The definition of a national security business will be prescribed in the accompanying Regulation and will, among other things, include certain critical infrastructure assets as defined in the *Security of Critical Infrastructure Act 2018*. As the Minister for Home Affairs is empowered to add assets to this class of businesses under that Act over time, the Minister will have regard to the link to the *Foreign Acquisitions and Takeovers Act* and the implications for the foreign investment regime when considering adding assets to the *Security of Critical Infrastructure Act*.