BCA
Business Council of Australia

11 June 2021

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Dear Secretary

I am writing to provide further comments and recommendations in relation to the proposed reforms to the *Security of Critical Infrastructure Act* (SOCI Act) currently being considered by the Committee. These are in addition to the comments provided in our submission provided earlier this year.

The Business Council suggests several modest changes to the proposed reforms to the Act. These changes will serve to both lift the security and resilience of Australia's critical infrastructure. Businesses are ready to work with government because Australia cannot afford to leave critical infrastructure vulnerable and risk people's lives are disrupted.

A cooperative approach is the best way to boost industry partnerships and to enhance our security, while avoiding inefficient and costly red tape. Getting the settings right will ensure Australia is not only more resilient but is also seen as a favoured destination for investment – increasing both our security and prosperity.

Object of the legislation

The object of the legislation is being amended to remove 'national security', to reflect a broader purpose of the Act to manage a wide range of threats to a broad range of sectors across the economy.

This has the effect of substantially broadening the number of sectors captured. The object of the Act could be amended to highlight that the Act provides "a framework for managing risks relating to critical infrastructure *that is critical to the economic and national security of Australia*..."

This would provide businesses and investors with certainty about the kinds of infrastructure that are intended to be captured by the legislation.

Links to foreign investment

The revised legislation expands the definition of 'critical infrastructure' from the existing four (electricity, port, water or gas) to eleven broadly defined sectors. This will have flow on consequences for foreign investment, particularly through the *Foreign Acquisitions and Takeovers Act 1975* (the FATA). Section 8AA of the regulations that underpin the FATA define a 'national security business' as a responsible entity for or a direct interest holder in a critical infrastructure asset as defined under the SOCI Act.

Level 42, 120 Collins Street,
Melbourne VIC 3000

T 03 8664 2664
F 03 8664 2666

GPO Box 1472, Melbourne 3001
www.bca.com.au

reception@bca.com.au

Linking the definitions creates an unnecessarily high hurdle in a wide array of sectors for businesses to invest in Australia. The automatic and arbitrary tying of these two definitions is not fit for purpose regulatory practice.

The explanatory memorandum for the first exposure draft of the legislation released by Home Affairs highlighted that if a supermarket "were to subcontract out the trucking of groceries from a warehouse to a supermarket, then the trucking portion of the food and grocery network would still be considered a critical food and grocery asset". The potential consequence of this could see a ballooning in the number of entities affected by these reforms, with the attendant regulatory costs and consequences, particularly for SMEs.

This statement has subsequently been removed, and the Department of Home Affairs has released draft rules setting out the entities which could be captured under the revised SOCI Act which narrows down the affected entities. However, it highlights the flaws in linking the definitions of the SOCI Act and FIRB regimes.

Instead, we recommend the 'national security business' definition in Section 8AA of the *Foreign Acquisitions and Takeovers Regulations 2015* should retain 'critical infrastructure assets' as meaning the existing four sectors (i.e. electricity, port, water or gas). A broadening of the definition of critical infrastructure assets should only apply to foreign investment regulations where they are reviewed against foreign investment policy objectives, including consideration of the added complexity for foreign investment stakeholders, resource implications for the regulator (FIRB), and an overall assessment of the impact on Australia's foreign investment attractiveness.

Intervention requests

The Bill provides the Minister with 'step in' powers where an entity is 'unwilling or unable' to comply with a direction. It also explicitly removes judicial review of decisions made in responding to a cyber incident.

As we have noted above, businesses are ready to support government in lifting security and responding to cyber incidents. Much like in responding to a fire or other emergency, Australians expect that reasonable efforts are made to respond to cyber security incidents that threaten lives or critical infrastructure. However, Australians also expect that responses to these incidents will be conducted in a way that does not unreasonably disrupt other services or cause a business undue harm.

The operation of infrastructure systems and networks are complex and the available options or consequences of a particular course of action may not be immediately apparent to the Minister in issuing either a direction or step in notice. An operator may have an alternative view on the best way to handle an incident that would address the national security risks while also preventing unnecessary harm or damage to the operator's networks or infrastructure.

Section 317WA of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* provide for a designated entity to request for an assessment whether a technical capability notice should be given. This model could be applied to the revised SOCI Act, to allow for a competent independent assessor to quickly (ie. in less than 12 hours) determine whether an alternative solution is a more appropriate mitigation for an incident.

Oversight

The legislation includes a range of safeguards and oversight mechanisms, including consultation between ministers and requirements to notify the Inspector-General of Intelligence and Security. It also includes a

requirement for the head of Australian Signal Directorate (ASD) to provide a post-activity report to the Home Affairs and Defence ministers as soon as possible after intervening (and not longer than three months after).

These new powers will provide government with substantial and untested new powers. We have been reassured the new step in powers will be used as a power of last resort when there is no other recourse to resolve a threat to Australia's national security. Given both the novelty and seriousness of any use of the step in powers, we recommend including a clause in section 35BH requiring the head of ASD to also provide the post-activity report (or similar document) to both the Prime Minister and the Parliamentary Joint Committee on Intelligence and Security. The report should provide a rationale for the actions taken by ASD if a critical infrastructure operator has disagreed with the requested approach, and the actions taken to ameliorate any reasonable concerns raised by the entity.

This will provide assurance to both the chair of the National Security Committee of Cabinet and the Parliament that national security risks to Australia's critical infrastructure have been addressed.

Immunities

Within the Bill there is currently no general immunity from suit or liability for staff, officers, and directors of the regulated entities under the Act. The BCA recommends that express immunity be granted to officers, directors, staff, and contractors who provide assistance or carry out activities that support the directions or instructions as given or issued pursuant to the Act (provided these are undertaken in good faith).

Such immunity should extend to all actions under the Act (not only in relation to a direction given by the Minister or for reporting of an incident). The revised Act does not, for example, provide immunity from suit or liability where an intervention request is made under section 35AX (the intervention / step in powers).

The express immunity would support compliance with the regime, by removing scope for argument and potential for ambiguity in what are complex working combinations of obligations that may be imposed under the Act. As noted above, responding to security incidents may involve decisive action with limited information and time to consider some of the factual or technical intricacies and possible unintended consequences. The Banking Act provides a good example of some of the immunities to be granted (see section 70AA).

Notification of cyber security incidents

As part of the Positive Security Obligations, entities can be required to comply with a reporting obligation for cyber security incidents. This includes a requirement to provide the Commonwealth with information (to be specified in subordinate rules) about any cyber security incidents that will have a significant impact on the availability of an asset with 12 hours.

This is inconsistent with similar jurisdictions (such as the UK) and other comparable domestic regimes (such as those managed by APRA), which require reports to be made within 72 hours.

Responding to cyber security incidents may require swift resolution to prevent undue harm to Australians or our national security. However, a requirement to furnish the Commonwealth with information about an incident may be unreasonable, particularly in instances where corporate systems are also unavailable or the specifics of the incident are still unclear.

Instead, it may be appropriate for entities to be required to provide an initial notification that an incident has taken place within 12 hours, with specific information as prescribed under the rules within 72 hours.

Consultation with other regulators

The revised legislation will provide the Minister for Home Affairs with substantial powers to prescribe or declare additional assets, where the Minister is satisfied the asset is critical to the social or economic stability of Australia or its people, the defence of Australia or national security.

Many of the proposed sectors are already highly regulated, including on the price of the services offered to consumers or on maximum revenue (such as for the energy network). This means that additional compliance costs from the SOCI Act (which would generally be passed on as costs for all consumers) will instead have to come from foregone investment or reduced efficiency and competition as it becomes increasingly unattractive for operators to participate in the market.

Existing regulators should be consulted on relevant decisions made under the SOCI Act to ensure they can consider potentially substantial regulatory compliance costs in making determinations relevant to their sector.

However, if there was not any inclination to require consultation with relevant regulators, the Act could instead require the Minister to consider the effects on the efficiency of and competition in the relevant sector ahead of 'turning on' any rules or designating a System of National, similar to the requirements under the TOLA Act (Section 317TAAA(6)(c)). This clause should be included at section 52B(2) at minimum, which outlines the considerations the Minister must have regard to before declaring a System of National Significance.

I trust this information is useful in the committee's consideration of the reforms to the SOCI Act. I have set out our six key recommendations in the one pager attached.

Yours sincerely

[redacted]

Jennifer Westacott
Chief Executive
Business Council of Australia

BCA
Business Council of Australia

Level 42, 120 Collins Street,
Melbourne VIC 3000

GPO Box 1472, Melbourne 3001
www.bca.com.au

T 03 8664 2664
F 03 8664 2666

reception@bca.com.au

Recommended changes to the SOCI Act

1. The object of the Act should be amended to highlight that the Act provides "a framework for managing risks relating to critical infrastructure *that is critical to the economic and national security of Australia*..."
2. The definition of 'national security business' in Section 8AA of the *Foreign Acquisitions and Takeovers Regulations 2015* should not be updated automatically with reference to the SOCI Act, and should instead retain the existing four sectors (i.e. electricity, port, water or gas).
3. In instances where there is a dispute about the appropriate mitigation to a cyber incident, the Act should provide for a competent independent assessor to determine within 12 hours whether an alternative solution put forward by the critical infrastructure owner or operator is a more appropriate mitigation for an incident.
    a. This could be modelled after the provisions in section 317WA of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.
4. An additional clause in section 35BH should be inserted to require the head of ASD to also provide the post-activity report (or similar document) to both the Prime Minister and the Parliamentary Joint Committee on Intelligence and Security.
    a. The report should provide a rationale for the actions taken by ASD if a critical infrastructure operator has disagreed with the requested approach, and the actions taken to ameliorate any reasonable concerns raised by the entity.
5. Express immunity should be granted to officers, directors, staff, and contractors who provide assistance or carry out activities that support the directions or instructions as given or issued pursuant to the Act (provided these are undertaken in good faith). This should extend to all actions under the Act.
    a. Such provisions could be modelled after the Banking Act (section 70AA).
6. The Act should require the Minister to consider the effects on the efficiency of and competition in the relevant sector ahead of 'turning on' any rules or designating a System of National, similar to the requirements under the TOLA Act (Section 317TAAA(6)(c)).
    a. This clause should be included at section 52B(2) at minimum, which outlines the considerations the Minister must have regard to before declaring a System of National Significance.

BCA
Business Council of Australia

Level 42, 120 Collins Street,
Melbourne VIC 3000

GPO Box 1472, Melbourne 3001
www.bca.com.au

T 03 8664 2664
F 03 8664 2666

reception@bca.com.au