BCA
Business Council of Australia

Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

February 2021

Contents

1. About this submission

This is the Business Council's submission to Parliamentary Joint Committee on Intelligence and Security regarding the Bill seeking to amend the *Security of Critical Infrastructure Act 2018* (the SOCI Act). The Bill will implement an enhanced framework to uplift the security and resilience of Australia's critical infrastructure.

2. Key recommendations

As noted in our previous submissions on these reforms, the Business Council supports the Government's goal of protecting essential services by uplifting the security and resilience of critical infrastructure.

Our key recommendations include:

1. As set out in our submission on the FIRB reforms, the definition of a 'national security business' should be explicitly spelt out in the updated FIRB legislation per the current definition in the SOCI Act, with no 'automatic update' by reference to a revised SOCI Act.
2. Any prescription or declaration of a 'critical asset' be undertaken in consultation with the Treasurer and relevant sectoral regulator. Additionally, prior to declaring a 'critical asset', 'turning on' any rules that apply to a sector, or designating a System of National Significance, the Minister for Home Affairs should be required to consult with the relevant sectoral regulator.
3. The cyber incident reporting requirements should be further developed to allow for information to flow between government and industry, rather than the current one-way reporting regime.
4. The requirement for notification of a critical cyber security incident should be reported within 12 hours to be revised to 72 hours, to align with other domestic and international requirements.
5. Government directions or direct action should be subject to quick appeal to an independent, but suitably qualified and cleared assessors, similar to the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.
6. 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.
7. In addition to the Home Affairs and Defence ministers, the head of Australian Signals Directorate (ASD) should provide a post-activity report to the Prime Minister and the Parliamentary Joint Committee on Intelligence and Security whenever government intervenes in a critical infrastructure sector.

3. Overview

The Business Council's previous submissions on these reforms have noted some of the cross-sectoral issues that would need to be addressed to deliver an effective regime to protect critical infrastructure and systems of national significance. We are not providing comment on the reviews of the SOCI Act or Telecommunications Sector Security Reforms (TSSR). This submission is intended to complement submissions made by individual businesses and other interested bodies, who are best placed to provide detailed responses on each of the sectors that have been identified and the reviews of the SOCI Act and TSSR.

We welcome the Minister's commitment to work with industry to make Australia's critical infrastructure as resilient as possible. Continuing to take a cooperative approach between business and government on these reforms will support industry partnerships and enhance our security.

We appreciate the changes the Government has made in response to the feedback it has received from industry, including those recognising the importance of avoiding duplication with existing regulation. We continue to strongly support the reuse of existing domestic and international standards wherever possible, and the harmonisation of relevant standards, such as those set by APRA, existing ISO standards and others.

The security uplift sought by this legislation is likely to be initially beyond the ability of some sectors to achieve (noting some sectors are also highly mature and have made substantial investments). Increasing the level of security of less mature sectors may be a multi-year journey that will require substantial investment. We support the Government working with industry to quickly clarify expectations for each sector to ensure investments can be planned and made well in advance.

The Business Council welcomes the Committee considering these reforms and recommends a close consideration of feedback provided by all sectors. Many of the key details and rules within the reforms are being left to industry co-design. We commend the Department of Home Affairs for taking an approach that involves close cooperation with industry in developing workable rules. Providing as much transparency on the industry co-design process will support industry certainty.

These are foundational reforms for Australia and will have substantial implications for both our security but also our ongoing economic prosperity. Both of these factors should be taken into account. Some of the new powers are, for example, a substantial increase in government's ability to intervene in what are global assets and services. The new powers will potentially open access to user, commercial and system data of citizens and businesses located in other countries. Given these powers will affect users in jurisdictions outside of Australia, it is not clear how these powers will interact with requirements under relevant US and European laws, such as privacy statutes and similar regulations. This may have a negative effect on business investment decisions on where to locate data centres or cloud services, particularly those necessary to support markets in Asia. While Australia will not lose access to the services hosted in these centres, it may be that Australia increasingly becomes an importer, rather than exporting the services. Getting the frameworks supporting these powers right will be vital to the success of these reforms.

4. Comments and Recommendations

4.1 Defining 'critical infrastructure' sectors and assets

The Bill substantially expands the sectors deemed 'critical infrastructure' and notes the government's intention to provide powers to designate specific assets as 'critical infrastructure sector assets' and 'systems of national significance'.

The explanatory memorandum and Bill provide substantial detail on the sectors that will be covered and how assets will be determined. Given the wide range of sectors and assets affected, we are not providing specific comments on each of the sectoral definitions.

4.1.1 Links to FIRB

We continue to recommend the definitions of 'critical infrastructure' under the SOCI Act and 'national security business' used by FIRB should be disentangled.

The policy objectives of these two pieces of legislation are substantially different and the current approach will lead to an unreasonably large number of entities being captured as 'national security businesses'. The

expansion of the definition in the SOCI Act (which currently covers the electricity, ports, gas, and water sectors) will broaden the scope dramatically.

The current approach – of linking the definitions between the Acts – will create 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.

4.1.2 Declaration of a 'critical asset'

The Bill notes the Minister for Home Affairs will have discretion to prescribe or declare additional assets (beyond those already defined in the legislation). To make this determination, the Minister must be satisfied the asset is critical to the social or economic stability of Australia or its people, the defence of Australia or national security.

Prescribing or declaring an asset will potentially have wider consequences, including additional regulatory and compliance costs, implications for competition in the market and foreign investment (as noted above), among others.

For this reason, the Business Council recommends the Minister be required to consult with the Treasurer and relevant sectoral regulator. Additionally, prior to making this declaration, 'turning on' any rules that apply to a sector, or designating a System of National Significance, the Minister should be required to consult with the relevant sectoral regulator.

4.2 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. There is risk this reporting requirement will create a substantial compliance overhead for industry. It could also potentially run counter to existing responsible vulnerability disclosure schemes already operated by industry. Consideration should also be given to, where appropriate, ensuring the protection and privacy of an organisation that has suffered a cyber security incident.

The Business Council supports information sharing being a two-way flow between government and industry, to best support security uplift across the economy. The regime being established only goes to industry reporting to government. We recommend this element of the reforms continue to be refined to ensure both government and industry can benefit from these information sharing arrangements. De-identification of shared information may support swifter sharing, particularly if it is intended to be shared with third parties.

We also recommend the Committee consider whether the reporting timeframes are reasonable and proportionate. The legislation requires a report within 12 hours, however other similar jurisdictions (such as the UK) require reports to be made within 72 hours. Similarly, requirements under other Australian regulatory regimes (such as those managed by APRA) impose a 72-hour reporting window. Consistency both domestically and internationally will ensure businesses can have confidence in their ability to comply with regulatory regimes.

4.3 Responding to cyber security incidents

The Bill sets out in detail powers the Minister has to authorise any actions under the regime in responding to a cyber security incident. These include:

- giving directions to a specific entity for the purpose of gathering information,
- giving specified directions to an entity to do one or more things to respond to an incident for the entity to take actions, or

- giving request to the authorised agency (the ASD, including the Australian Cyber Security Centre (ACSC)) to provide specified assistance and cooperation to respond to the incident.

We are supportive of these powers only being used in the most serious of circumstances where Australia's national interests are being seriously prejudiced. We also support the Minister being required to consider whether other existing regulatory regimes could provide an effective response.

4.3.1 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.

The operations of infrastructure systems and networks are complex and the available options or consequences of a particular course of action may not be immediately apparent. The Committee may wish to consider whether the drafting allows for scenarios where an entity or operator supports taking action to remedy a cyber incident but, given their greater knowledge of their own networks and interdependencies, disagrees that the government's direction is the best way to deal with the incident.

This could include provisions like those provided in the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA). These provide for a designated entity to request for an assessment whether a technical capability notice should be given.

It would be appropriate for infrastructure operators to be able to make a quick appeal whether a given direction is the most appropriate mitigation for an incident. Like under TOLA, this should be reviewed by independent, but suitably qualified and cleared assessors.

4.3.2 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 that these activities or tasks, including omissions, if any, are undertaken in good faith).

Such immunity should extend to all actions under the Act (not only in relation to subsections 35AAB(2), 35AW(2), 35BB(5) and 30BE(2) of the Act). 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 sections 70AA(1)(c) and 70AA(3)).

4.3.3 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 ASD to provide a post-activity report to the Home Affairs and Defence ministers as soon as possible after intervening.

Given the substantial and new intervention this represents, we recommend this report also be provided to the Prime Minister, and to the Parliamentary Joint Committee on Intelligence and Security.

BUSINESS COUNCIL OF AUSTRALIA

42/120 Collins Street Melbourne 3000 T 03 8664 2664 F 03 8664 2666 www.bca.com.au