BCA
Business Council of Australia

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Submission to the PJCIS

March 2022

Contents

1. About this submission 2
2. Key recommendations 2
3. Overview 2
4. Key points 3
   4.1 Areas for additional improvement 3
      4.1.1 Positive Security Obligations 3
      4.1.2 Systems of national significance and related powers 4
   4.2 Improvements to already-legislated powers 4
      4.2.1 Government Assistance Measures 4
      4.2.2 Definitions 5
   4.3 Need for early review of the Bill 5

1. About this submission

This is the Business Council's submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) regarding the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022.

The Business Council represents businesses across a range of sectors, including manufacturing, infrastructure, information technology, mining, retail, financial services and banking, energy, professional services, transport, and telecommunications.

2. Key recommendations

The Business Council recommends:

1. Using this opportunity to address concerns about the already-legislated powers, including:
    a. providing businesses with the option to seek quick appeal where there is disagreement about whether a government direction or intervention is the best way to deal with an incident, and
    b. amending definitions for some sectors, such as the data storage and processing sector, to better target their scope.
    c. that a 'national security business' should be explicitly spelt out in the updated FIRB legislation, with no 'automatic update' by reference to a revised SOCI Act.
2. Making minor amendments to the proposed new obligations in this Bill to ensure the new requirements effectively deliver enhanced security without creating undue regulatory burdens:
    a. Removing the ability of the Secretary to require the installation of software on a system of national significance (section 30DJ).
    b. Government having an ongoing role of working with employers and employee representatives on any new obligations for employee screening, including through AusCheck.
    c. Excluding assets that are nearing end of life from any new rules or obligations, to ensure their final years of operation are not rendered uneconomic.
3. Reviewing the wide range of reporting requirements for cyber incidents with a view to rationalisation.
4. If passed, including an early review of the Act, to ensure emerging technologies can be accounted for, definitions can be updated to exclude from coverage under the Act where appropriate, and business can provide further feedback on the efficacy and regulatory burden of the new powers that have been created.
5. Consideration of existing cyber security skills shortages in both compliance measures, but also as a priority issue to address more broadly.

3. Overview

As we have highlighted in our previous submissions to the Department of Home Affairs and the PCJIS, the Business Council supports the government's ambition to build critical infrastructure security and resilience. Businesses are ready to work with government on this, as Australia cannot afford to leave critical infrastructure vulnerable and risk serious disruption to businesses and people's lives.

We welcome the Committee's consideration of the Bill, which updates the *Security of Critical Infrastructure Act* and the draft asset definition and risk management program rules. The changes that are the subject of this

exposure draft (Bill Two) will introduce the Risk Management Program (an addition to the Positive Security Obligation) and introduce enhanced cyber security obligations. The proposed changes build on the changes that were legislated in December 2021 (Bill One), which, among other things, expanded the definition of 'critical infrastructure' from four to eleven sectors, and established cyber incident reporting and government assistance measures.

The reforms were split into two in response to recommendations made by this Committee, to allow for further consultation with affected industries and representative bodies. In addition, the Committee recommended the rules that underpin Bill Two be co-designed, agreed and finalised to the extent possible before reintroduction of Bill two. This was intended, among other things, to allow for the "fullest consultation and establishment of regulatory impacts to be established" before Parliament considered the reforms.

In our view the Department has, within the timeframes allowed, sought to undertake further and inclusive consultation. We note the Department has held multiple open townhalls for affected businesses to provide feedback and seek clarification on the proposed approach and have appreciated their willingness to meet with our members directly. We appreciate the changes that Home Affairs has made in response to the feedback provided by businesses, including to some of the definitions of critical infrastructure assets and expanding the scope of immunities availably to responsible entities and their employees.

Unfortunately, due to the compressed timeframes the Department is seeking to meet to introduce Bill Two, there are still areas where businesses remain unclear on the implications of the proposed approach, or where the regulatory costs are still to be determined. We also consider areas remain that could be improved, in both the proposed Bill and the reforms that have already been legislated – particularly the government assistance measures. We continue to think that greater oversight of these powers and opportunities for businesses to work with government will be critical to balancing the needs of government, business, and the community.

We also urge the Committee and Government to be mindful of other constraining factors in the practical implementation of this Bill. Cyber security remains top of mind for all business leaders. One of the key barriers to achieving better security outcomes remains a lack of skilled cyber security workforce and expertise at all levels. For many businesses, there is not sufficient skilled workers to meet existing needs – new requirements will create additional pressure. While the Committee has not sought comment on this as part of its inquiry, it will remain a substantial factor in the success of these reforms. Further government action to meet these skills needs will be critical.

This Bill will create substantial new obligations for a large part of the economy. The costs of the requirements that have been enacted and that are being proposed will not be insignificant and will potentially be borne by all Australians through higher prices for goods and services. We strongly support the Committee's consideration of the views provided by all stakeholders as to whether the Bill has struck the right balance: getting this right will be critical to Australia's future prosperity.

4. Key points

4.1 Areas for additional improvement

4.1.1 Positive Security Obligations

We have previously advocated for any new obligations created under this legislation to align as much as possible with existing international standards. We have appreciated the Department's assurance that the intention is to not create unnecessary Australia-specific rules. Taking this approach will ensure Australian businesses do not face additional regulatory costs when looking to operate overseas, and that international businesses do not have unreasonably high barriers to creating jobs in Australia.

We also appreciate the consultation that has already taken place on the risk management program rules through late 2021 and early 2022.

The rules may require a risk management program to include one or more provisions permitting a background check of an individual under the AusCheck scheme. As we highlighted in our submission to the Department in early 2022, it would be sensible for government to continue to engage with employee representatives and provide a central point of coordination on these requirements, to ensure any concerns businesses and their employees have about this requirement are being managed consistently.

4.1.2 Systems of national significance and related powers

The thresholds and criteria for businesses that may be identified as a 'system of national significance' remain unclear. Because of this, the regulatory costs of these reforms are challenging to determine. However, for those entities designated as a system of national significance, it will be high. This includes both financial and other costs to implement requirements such as providing 'real time' system information or undertaking vulnerability assessments that meet government requirements. Similarly, legal concerns (such as intellectual property rights for proprietary systems) will need to be worked through, which may be additionally challenging for global businesses working in Australia.

Further, the new Section 30DJ of the SOCI Act allows the Secretary to require the installation of specified computer programs on a system of national significance. The Bill explains this is intended only for the Australian Signals Directorate (ASD) to have an enhanced threat picture and to develop mitigations and advice for the entity. The potential costs of the use of this kind of power are well beyond the possible benefits. The explanatory memorandum suggests this will be a simple installation of a computer program. However, this may create unintended conflicts with existing software used by the provider, threatening the stability of the service.

More importantly, it will create concerns for international businesses considering investing in Australia or considering purchasing Australian based services. While the ASD does not have a regulatory role, it is Australia's signals intelligence collection agency. The ability to compel businesses in Australia to install computer programs will raise concerns (however unfounded) that a business has been suborned to support the collection of intelligence, potentially jeopardising the ability of Australian based businesses and services from competing internationally.

Many businesses are developing investment and business cases based on the requirements set out in Bills one and two. Potential designation as a system of national significance will potentially affect these considerations substantially and may affect decisions to invest in or use services based out of Australia. Businesses would welcome quick clarity where government may be considering their designation as a system of national significance, and a clear definition of the outcome government wants to see achieved where a designation is made. This will help ensure businesses are able to meet requirements efficiently and effectively.

4.2 Improvements to already-legislated powers

4.2.1 Government Assistance Measures

We have previously argued for the government assistance measures to include a 'right of reply'. This should allow 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, as it may cause greater damage or harm.

We acknowledge the government's view that this is intended to be used as a 'last resort' and only in the most critical of circumstances. We also accept that it was the key change that required the expeditious passage of the reforms last year, and that this meant that this type of proposal (suggested by organisations like the BCA and other bodies) were not incorporated.

However, given the powers have now been legislated, this second Bill is a good opportunity to make changes that better balance the legitimate interests of businesses that might be subject to government intervention. Existing provisions are already included in other legislation, such as the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA). TOLA provide for a designated entity to request for an assessment whether a technical capability notice should be given.

We continue to recommend that infrastructure operators be able to make a quick appeal as to 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. Any authority to compel or require businesses to take any actions through either the directions or intervention powers should also be explicitly required to be in line with the Act's objectives.

4.2.2 Definitions

This Bill is also a chance to address some challenges with definitions that have already been created. This includes building in an exclusion for the reforms for critical infrastructure assets that are going to be retired in the near future or shortly after imposition of any legislated requirements. The implementation costs of these reforms for many sectors will be high. Including assets near the end of service life in the regime may see jobs lost and services cut off when the regulatory costs make keeping them in operation uneconomic.

Similarly, for the definitions of 'data storage or processing service' and 'data storage and processing asset' – we recommend retaining the 'wholly or primarily' requirement when determining the eligibility of the asset. This would better target the legislation and avoid inadvertently capturing many unrelated businesses.

As we have advocated throughout this and related processes, we also continue to recommend government disentangle the definition of 'national security business' in the FIRB Act from critical infrastructure legislation. As we have stated throughout the development of these reforms, 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' and increasing the hurdle for businesses looking to invest in Australia.

4.3 Need for early review of the Bill

If the Committee supports the passage of the Bill and it receives passage through Parliament, we recommend an early review of the legislation be undertaken. This should have a view to addressing any implementation challenges businesses are facing in meeting new requirements, amending definitions to remove businesses that have inadvertently been included within the legislation, and adjusting legislated requirements to meet evolving markets and challenges.

For example, as sectors evolve or new technologies emerge, new 'critical' services may emerge. It is not clear how the reforms contemplate distributed assets (such as virtual power plants) for example, which may constitute increasingly large parts of the relevant markets. This would also provide an opportunity for sectors and assets which no longer need to be covered by the Act to be removed from the regime.

It would also provide an opportunity to consider the effectiveness and utility of the multiple cyber incident reporting obligations that are being imposed, including through existing mechanisms (such as this legislation, sector specific requirements, or the notifiable data breach scheme) and possible new mechanisms (such as the recently announced mandatory ransomware reporting scheme or revised obligations following the review of the Privacy Act). We support government considering how best to develop a 'single touch' reporting scheme – in the event of a cyber incident, businesses should be focused on restoring services to Australians, not meeting compliance requirements.

BUSINESS COUNCIL OF AUSTRALIA

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