BCA

Business Council of Australia

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Submission in response to Exposure Draft

February 2022

Contents

1. About this submission

This is the Business Council's submission in response to the exposure draft of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022. This submission also provides feedback on the critical infrastructure asset definition rules, and the risk management program rules.

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 government continue to work closely with affected businesses to provide clarity and certainty on the requirements these reforms will impose for both entire sectors and individual businesses.

We also make a number of specific recommendations:

1. Government continue to work in the spirit of the recommendations made by the Parliamentary Joint Committee on Intelligence and Security, and ensure parliament is able to take future decisions based on the fullest consultation and understanding of regulatory costs as possible.
2. Consideration of existing cyber security skills shortages in both compliance measures, but also as a priority issue to address more broadly.
3. Taking this opportunity to address concerns about the already-legislated powers, including 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.
4. Narrowing the scope of incident reporting requirements to only require reporting where an incident is occurring in or affecting Australia.
5. Reviewing the wide range of reporting requirements with a view to rationalisation.
6. Clarifying areas of uncertainty in definitions (such as whether physical records are considered 'data' or how shared systems should be considered).
7. Retaining the 'wholly or primarily' component of the definition for the data storage and processing sectoral definitions.
8. Limiting the definition of 'critical data storage or processing assets' to those managing 'business critical data', even if the asset is being provided to government entities.
9. Include an ongoing review process of the definitions, to ensure emerging technologies can be accounted for and sectors can be removed from regulation where appropriate.
10. 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.
11. 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. Overview

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 opportunity to provide further feedback on the newest Bill updating 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.

While we support the government's ambition, we continue to believe there are areas where already-legislated reforms could be improved – particularly for the government assistance measures. We continue to think that greater oversight and opportunities for businesses to work with government will be critical to balancing the needs of government, business, and the community.

We also welcome the substantial consultation that has been undertaken by the government, including the Department of Home Affairs, on these reforms. We appreciate the changes that have already been made following feedback from business and the community since the reforms were first unveiled in 2020, including to incorporate additional protections for businesses responding to a direction from the Minister. Given the substantial scope and complexity of these changes, we look forward to working with the government on these reforms.

The reforms were split into two in response to recommendations made by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). The Committee recommended the second Bill (the subject of this consultation process) be released as "an exposure draft for extensive consultation with affected industries and representative bodies, with follow-up consultation meetings to be held on the collective feedback received from that exposure draft process." 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. We continue to believe this approach remains sensible, and we encourage the government to work in the spirit of the Committee's recommendation.

For these reforms to be successful, government will also need to consider its practical implementation. A substantial part of the reforms focuses on lifting the cyber security of Australia's critical infrastructure. Cyber security remains top of mind for all business leaders, but one of the main barriers to reform remains a lack of skilled cyber security workforce and expertise at all levels. For many businesses, there is not sufficient skilled workers to deliver on existing requirements, let alone any further obligations imposed by this legislation. We strongly recommend the government consider this constraining factor in timing any compliance measures, but also as part of wider efforts to attract, train, and retain the cyber security workforce Australia needs.

These are landmark reforms that will be foundational to a large part of the economy. The requirements that have been enacted and that are being proposed will not be free. The costs of these reforms will not be low and will potentially be borne by all Australians through higher prices for goods and services. It will be critical to Australia's future prosperity that we get this legislation right.

4. Key points

4.1 Government assistance measures

As noted above, the government assistance measures were legislated in December 2021. This provides the Minister with 'step in' powers where an entity is 'unwilling or unable' to comply with a direction in responding to a cyber incident. Businesses from across many sectors have highlighted their willingness to work with government in responding to potentially catastrophic cyber incidents. The government has noted this is intended to be used as a 'last resort' and only in the most critical of circumstances, but that it was the key change that required the expeditious passage of the reforms. We understand this meant that some of the changes suggested by organisations like the BCA and other peak bodies were not incorporated.

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.

As we have previously noted, 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 step-in powers 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.

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.

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. 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 objectives of the Act.

4.2 Incident reporting

As part of Bill one, mandatory cyber incident reporting obligations were imposed. We have welcomed the government's changes to the timeframes for reporting these incidents. The government is now seeking feedback on the proposed extension of these requirements to a number of critical asset classes.

The current drafting of the legislation could be helpfully narrowed – currently the legislation requires the reporting of all incidents that have a significant impact, which may have knock on impacts where global organisations have to report incidents reported in other jurisdictions that do not affect Australia or Australians. We recommend government narrow the scope of the reporting requirements to only require the reporting of incidents that are, or could reasonably be supposed to be, affecting the provision of goods or services in Australia.

More broadly, we recommend government consider how best to rationalise the wide range of reporting schemes which exist or are being developed. These include not only the requirements imposed through the critical infrastructure act, but also the notifiable data breaches scheme, sector specific requirements, and the recently announced mandatory ransomware reporting scheme, along with the range of various state and territory disclosure requirements. While each of these reporting schemes have different policy intents, it would be sensible to limit the number of reports a business has to make, particularly during a potential crisis. We suggest government undertake a review of the various reporting requirements and consider how best to develop a 'single touch' reporting scheme.

4.3 Definitions

We continue to consider the definitions that underpin the Act could continue to be updated to reflect industry feedback.

There remain areas where the definitions are still unclear. For example, it's not apparent whether the intention is to exclude physical record archives. The exposure draft explanatory document refers to computerised data but the exposure draft refers to data. Similarly, government will need to provide clarity on how businesses with shared systems will be managed (e.g. for energy businesses with shared generator or retailer systems).

Further, the proposed changes appear to confirm that that all forms of 'as a service' computer services are captured. The requirements to notify data storage and processing suppliers are based on business-critical data. Given the size of some organisations using thresholds of 20,000 individuals is quite low, and may inadvertently capture a larger portion of the economy than necessary. In addition, some elements of business-critical data (e.g. risk management information) do not have the same context across different industries.

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 not inadvertently capture many unrelated businesses. Similarly, to ensure the regulation is proportionate and well targeted, the definition should be amended to only capture assets managing 'business critical data', even if the asset is being provided to government entities.

It would also be helpful to build in an ongoing review process for the definitions of what constitutes a 'critical infrastructure' asset. 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.

Lastly, we continue to recommend government disentangle the definition of 'national security business' in the FIRB Act from critical infrastructure legislation. 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.

4.4 Enhanced cyber security obligations and positive security obligations

In line with our previous recommendations, we continue to recommend the government ensure that any new obligations created under this legislation align as much as possible with existing international standards. We have appreciated the government'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 recommend building in an exclusion for the reforms for critical infrastructure assets which 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.

While many of the rules for specific sectors are being developed, it would be helpful for government to provide as much notice and 'grace periods' for any future updates that lift the bar. Part of the attraction of Australia as a location to invest is the certainty and stability provided by government. For businesses developing investment cases, sudden changes create additional risk. This may deter job and wealth creating investments.

To provide businesses with additional certainty, it would also be helpful for government to clarify several aspects of the Positive Security Obligations, including for the Risk Management Program. For many sectors, it remains

unclear what additional uplift may be required where existing regulations are already in place (or if indeed these obligations are considered sufficient as a baseline across an industry).

Where there are rules that are considered 'sufficient', it would be helpful for government to clarify how it expects additional risks or hazards will be considered. It would not be sensible to 'layer' additional rules on top of existing requirements to address other risks. It may be helpful for government to confirm that risk information is being shared across regulators to ensure possible new or emerging hazards are being factored into sector specific regulations.

The rules may also require a risk management program to include one or more provisions permitting a background check of an individual under the AusCheck scheme. 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 employees may have about this requirement are being managed consistently.

Finally, it would also be helpful for government to clarify whether it expects the risk management program to be approved by the Board, Council, or other Governing Body to allow for an operational senior management forum (as opposed to a Board level governance body such as a Board Risk Management Committee) to approve.

Given the lack of clarity on these points, we also recommend government extend the 'grace period' for achieving compliance with the risk management programs from six months to 12.

4.5 Systems of national significance

The thresholds and criteria for businesses that may be identified as a 'system of national significance' remain unclear.

As noted above, the implementation costs of these reforms will be high, and designation as a system of national significance will be even higher, including to implement requirements such as providing 'real time' system information or to undertake 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.

As noted above, many businesses are developing investment and businesses 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.

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.

BUSINESS COUNCIL OF AUSTRALIA

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