Business Council of Australia

SUBMISSION

Protecting Critical Infrastructure and Systems of National Significance

September 2020

Business Council of Australia ABN 75 008 483 216

CONTENTS

ABOUT THIS SUBMISSION

This is the Business Council's submission to the Department of Home Affairs in response to the Protecting Critical Infrastructure and Systems of National Significance Consultation Paper.

In August 2020, as part of Australia's Cyber Security Strategy 2020, the Government announced it was introducing a new security framework for critical infrastructure. This is intended to bolster the nation's resilience and give the Government powers to act quickly in an emergency.

KEY RECOMMENDATIONS

The Business Council supports the Government's goal of protecting essential services all Australians rely on by uplifting the security and resilience of critical infrastructure. Given the wide scope of these reforms and potential consequences for Australia's security and economic future, Business Council members look forward to working through the detail with the Department to design a workable and effective framework in accordance with best practice regulatory principles.

Our key recommendations include:

1. The listed sectors are a substantial expansion of the existing definition of what constitutes 'critical infrastructure' and could capture most businesses within the economy We recommend appropriately targeting the definition of 'critical infrastructure' to account for whether legislation and regulation are the best way to achieve security uplift.
2. Existing frameworks and standards should be used and not replaced with requirements under a revised Security of Critical Infrastructure Act (SOCI Act).
3. Any new regulatory requirements should recognise and minimise the cross sectoral impacts for both critical infrastructure entities and businesses in the supply chain.
4. New obligations under the Positive Security Obligations should be proportionate to the risk and recognise the need to maintain affordable services.
5. Regulators' roles should be clearly defined and they should be appropriately resourced to oversee new obligations.
6. Establishment of a working group to provide further advice.

OVERVIEW

The Government is consulting on the details of agreed reforms to protect critical infrastructure and systems of national significance.

The Government is intending to introduce an enhanced regulatory framework for critical infrastructure operators. The framework will apply to a wide range of sectors, and include:

- a positive security obligation for regulated critical infrastructure entities;

- enhanced cyber security obligations for entities most important to the nation; and
- Government assistance to entities in response to cyber-attacks on Australian systems.

Though the reforms were announced as part of the Cyber Security Strategy, their scope extends beyond cyber security. The consultation paper notes, for example, new Positive Security Obligations will cover cyber security, as well as the security of information, personnel, and supply chains.

The reforms are also a substantial expansion on the existing legislation, both in what it applies to and the risks it seeks to manage. The proposed reforms expand what is considered 'critical infrastructure': the revised definition could include a substantial number of businesses in the Australian economy. It also expands the risks being managed from 'national security' (espionage, sabotage, coercion) to 'all hazards'.

Given this wide scope, this submission provides a macro perspective and identifies some of the cross-sectoral issues which need to be addressed to deliver an effective regime that encourages economic growth while managing potential risks. It is intended to complement submissions made by individual businesses and other interested bodies, who are best placed to provide detailed answers to the questions posed in the consultation paper.

We note the Parliamentary Joint Committee on Intelligence and Security is currently undertaking a review of the Telecommunication Sector Security Reforms. The SOCI Act also requires the Committee to begin a review of the SOCI Act three years after it received Royal Assent (April 2018 – a review is required to commence before April 2021). The proposed reforms are being progressed ahead of these reviews. It may be more appropriate for any reforms to be held over until these reviews are completed. This is particularly important given the proposed approach expands requirements across a large portion of the economy.

In the context of recovery from both the recent bushfires and the ongoing economic and health crises, Government has taken action to support economic recovery. This included early regulatory changes in respond to COVID-19 to provide greater flexibility and protections to keep businesses operating. This approach should be maintained: well-intentioned regulation still puts a damper on economic activity and business investment when it is onerous or disproportionate to the policy problem. This will ultimately lead to a deterioration of Australia's prosperity and security.

Even prior to the ongoing COVID crisis, investment was relatively weak, especially outside the mining sector. For this reason, adherence to best practice regulatory principles will be vital to the success of the proposed reforms. Any new requirements should be efficient, proportionate and balanced, to ensure Australia remains an attractive place to invest and do business.

Many businesses already manage hazards across the spectrum as a routine part of their business. Any new regulations should be complementary to existing efforts and where there is a demonstrated need and avoid attempting to manage every possible risk (such as food security), as this would make a regime unworkable. A central focus should be maintained on protecting against national security risks.

The security of critical infrastructure and systems of national significance will be an ongoing process. The protection of critical infrastructure will need to evolve as possible hazards emerge and change. Government could consider starting with pilot regulations to test the efficacy and efficiency of any changes or additions.

We welcome the substantial consultation the Department of Home Affairs has undertaken as part of this consultation paper process. These reforms will still require further development, including through legislative drafting and the development of regulation. We support Home Affairs establishing a working group to bring together experts from government, industry, regulators, and other interested parties. This working group could provide a forum to work through the development of these important reforms, in addition to further consultation.

COMMENTS AND RECOMMENDATIONS

The Act should be appropriately targeted

The consultation paper notes the reforms will impose security obligations on a number of sectors: banking and finance; communications; data and the cloud; defence industry; education; research and innovation; energy; food and grocery; health; space; transport; and, water. As noted earlier, the listed sectors are a substantial expansion of the existing definition of what constitutes 'critical infrastructure' and could capture most businesses within the economy.

The consultation paper also notes the Government will classify entities within three broad categories: critical infrastructure entities; regulated critical infrastructure entities; and systems of national significance. We support the use of a gradated approach that allows for intervention and obligations proportionate to the policy problem.

In determining what should fall within each category, the consultation paper notes two factors will be considered: its interdependency with other functions, and the consequence of any compromise.

Additional factors should also consider whether legislation and regulation is the best way to address this policy problem, and whether there is sufficient case for any government intervention. To this end we recommend two additional factors be considered:

- Whether sectors are already meeting comparable requirements under existing regulation or as part of their routine business; and
- The likelihood of any risk materialising.

If entities are already secure and of low risk, capturing them under the revised legislation will not generate any benefits for the community. Instead, it will soak up limited regulator resources and restrict the ability of entities to respond flexibly to changing risks.

The specific criteria used to determine how entities are placed in each criteria should be transparent, and – given the substantial regulatory costs at stake and changing risk environment – the allocation of entities should be subject to regular review and entities provided the opportunity to appeal.

Foreign investment

Appropriately identifying the entities captured under the revised legislation will have important flow on implications. As noted in our submission to the Treasury on the exposure draft of the Foreign Investment Reform (Protecting Australia's National Security) Bill 2020, the foreign investment thresholds use the SOCI Act in defining a 'national security business'.

As part of our submission to the Treasury, the BCA recommended the existing entities captured as a 'national security business' should be retained, with any new critical infrastructure reviewed before it is added. We continue to recommend this approach.

'Critical' business elements and assets

Any framework should recognise that businesses are not monolithic. There are a variety of functions within a business that may not be 'critical', where requirements for an improved security posture would create additional regulatory cost disproportionate to the policy problem.

Any new requirements should identify and only be applied to elements and assets of the entity that are truly 'critical', and not to the entire entity.

Cross-sectoral impacts

Different businesses and assets within a single business may also be captured across multiple sectors. A single business (or business asset) may simultaneously provide food and grocery, communications, health, and other services, for example. This might result in them being subject to overlapping requirements (and potentially penalties).

This scenario would result in a poor use of both regulator and business resources. We recommend that any businesses which sit across multiple sectors be subject to only one regime.

The reformed Act should use existing regimes wherever possible

The consultation paper is seeking views on possible requirements and obligations that may be imposed on critical infrastructure entities. As the paper notes, these will need to vary from sector to sector, and will need to recognise, use, and complement existing frameworks. The consultation paper notes the new approach will build on and not duplicate existing regulatory frameworks.

We strongly support this approach, and recommend the Government should, wherever possible, use existing regulatory frameworks (such as the Telecommunications Sector Security Reforms (TSSR)), and avoid replacing these with new regimes. Any new requirements should also be based, wherever possible, on existing international or domestic standards (such as ASD's Essential Eight or the ISO 27000).

The existing regulatory frameworks and standards have been subject to substantial work between Government and business, to ensure they are workable and deliver the right outcomes for Australia and Australians. Replacing them would be a step backwards. For sectors already subject to substantial security requirements, consideration should be given to whether any additional requirements are necessary or if risks are already being adequately managed.

Similarly, regulation should not be used to replace existing voluntary processes. For example, threat visibility and sharing should be based on trust relationships, supported by an uplift to ensure effective sharing platforms and processes. Regulation should not degrade the quality of the information shared to bare minimum technical indicators, rather than rich contextualised information. A move towards mandatory information sharing may also impact

information sharing in the short term given the consultation process has flagged that information shared will be mandated at a later date.

Positive Security Obligation

The consultation paper seeks views on the principles underpinning the Positive Security Obligation. The proposed principles would place a responsibility on businesses to identify and understand risks, mitigate these risks to prevent incidents, minimise the impact of realised incidents and maintain effective governance and accountability.

The specific obligations (and therefore the regulatory costs) are still to be determined. However, it is unlikely these will be cost-free, including in sectors which are already heavily regulated. Any new obligations should consider who will ultimately pay, in either higher costs or foregone services. Given the as yet unknown but potentially substantial costs of compliance with the new regulatory regimes, Government should consider whether support to entities uplifting their security is appropriate.

In line with best practice regulatory principles, the benefits of these obligations should outweigh the costs to the community. We recommend the Government consider an additional principle asking entities to put in place controls proportionate to the risk and which recognise the need to maintain affordable services for the Australian community and industry.

Supply chain management

The paper notes that supply chains will be part of the security obligations for critical infrastructure operators. Depending on the nature of the requirements, this may require businesses down the supply chain to demonstrate appropriate risk management compliance.

There may be some suppliers who work with multiple critical infrastructure operators across different sectors. In this instance, they may be required to demonstrate compliance with security requirements for each sector. This would be duplicative and inefficient. It would also have a disproportionately negative impact on SMEs.

We support lifting security through the supply chain. However, the changes should be outcomes based and avoid inefficiency or duplication. Consideration should be given to ways to ensure any regulatory burden associated with supply chain security is not duplicative when businesses are working in more than one sector. It may be appropriate for the Government to implement clear guidelines as to how supply chain security should be implemented. This could include providing templates and pro forma standards or questions which will ensure consistency in how entities set expectations in their supply chain. This will benefit smaller entities down the supply chain who can adopt practices and responses which will meet the standardised requirements of their customers.

Government directions and direct action

The consultation paper notes the Government is proposing to establish powers to provide reasonable, proportionate, and time-sensitive directions to critical infrastructure operators where there is an imminent cyber threat or incident. The consultation paper also notes the Government is proposing to establish powers that would allow Government, in exceptional circumstances, to take direct action to protect a critical infrastructure entity or system from a cyber-related threat.

We support these powers only being used in an emergency, where there is a clear cyber threat to Australia's ongoing security or prosperity that requires government intervention. It should be undertaken only after the entity has had the opportunity to remediate any threats, after good faith negotiations have taken place, and after considering the costs and consequences. Any decisions should be subject to a merits and judicial review.

The operations of networks and systems are complex. Third party interventions, even where taken in the best interests of the network or Australians, may have unintended negative consequences (such as damage to a network or business or to the interests of Australians and Australian businesses).

We recommend the consideration be given to the remediation if Government action or direction result in a substantial negative consequence. Entities and the community will need comfort that the downsides of any (lawful) intervention are appropriately managed.

Regulator roles should be clearly defined and regulators appropriately resourced

The consultation paper indicates existing regulators, where possible, will be responsible for administration of new regulations. The conduct and behaviour of Australia's regulators can substantially affect economic growth. By making timely decisions, engaging constructively, and meeting performance measures, Australia's regulators can have a positive impact on economic growth.

The details of the new regulations are still to be settled, including arrangements where there is not an appropriate existing regulator. Regulators should be selected based on their expertise and relationships with relevant sectors. The appropriate selection of regulators, arrangements where no existing regulator exists, along with any new penalty arrangements, could be considered by the proposed working group.

Further, it is likely the oversight of security regulation may constitute a new function and area of expertise for some regulators. The consultation paper also canvasses personnel security assessment by ASIO and police checks.

To ensure regulators and assessment agencies can perform their duties appropriately, the Government should ensure they are resourced appropriately and proportionately for any new functions. Any new functions should not detract from the ability of regulators to perform their existing functions in a timely and effective manner.

Any new requirements should also be subject to appropriate oversight and checks and balances. This will be particularly important in where government issues a direction or directly intervenes in the networks of a critical infrastructure operator.

The Regulator Performance Framework measures the performance of regulators. It gives businesses, community, and individuals confidence that regulators are effectively and flexibly managing risks. To provide accountability and transparency, this Framework should be applied to the administration of any new regulations that are put in place. Any new legislation should also include annual reporting for new powers, including of instances where any directions powers were used.

If the public reporting of these instances would raise national security concerns, then we recommend reporting be provided to either the Parliamentary Joint Committee on Intelligence and Security or to the Inspector-General of 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