

6 May 2026

Sophie Bazzana
Assistant Secretary
Critical Infrastructure Security Policy Branch
Department of Home Affairs

Via email

Dear Ms Bazzana,

The Business Council of Australia (BCA) welcomes the opportunity to comment on the proposed amendments to the Ministerial Directions Powers under the *Security of Critical Infrastructure Act 2018* (SOCI Act).

Feedback on Ministerial Directions Powers

The BCA recognises the intent of the changes to the Ministerial Directions Powers, which would enable more focused Government intervention in the governance, technology and supply chains of critical infrastructure entities. The proposed changes also seek to enable faster Government action in the face of a more dynamic threat environment, including responding to the risks posed by AI-enabled cyber threats.

However, the BCA has concerns that the proposed changes significantly expand existing Government powers requiring regulated entities to take certain actions on an ongoing basis, or in relation to their major SOCI suppliers. The BCA is concerned the regulatory burden from changes is potentially disproportionate to the risks they are seeking to address.

Consistent with the current powers under Part 3 of the SOCI Act, the proposed measures should continue to operate as exceptional, last-resort tools. Their use should be tightly constrained, applied only in extreme circumstances of material risk, and be subject to robust safeguards and oversight.

Measure 2: Conditions power

It is proposed to enable the Minister to impose targeted, conditions on reporting entities where ownership, control, or governance arrangements create a “material risk to national security that cannot be sufficiently mitigated through existing regulatory obligations or voluntary measures”.

Feedback: This power could help address governance vulnerabilities in a more targeted and predictable manner. However, it is broad in scope and there is a potential conflict between the conditions and other regulations, such as director’s duties under the Corporations Act. The

consultation paper includes examples of conditions that have potential conflicts with the Corporations Act:

- Targeted board voting exclusions or restrictions for decisions that materially affect the security posture of an asset (e.g. procurement, network architecture, operational arrangements, or high-impact financial decisions linked to resilience of the asset). These potentially undermine the role of a board.
- Requirements relating to board composition, such as minimum number of independent, Australian security-cleared directors. This may undermine the ability for Australian companies to appropriately leverage global talent pools for their boards.

In addition, the example of a requirement to implement specified cyber security baseline controls lacks clarity. These controls could be extensive in scope, and the definition in what is considered ‘baseline’ by the cyber security industry is constantly shifting. Requiring businesses to implement externally defined baseline controls risks overriding entities existing, sophisticated risk-management frameworks, and could require the adoption of redundant or incompatible security architectures at significant and unnecessary expense.

Measure 3: New “vendor-risk direction power”

It is proposed to introduce a new power to enable the Minister to issue targeted risk-based directions to responsible entities, either individually or by class, where a vendor or technology dependency creates a “material national security risk” where necessary to mitigate or eliminate the risk.

Feedback: The BCA submits that a thorough Impact Analysis of this proposal is required. If a direction forces removal or restriction of a vendor, technology or product, this could lead to serious operational impacts. BCA members often operate in highly integrated environments and removal or restriction of one component can have wide reaching impacts and costs. This could be made even more challenging at times of significant supply chain disruptions – such as those being currently experienced.

Transition timeframes will need to be carefully considered because replacing embedded supply-chain technology requires significant capital expenditures and multi-year lead times. Any directions involving third parties, including any vendor restriction must be accompanied by realistic, phased transition timeframes that align with individual entities contractual timelines. Legal clarity is also required for entities where compliance with a direction requires early termination or modification of a contract or agreement with a vendor or customer.

BCA members also note that vendor restrictions may impact on service delivery. This may create issues where regulators require (or expect) certain service delivery, reliability and performance standards to be met.

The consultation paper states affected entities would be consulted wherever reasonably practicable. The BCA recommends that this requirement should be explicitly legislated to put appropriate guardrails on the use of this measure. We note the AML/CTF reforms currently before Parliament require AUSTRAC to conduct a minimum 30-day public consultation before prohibiting the use of a product or service, with limited exceptions.¹

¹ Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026, proposed new section 77B.

Measure 4: Public Disclosures

The proposed changes would create a temporary, time-bound power to delay public disclosures (where a publicly listed company must disclose major events, such as a severe cyber attack) in rare, high-risk cyber incidents.

Response: BCA recognises there may be rare instances where a public disclosure delay could help manage cyber incidents involving extraordinary national security or public safety risks.

However, delaying an official ASX disclosure may create issues if the relevant information at some point becomes no longer confidential – for example due to unauthorised disclosure or public speculation. In this case, there could be market speculation, share price volatility and in the context of retail investors, anticipatory or speculative buying. The business would also be in a difficult situation, being effectively unable to comment on public speculation.

A clear mechanism for managing public messaging to mitigate customer and public trust issues during an incident is incredibly important. The solution is not simply delaying an ASX disclosure. If either model in the consultation paper is adopted, strict safeguards and oversight will need to apply.

If this measure is implemented, we recommend the addition of a clear safe harbour in the Corporations Act to protect businesses and directors acting in good faith to comply with a direction under this measure. There are concerns the exemption under the ASX Listing Rules would not be sufficient on its own to provide adequate safeguards, particularly in relation to the director duties under the Corporations Act. Protection against regulator and third-party actions is also warranted.

Measure 5: Increased civil penalties

Response: The legislation should ensure there is protection for entities that engage in good faith. For example, compliance with the scheme may impact the provision of essential goods and services in order to comply with a Ministerial Direction.

General feedback

We seek further clarity on how these changes will apply across interconnected environments. Given the highly interdependent networks across physical and digital environments, we request further guidance on how this change may apply if a direction requires action from suppliers or if there is a dependency on a supplier.

We also request further information about who is liable for the cost impact resulting from entities taking directed action. We recommend the Government provide clear legal protections for entities acting in good faith under a direction.

General comments

The BCA makes the following general comments:

- The proposed amendments should have clear, objective and transparent criteria for identifying “high risk vendors”;

- It is important for the proposed amendments to have operationally realistic transition periods where vendors or technologies are restricted or phased out to minimise unintended security gaps;
- The proposed amendments should recognise that vendor concentration, limited substitutability and global supply chain constraints may restrict diversification options in certain categories;
- Businesses should be able to rely on legislative levers during contract negotiations (i.e. the SOCI Act requires covered businesses to have in place suspension/termination/change regimes which must occur if directed by the Minister under the new rules);
- The proposed amendments should take into consideration the costs that may be incurred by business if directions were made by the Minister;
- The proposed amendments should ensure clear legal safe harbours apply across overlapping regimes (for example, ASIC, ASX, Privacy Act and directors' duties) or otherwise reduce such duplication through a "report once" framework; and
- There is a need for clear guidance on post-delay ASX disclosure expectations and coordination with regulators.

If you wish to discuss this submission further, please contact [REDACTED] at the BCA on [REDACTED]

[REDACTED]

Yours sincerely

[REDACTED]

[REDACTED]

[REDACTED]

Business Council of Australia