Insurance Council of Australia

28 April 2026

Department of Home Affairs

Via upload

Dear Sir/Madam

Proposed amendments to the Ministerial Directions Powers in Part 3 of the *Security of Critical Infrastructure Act 2018*

The Insurance Council of Australia (Insurance Council) welcomes the opportunity to provide a submission on behalf of our members in response to the *Consultation Paper: Proposed amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure Act 2018* (the Consultation Paper).

The Insurance Council is the representative body of Australia's general insurance industry. Our members account for approximately 90 per cent of total premium written by general insurers and reinsurers. As a foundational component of the Australian economy, the general insurance industry writes 90 million policies a year, paying out $58.9 billion in claims in 2025 – an average of $226 million every working day.

The general insurance industry supports the intent of strengthening government's ability to respond rapidly to credible and serious national security risks affecting critical infrastructure, including cyber risk and supply chain vulnerabilities.

We consider that any uplift to Part 3 Directions Powers should remain an escalation mechanism with strong safeguards, including proportionality, transparent decision criteria, whole-of-government coordination, and practical implementation pathways that avoid unintended disruption to essential services and markets.

We suggest that the Department consider that regulated entities will need time to ensure they can meet their updated obligations under the proposed changes.

We offer the following comments on the Consultation Paper.

Measure 1 – Amendment to the existing directions powers in section 31

We support the intent of replacing the existing Adverse Security Assessment with a tailored threat advice from the Australian Security Intelligence Organisation (ASIO). We also support expanded consultation among relevant Commonwealth entities alongside the retention of existing State and Territory consultation requirements.

We recommend that this amendment be accompanied by guidance on minimum content expectations for ASIO advice and on how "material risk" and proportionality are assessed, to provide predictability and reduce dispute risk.

With respect to the scenario provided, balancing of the considerations listed is reflective of the current experience for many regulated entities operating within complex global supply chains and regulatory landscapes. Despite best endeavours in innovation, it remains common that regulated entities are reliant on manual and point-in-time processes and governance when managing engagements with

external parties and technology changes. We expect these conditions would prevail even in the circumstance of adhering to a Ministerial Direction as regulated entities will still need to comply with legal and regulatory obligations applicable to procurement, implementation and ongoing management of an onshore technology solution deployed in response to a direction. Regulated entities would also need to bear the corresponding costs, for example prioritisation or raising of necessary capital funding, supplier contracting, third party risk assessments, architectural design, testing and change management, reporting and oversight by Executive and Board levels.

These considerations reinforce the importance of active and consultative engagement between the Government and the regulated entity in addressing a national security threat, and the use of Ministerial Directions as a measure of last resort. In contrast to the scenario, the least operationally disruptive and cost-efficient approach is one in which adequacy of risk mitigation is agreed, executed and assured without protracted or repeat work, or a material variation in late stages after considerable investment by the regulated entity to that point.

This can be supported with clear guidance material outlining how engagement between Government and regulated entities will operate before and during the making of any Ministerial Direction. Guidance material should also address how engagement with and issuing of Ministerial Directions operates in the context of other obligations (e.g. regulatory requirements, directors duties etc.). Supporting materials should also outline the process that would be followed in terms of making Ministerial Directions, including how regulated entities would be engaged throughout the process such that they are clear on the steps and timelines and where they would have the opportunity to highlight:

- any specific factors they wish to be taken into account when issuing of Ministerial Directions are contemplated
- support they could avail themselves of from the Government (particularly for entities that have lower levels of security maturity)
- mechanisms to raise and escalate concerns or challenges about a proposed or issued Ministerial direction and seek reconsideration or appeal.

We also suggest additional consideration be given to organisations with head offices, core platforms, or critical systems located offshore. For multinational entities, mandated requirements to relocate systems or data onshore may be impractical due to architectural complexity, interdependencies, and contractual or regulatory constraints across jurisdictions. For these businesses, we encourage flexibility in how compliance is assessed, including the ability to adopt alternative risk mitigation measures where physical relocation is not feasible, consistent with the Consultation Paper's stated objective of maintaining proportionality and operational practicality.

Measure 2 – Conditions Power

We acknowledge that targeted conditions on reporting entities can mitigate national security risks where existing regulatory obligations and voluntary measures fall short.

However, we note that the insurance industry already operates within comprehensive regulatory regimes, including those administered by APRA and under the *Corporations Act 2001*, which impose robust obligations relating to operational resilience, outsourcing, incident management, and governance. We therefore support the view that the application of any new conditions power should take existing regulatory coverage into account, and that additional powers should be targeted primarily at critical infrastructure sectors or entities not subject to comparably mature regulatory oversight, to minimise overlap and regulatory burden.

Insurance Council of Australia

Consistent with our feedback in respect of *Measure 1 – Amendment to the existing directions powers in section 31*, the scenario contemplated further highlights the importance of active and consultative engagement between the Government and the regulated entity in addressing a national security threat. Notwithstanding that the enhanced conditions powers would be used as a measure of last resort where commensurate outcomes cannot be achieved through other means, we recommend the Government provide supporting guidance to regulated entities outlining how engagement between the entity and the Government will work ahead of and during the application of conditions. This guidance should include how entities can highlight factors for ministerial consideration, seek government support, and escalate concerns or challenges with the conditions imposed. Noting the conditions power is a 'step-up' to the Critical Infrastructure Risk Management Program (CIRMP), this guidance will be of particular importance to regulated entities excluded from the CIRMP obligations.

Further, we note that should this amendment be made, regulated entities will need to review their incident management arrangements to ensure they encompass an established and coordinated approach to complying with conditions that are imposed, alongside existing incident management and reporting obligations that exist across various regulations.

We recommend the threshold and evidentiary standard for applying conditions be clearly defined, and that conditions be time-bound and reviewable, with explicit coordination across relevant regulators to avoid duplication or conflicting obligations. Predictable engagement pathways will also support regulated entities to meet their obligations.

We also recommend that transitional timeframes are set, to enable sufficient time for regulated entities to make adjustments to incident management processes and other governance as noted above.

Measure 3 – Restrictions on the use of high-risk vendors, products or services

The Insurance Council and our members support a coordinated approach to systemic vendor and supply chain risks. Given the potential operational and contractual impacts, we recommend clear process safeguards (including opportunity for mitigation proposals), realistic transition pathways, and consistent cross-sector implementation to avoid fragmented or inconsistent outcomes. We also support the factors required for the Minister to consider in issuing a direction outlined at the top of page 15 of the Consultation Paper.

We expect that regulated entities will, in some cases, need to consider and prepare vendor exit strategies and technology substitution planning.

We support the Government producing model contract clauses, which will assist businesses to document compliance. Such clauses should ideally allow for heightened monitoring, testing and exit clauses predicated on the contracted supplier outsourcing work that could lead to national security risk.

Transitional timeframes for these updated powers will also enable regulated entities to consider, negotiate, and implement these changes into relevant supplier contracts where required.

Further, we expect introduction of requirements focused on transparency of supply chain risk management practices and third and fourth-party incident exposure would be of benefit. Such requirements should extend beyond the time of onboarding and instead operate as a routine process would be beneficial to provide regulated entities with bargaining power in negotiating enhanced obligations into contracts, particularly with large multi-national technology suppliers.

Additionally, consideration could be given to incentivisation – for example via tax credits – for investment in domestic partners to help smaller domestic players build sovereign capability and expand market competition.

Insurance Council of Australia

Finally, it may be useful to explore if, in defined circumstances, Directions Powers could extend to certain common or shared service providers during significant cyber security or national security incidents. This could strengthen coordinated incident response across interconnected entities, provided appropriate safeguards and thresholds are maintained.

Measure 4 – Delay continuous disclosure requirements

Insurance Council members support the objective of preventing public disclosure of a cyber incident where such disclosure would threaten national security or public safety. Insurance Council members prefer leveraging the existing exemption mechanism with agreed guidance under Option 1. Option 1 will preserve market integrity checks and reduce the risk of conflicting statutory obligations.

Measure 5 – Increase civil penalty provisions

Insurance Council members support the intent of strengthening compliance incentives, including the proposal to increase maximum civil penalties for non-compliance with a Ministerial direction. which we expect will further amplify civil penalties as a deterrent for a failure to comply with a Ministerial direction.

Notwithstanding our support, we take the view that the use of civil penalties be adopted as a measure of 'last resort' as other measures such as enforceable undertakings and injunctions are likely to have a more immediate and direct impact on resolving risks to national security.

Further, it is foreseeable that some regulated entities issued with a Ministerial Direction may face real challenges to being able to meet the direction. For example, entities with resourcing constraints, facing insolvency, administration or wind-up, or those faced with multiple concurrent and competing or conflicting compliance obligations. In these cases, application of civil penalties may magnify such challenges achieving no discernible security outcome. This potential perverse outcome reinforces the importance of ensuring thorough engagement and consultation between the Government and the regulated entity in focus to ensure relevant matters have been adequately considered in the formation and issue of any Ministerial Direction.

To this end, any penalty uplift should be accompanied by clear guidance and reasonable implementation expectations, a transition or grace period before increased penalties apply or are imposed, and limiting application of penalties to situations where the regulated entity has not taken reasonable steps to comply with the direction, particularly where compliance depends on complex vendor or technology transition activity.

Finally, given the focus on critical infrastructure and the scale of impact that could result from endangerment of national security interests, we support that penalties for a failure to adhere to a Ministerial Direction be at least consistent with those applicable for failures to meet more general security and privacy obligations, such as those prescribed under the *Privacy Act 1988*, or *Corporations Act 2001*.

[redacted]