Tech Council of Australia

Ministerial Directions Powers in Part 3 of the SOCI Act

Tech Council of Australia Submission

May 2026

techcouncil.com.au

Introduction

The Tech Council of Australia (TCA) is the peak industry body representing Australia's technology sector. Our members include leading global and domestic technology companies who deliver services that underpin every sector of the economy, and operate or supply infrastructure that has been deemed critical under the *Security of Critical Infrastructure Act 2018* (SOCI Act).

TCA convenes the National Security Tech Alliance (NSTA), a forum that brings together leading domestic and multinational technology companies on national security and defence technology issues. This submission was informed through consultation with NSTA members, including hyperscale cloud providers, network equipment manufacturers, and other technology vendors with operational experience of the SOCI framework. The views expressed reflect the collective input received during that process.

TCA welcomes the opportunity to respond to the Department of Home Affairs' (the Department) consultation on its proposed amendments to the Ministerial Directions Powers in Part 3 of the SOCI Act. We share the Department's view that the threat environment facing Australia's critical infrastructure is becoming more dynamic, that supply chain and governance vulnerabilities present continued risks to national security, and that there is a legitimate case for ensuring the directions framework is fit for purpose.

The Ministerial Directions Powers in Part 3 of the SOCI Act are extraordinary tools. They can be used by the Minister to compel an entity to do, or refrain from doing, actions that can have material commercial, operational and contractual consequences for entities, and their use is not subject to publication.

TCA's overarching view is that these powers must only be used as a last resort, and that the strength of the powers conferred must be matched by the strength of the safeguards surrounding them. Proposed reforms that would make the powers easier to use should be accompanied by clear, legislated procedural protections, and new powers must only be legislated where strictly necessary.

Throughout this submission, TCA has sought to engage constructively with the Department's objectives. We would welcome continued consultation from the Department if legislative design progresses.

Measure 1 – Amending the existing directions power

TCA **does not support** the proposed amendments to the section 32 power. The Adverse Security Assessment (ASA) requirement and regulatory exhaustion test are central safeguards that balance the extraordinary nature of the power. The proposed reforms would remove the ASA precondition (including the embedded notice and review rights) and convert the regulatory exhaustion test from a precondition into a consideration. These amendments would materially weaken the procedural protections that apply to one of the most significant powers in the SOCI Act, while simultaneously expanding the reach of the directions framework under the proposals in Measures 2 and 3.

TCA acknowledges the Department's intention to introduce greater flexibility and efficiency in the Minister's use of the section 32 power in order to effectively manage threats to Australia's national security. However, we view the ASA precondition and regulatory exhaustion test as necessary safeguards. The ASA requirement ensures an independent assessment of risk and aligns the framework with established intelligence processes, while the regulatory exhaustion test reinforces that the directions power will only be used as a measure of last resort.

TCA does not object to the Department's specific proposals to retain the consultation requirements in section 33 of the SOCI Act and expand consultation requirements to ensure that relevant Commonwealth Ministers and agencies are consulted.

Should the Department wish to proceed with the reforms proposed in this measure, TCA makes the following recommendations.

Recommendation 1 – Implement a merits review

Due to the extraordinary nature of the section 32 power, the legislation should provide for an express merits review of decisions made under Part 3 of the SOCI Act, and the Department should clarify the forum through which that review will be available (for example, the Administrative Review Tribunal).

The residual safeguards relied upon in the consultation paper – good-faith negotiation, consultation, and judicial review – afford insufficient protections to industry. Judicial review in particular is narrowly concerned with the legality of the decision-making process – it does not test the factual or technical accuracy of the underlying threat assessment or the reasonableness of the proposed direction, which are likely to be the issues most in dispute between the Minister and affected entities.

Recommendation 2 – Engage cleared industry personnel on threat advice

The directions framework would benefit from a structured mechanism for engaging appropriately cleared industry personnel on classified threat advice. Establishing such a framework under the SOCI Act – under which cleared, accountable contacts within entities can be consulted early – would ensure that Australian Security Intelligence Organisation (ASIO) advice and the Minister's ultimate decision are grounded in a complete understanding of an entity's technical and operational context.

Recommendation 3 – Recalibrate the regulatory exhaustion requirement

The legislation should require that the Minister give substantive weight to the existence of, and the entity's compliance with, other Commonwealth, State or Territory regulatory frameworks, and to articulate in a statement of reasons supporting any direction why those frameworks are insufficient to address the identified risk.

Measure 2 – Conditions power

TCA **does not support** the introduction of a new conditions power as currently proposed in the consultation paper. The proposed power is open-ended and overlaps materially with risks already addressed through existing frameworks.

The categories of conditions described in the consultation paper – including access controls, personnel security, board governance, cyber security baselines, transparency and audit – correspond closely to obligations imposed on entities under the Critical Infrastructure Risk Management Program (CIRMP) framework and Hosting Certification Framework (HCF).

The consultation paper acknowledges overlap in respect of the *Foreign Acquisitions and Takeovers Act 1975* (FATA), and indicates an intention to develop coordination arrangements between regimes. However, TCA does not consider that this is a sufficient response to the risk of regulatory duplication.

The legislation should make clear that where an entity is materially compliant with CIRMP and holds existing HCF certifications (where applicable), the entity should be exempt from any obligations under the proposed new conditions power. Compliance with these frameworks reflects a substantial, ongoing investment in security uplift, and entities that have made that investment should be able to rely on it as the primary means of demonstrating they are managing governance and control risks responsibly.

Should the Department wish to proceed with legislating the new conditions power proposed in this measure, TCA makes the following recommendations.

Recommendation 1 – Impose clear safeguards

TCA considers that the following safeguards are necessary to ensure a conditions power is proportionate and is used by the Minister as a last resort:

- The Minister must be satisfied that there are no other less intrusive measures (including the CIRMP and HCF) that are available that could be used to effectively reduce or remove the risk (this should be drafted as a pre-condition, not a consideration).
- A condition must be reasonably expected to result in a material and measurable uplift in the security of the relevant asset(s).
- A condition must not create or exacerbate any vulnerability or undermine availability or security of the relevant asset(s).
- A condition must be appropriately tailored to the specific asset(s) and responsible entity for the asset(s).
- A condition must allow the entity to implement compensating controls in lieu of the specific condition.
- The Minister must have expressly considered the technical and operational feasibility of the condition, and whether compliance would degrade the availability, reliability or security of the asset or services provided to customers.

Recommendation 2 – Provide clear timeframes and protections

The legislation should provide transition timeframes that are realistic in respect of the affected entity and commensurate to the impact of the condition. The legislation should also provide that directors who act in compliance with a condition direction are not in breach of

their legal duties (including under the *Corporations Act 2001*) and that companies are immune from any loss or damage resulting from the direction.

Recommendation 3 – Implement appropriate review and accountability measures

Similar to Recommendation 1 under Measure 1 above, affected entities should have an express right to seek a merits review in response to the conditions power. Likewise, legislation should provide the opportunity for conditions to be revoked or varied immediately where entities have implemented appropriate compensating controls.

The proposed review cycle (12 months and every 24 months thereafter) should be reduced to 6 months, with subsequent reviews at intervals of no more than 12 months. The right of an entity to trigger a review on notice of material change should be retained.

Conditions should be imposed for the shortest possible timeframe necessary to achieve the identified security uplift, with an express expectation in the legislation that conditions must be revoked once that uplift is achieved.

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

TCA **supports this measure in principle**. We accept that systemic supply chain and vendor-related risks cannot always be effectively managed at the level of an individual entity, and that there may be a legitimate case for a coordinated, sector-level mechanism. However, the breadth and potential cumulative effect of any vendor-level restriction mean that appropriate legislative design is critical. TCA support is conditional on the following safeguards.

Recommendation 1 – Mandatory consultation

Given that a single direction under this power can affect the shared architecture relied upon by many entities simultaneously, we consider that legislated, mandatory consultation requirements are essential. Specifically, we recommend that consultation be mandatory in respect of any proposed direction and have a default minimum period of 28 days.

Comparable international regimes – including in United Kingdom and European Union frameworks – rely heavily on structured engagement with industry to ensure that vendor-related decisions are proportionate, technically informed, and implementable without unintended resilience impacts. Aligning Australia's framework with international norms would also reduce compliance friction for Australian operators and vendors that are part of global technology ecosystems.

Where the Department considers that a narrow carve-out from the consultation requirement in genuinely time-critical national security circumstances is unavoidable, that exception should:

- be expressly limited to circumstances in which the Minister is satisfied that proceeding with the standard consultation period would result in serious and irreversible harm to national security

- attract heightened transparency requirements after the fact, including post-direction consultation and reporting, and
- not be available where the underlying risk could be addressed by compensating controls during the standard consultation period.

Recommendation 2 – Compensating controls should be the default

The power proposes a variety of directions, ranging from compensating controls through to prohibitions on the use of specified products or services. TCA recommends that the legislation explicitly treat compensating controls as the default mitigation pathway, with restriction and prohibition used as a measure of genuine last resort.

This is particularly important, for example, in multi-tenant cloud environments or in network infrastructure, where implementing supply chain changes cannot be easily achieved or would otherwise require lead times measured in many months, and where the removal of a product or service can compromise the availability and security of an asset (rather than improve it).

TCA accepts that there may still be circumstances where superior directions (i.e. beyond compensating controls) remain necessary to address national security risks.

Recommendation 3 – Clarifying scope and supporting transition

The legislation should clearly define the categories of 'vendor', 'product' and 'service' that fall within the scope of the power. Without this, entities risk being asked to undertake disproportionate due diligence across long trails of suppliers.

The legislation should also be structured to permit entities – given their intimate knowledge of their operations – to provide government with a reasonable timeframe for transition, having regard to factors such as the complexity of the environment, the hardware or firmware in question, and implementation of interim compensating controls.

Recommendation 4 – Review and contractual protections

As per previous recommendations, the legislation should provide for an express merits review of decisions made.

Where a direction requires an entity to cease using or to modify a vendor relationship, entities may face exposure under existing commercial contracts. The legislation should therefore provide that compliance with a direction is a complete defence to claims for breach of contract and customer claims from service degradation or availability.

Measure 4 – Delay continuous disclosure requirements

TCA **supports this measure in principle**. But to ensure this measure is operationally feasible, government must clarify how a direction to delay or restrict disclosure would work in practice.

For example, because cloud transparency tools are automated and broadcast-style, pausing or restricting updates for specific customers is often technically unfeasible without disabling

transparency for the entire market. Bypassing these automated systems in favour of manual notifications could introduce dangerous delays. Any implementation of Measure 4 must be aligned and integrated with current incident reporting obligations.

As an alternative solution, TCA suggests that compliance with a notification direction should be met when a provider uses its existing transparency platforms, ensuring rapid information flow while allowing government to manage broader public messaging.

Measure 5 – Increased civil penalty provisions

While TCA recognises that an effective deterrence regime is part of a credible compliance framework, we **do not consider it warranted** to increase the maximum civil penalty for non-compliance with a Ministerial direction under Part 3 to 2,000 penalty units.

Should the Department implement Measure 5, TCA proposes that any increase be contingent on the strength of the safeguards attached to the powers themselves. A larger maximum penalty applied to powers with weaker procedural protections would not, on balance, support a fair and predictable compliance framework. The proposed increase should therefore be considered alongside the amendments and safeguards recommended in this submission.

Closing remarks

TCA appreciates the Department's engagement with industry on these reforms and the opportunity to provide input at this stage of the policy development process. The proposals raise important issues for the operation of Australia's critical infrastructure and for the technology sector that supports it.

We are committed to working constructively with the Department to ensure that the final legislative design supports government's national security objectives, while maintaining the safeguards, technical realism and commercial workability on which a durable and effective regime depends.

We would welcome the opportunity to discuss this submission further, and to participate in any post-consultation activities.