Aussie Broadband Limited
PO Box 3351
Gippsland Mail Centre
Victoria 3841
P 1300 880 905
E info@aussiebroadband.com.au

aussiebroadband.com.au

6 May 2026

[redacted]

Critical Infrastructure Strategic Policy
Department of Home Affairs
ci.reforms@homeaffairs.gov.au

Via email

[redacted]

Subject: Consultation on proposed amendments to Ministerial Directions powers in Part 3 of the Security of Critical Infrastructure Act 2018

Aussie Broadband Limited (Aussie Broadband) welcomes the opportunity to provide a submission on the proposed reforms to Ministerial Directions powers under the Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act).

Aussie Broadband is an Australian telecommunications provider operating fixed, mobile, voice, enterprise and wholesale services, and relies on complex domestic and international supply chains, technology vendors and managed-service arrangements to deliver critical communications services.

In summary, Aussie Broadband recommends that the reforms be supported by clear proportionality requirements, transparent risk assessment criteria, minimum notice and transition expectations where service continuity may be affected, and structured engagement with affected entities before and after directions are issued.

Further, Aussie Broadband supports the Government's objective of enabling earlier, more decisive intervention to manage serious national security risks across critical infrastructure sectors. We recognise the need for tools that are responsive to evolving threat environments, particularly where risks arise from complex supply chains, foreign ownership, control and influence (FOCI), and increasing interdependence across sectors.

We commend the Government on its efforts to improve clarity, flexibility and alignment with comparable frameworks, including the Foreign Acquisitions and Takeovers Act 1975 (Cth). In our view, the proposed reforms represent a material strengthening of the Commonwealth's ability to respond to emerging risks. However, given the foundational role telecommunications providers play across all SOCI sectors, it is critical that these powers are exercised with clear guardrails, transparency and practical implementation pathways.

Key observations and considerations

1. Expanded and more usable directions power (Measure 1)

Aussie Broadband acknowledges the benefit of replacing the current Adverse Security Assessment requirement with more tailored ASIO advice, which will allow for more timely and flexible responses in high-risk scenarios. However, this change materially lowers the procedural threshold for intervention. For telecommunications providers, this increases the likelihood of directions affecting network architecture, offshore operations, vendor arrangements and access controls, potentially at short notice.

We note in particular:

- The reframing of the "last resort" test will make it easier for ministerial directions to be preferred over existing regulatory mechanisms.
- The types of scenarios contemplated closely mirror current telco operating models, including offshore managed services, global vendors and distributed network management.

Given this, it is important that:

- proportionality is explicitly codified, including consideration of staged implementation where immediate cessation would disrupt essential services
- minimum notice and transition expectations are clearly articulated where customer or service continuity impacts arise
- structured engagement occurs with affected entities to test feasibility prior to issuing directions wherever possible.

2. Introduction of a conditions power (Measure 2)

The proposed conditions power represents a significant expansion into governance, ownership and operational structures. Aussie Broadband recognises the policy rationale, particularly in addressing risks associated with FOCI and insider access to sensitive systems and information. However, the scope of potential conditions, including board composition, access to information, and operational segregation, has far-reaching implications.

From a telecommunications perspective, this raises:

- the potential for mandated changes to board and committee structures, including restrictions on access to security-sensitive information.
- requirements to segregate systems and operations from global or group environments, including offshore support arrangements; and
- increased compliance, audit and assurance obligations.

To support effective implementation, we recommend:

- clear criteria and transparency around how governance and vendor-related risks are assessed
- alignment guidance addressing interaction with Corporations Act duties and listing obligations
- mechanisms for ongoing dialogue, including technical working groups and scenario planning, to support both pre- and post-implementation phases.

3. Restrictions on high-risk vendors, products and services (Measure 3)

Aussie Broadband considers this measure to be particularly significant for the telecommunications sector.

The proposed power to restrict or prohibit the use of certain vendors, products or services introduces a more formal and durable mechanism for managing supply chain risk. While this provides clarity relative to informal processes, it also introduces substantial operational and commercial implications.

For telecommunications providers, this may result in:

- directed changes to vendor selection, including prohibition or phase-out of specific suppliers
- requirements to localise or diversify critical network functions
- additional controls on remote access, updates and system administration.

We support the intent of this measure, but emphasise the importance of:

- transparent and consistent criteria for identifying high-risk vendors and services
- proportional, staged implementation approaches where large-scale remediation is required
- recognition of contractual, technical and supply chain constraints that may impact transition timelines.

4. Disclosure settings (Measure 4)

Aussie Broadband, as an ASX-listed entity subject to continuous disclosure obligations, is generally supportive of the proposal to provide temporary relief from continuous disclosure requirements where disclosure would create or exacerbate national security risks.

Our preference is for Option 2, under which a new directions power would be inserted into the SOCI Act allowing the Minister for Home Affairs to direct an affected entity not to publicly disclose the existence of a cyber incident for a prescribed period. This approach would appropriately engage the ASX Listing Rule carve-out where disclosure would otherwise constitute a breach of law.

While the intent of the proposed measure is supported, Aussie Broadband is concerned that the scope of relief is too narrow. In particular, limiting protection to continuous disclosure obligations may leave entities exposed to ancillary legal risks, including potential allegations of misleading or deceptive conduct, where public statements are constrained by a lawful non-disclosure direction. We would therefore encourage consideration of targeted legal protections for entities acting in good faith and in accordance with such a direction.

5. Enforcement (Measure 5)

Aussie Broadband recognises the policy intent underpinning the proposal to expand the civil penalty framework. However, where entities are acting in good faith to comply with directions in complex and time-critical circumstances, the effectiveness of the regime will be best achieved through a regulatory approach that emphasises cooperation, transparency, guidance and support, rather than default reliance on punitive enforcement measures.

Enforcement should remain available for serious, reckless or persistent non-compliance, but should be applied in a way that recognises operational complexity, service-continuity risks and the need for rapid decision-making during national security incidents. A collaborative approach will better enable entities to comply with directions in a timely and operationally feasible manner, particularly in circumstances involving complex cyber incidents where entities are acting swiftly and in good faith to manage national security risks.

Conclusion

Aussie Broadband supports the overall policy intent of the proposed reforms and recognises the need for a more agile and effective framework to address national security risks in critical infrastructure.

Given the central role telecommunications providers play as enabling infrastructure for all SOCI sectors, it is essential that the expanded powers are accompanied by clear safeguards, transparent risk assessment frameworks, and practical implementation mechanisms.

In particular, we encourage the Department to:

- codify proportionality and staged implementation approaches
- provide clarity on vendor and governance risk assessment criteria
- establish minimum expectations for notice and transition where service continuity is at risk
- embed structured engagement mechanisms with industry before and after the exercise of powers.

We would welcome the opportunity to continue working with the Department to ensure these reforms are both effective in addressing national security risks and practical to implement in complex, real-world telecommunications environments.

Warm regards,