INTERNET ASSOCIATION OF AUSTRALIA LTD
ABN 71 817 988 968
ACN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

01 May 2026

To the Department of Home Affairs

By submission: Department of Home Affairs - Submission Form

RE: Proposed amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure Act 2018 – Consultation Paper

The Internet Association of Australia Ltd (**IAA**) thanks the Department of Home Affairs (**Department**) for the opportunity to respond to the Consultation Paper on the Proposed amendments to the Ministerial Directions Powers in Part 3 of the *Security of Critical Infrastructure Act 2018* (**SOCI Act**).

IAA is a member-based association representing Australia's Internet community. Our membership is largely comprised of small to medium sized Internet service providers (**ISPs**), on whose behalf IAA has been actively engaged in the development of the SOCI Act and subordinate legislative instruments that apply to the telecommunications sector. We write this response to the proposed Ministerial Directions Powers Reform similarly on behalf of our membership. Further, as a licensed carrier operating Internet exchanges across Australia, IAA itself is also a responsible entity subject to the SOCI Act, and is likely to be affected by the changes proposed in the Consultation Paper.

From the outset, we recognise and appreciate the ongoing work of the Department to continually improve the security and resilience level of Australia critical infrastructure. We understand the intent in pursuing the proposed reforms to ensure Government has legislative frameworks in place to proactively intervene in response to threats to Australia's national security. Indeed, given shifting global geopolitics and the continually evolving threat landscape, we understand the need for and support the development of legislative frameworks that allow for agility.

However, we are also concerned overall that the proposed reforms raise the risk of government encroaching on how industry conducts business, without due evidence that such reforms are indeed necessary. Given the ministerial powers are prescriptive in nature, we consider increased transparency is necessary to justify the changes being proposed to ensure the reform is fit for purpose and measured in the circumstances. Furthermore, we are concerned that the proposed reforms to the Part 3 of the SOCI Act raise the risk of blurring the distinction between the Part 3 powers and those addressed via other sections of the SOCI Act.

Our concerns are detailed further in relation to the respective measures throughout this response.

MEASURE 1 – AMENDMENTS TO THE EXISTING DIRECTIONS POWER IN SECTION 32

We understand that this proposed reform effectively relaxes restrictions and allow the Minister to issue directions in a more practical and expedient manner. We acknowledge the principle driving this reform as the current requirements are considered to not allow the Minister to intervene in a timely manner where such expedience is necessary given the serious nature of the threats posed to Australia's critical infrastructure, and thereby our overall national security.

However, we consider this is already addressed via the Part 3A powers where rapid Government intervention can be pursued in response to serious and time-sensitive threats. In recognition of the urgency and grave impact, there is a materially lower procedural threshold that applies to the Minister's use of the Part 3A powers. This is then balanced by stronger safeguards by way of reporting to the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) on the use of the Part 3A powers.

This is a key distinction to the circumstances giving rise to the use of the Part 3 directions power, which are intended to address risks that are not necessarily tied to a specific, time-sensitive incident. Hence the prescriptive Ministerial power under Part 3 is subject to greater checks and balances.

The concerns raised in the Consultation Paper in relation to current restraints and guardrails in relation to the Part 3 power seem to centre around timely action to proactively counter risks before they materialise. It is however unclear from the information provided what sort of risks require such timely intervention to justify the relaxing of restraints that would not be covered under the emergency-style intervention regime under Part 3A. We are thus concerned that reducing the restrictions on the Minister from issuing a section 32 direction would blur the lines between the Part 3 and Part 3A powers and conflates pre-emptive and proactive intervention with urgency.

We therefore request greater transparency and information to justify the proposed changes which would in effect, relax the checks and controls that have been set. To the extent it does not pose a threat to Australia's security, we would appreciate information on actual cases where, or in fact whether, there have been any actual threats that were unable to be mitigated or were less effectively mitigated due to the current constraints on the section 32 directions power, that also fell outside of the Part 3A regime. We consider this information necessary to fully understand whether and how the current limits and controls should be amended.

This is particularly the case in relation to the proposal to amend the 'regulatory exhaustion' requirement. We do not support that the proposed recalibration to merely consider whether other regulatory mechanisms could ***more*** effectively address an identified risk is sufficient in curtailing the use of the sections 32 directions power. Again, where there is a truly time-critical risk requiring government intervention, this should fall under Part 3A powers, which has commensurate scrutiny safeguards to ensure its proper use.

The current pre-condition that the Minister be satisfied that no other regulatory measure could be used to eliminate or reduce the identified security risk recognises that the directions power is extraordinarily prescriptive and should only be relied upon as a matter of last resort in rare circumstances where it is genuinely necessary to do so. Where there are other less prescriptive regulatory measures that can be taken, these should be prioritised, and not only 'considered'. This proposed threshold poses the risk of the directions power being used as a first-line tool, as opposed to remaining an exceptional power reserved for serious cases, undermining the legislative principle of proportionality that underpins the SOCI Act. Noting there are no requirements for the Minister to report on the use of the Part 3 powers to ensure its proper and justified use, this is particularly concerning.

Notwithstanding our position that reform to the current restraints on the use of the Part 3 power has not been fully justified and therefore cannot be supported, we make the below recommendations in the event the reforms are pursued:

At minimum, there must be public reporting obligations on the use of the Part 3 directions power to ensure appropriate scrutiny.

Currently, there are no corresponding requirements for reporting on the use of the Part 3 directions power to the PJCIS as is the case for use of Part 3A powers. We consider transparency on the use of extraordinary powers as critical, especially where use of the Part 3 directions powers will be subject to lower procedural thresholds.

We also recommend the recalibration of paragraph 32(3)(d) as follows:

> *(d) the Minister is satisfied on reasonable grounds that existing regulatory systems of the Commonwealth, a State or Territory have:*
>
> *(i) been considered and, where reasonably practicable, utilised; and*
>
> *(ii) been found not to be sufficient, whether individually or in combination, to eliminate or adequately reduce the risk mentioned in subsection (1) within a reasonable timeframe.*

We consider this approach strikes a more appropriate balance by introducing the flexibility sought under the proposed reform, and ensuring that the consideration and use of other regulatory measures is tied to effectiveness and not just theoretical availability that is weaponised to unnecessarily delay action.

We fully support the proposal that the list of Ministers that must be consulted under section 33 be expanded to include relevant Commonwealth Ministers and agencies.

MEASURE 2 – CONDITIONS POWER

1. ***Relative to maintaining the status quo, what non-regulatory or lighter-touch approaches could reasonably achieve a similar outcome in your context?***

Again, we understand the intent behind the proposed new conditions power but reiterate our concerns about increasing Government encroachment on how industry conducts business. However, we consider the issue is already addressed via the Critical Infrastructure Risk Management Program (**CIRMP**) obligations. Additionally, to improve overall management of risks in governance arrangements across Australia's critical infrastructure ecosystem, **we recommend the Department publish guidance on governance safeguards to mitigate risks relating to governance controls.**

Should this conditions power still be seen as necessary for extreme scenarios, given its extraordinarily prescriptive nature, we note that there should be increased transparency in its use and effectiveness. **Similar to our recommendation in respect of Measure 1, use of the conditions power should be subject to reporting.**

MEASURE 3 – RESTRICTIONS ON USE OF HIGH-RISK VENDORS, PRODUCTS AND SERVICES

We iterate our concerns that the Government is increasing its ability to prescribe how industry does business. We understand that supply chain hazards are a serious concern especially in times of evolving geopolitical uncertainty and thus supply chain assurance is one of the core hazards addressed under the CIRMP.

Additionally, the proposed enhanced CIRMP rules, currently under simultaneous consultation, further addresses this for those asset classes that would be subject to the enhanced rules. In the consultation paper for the enhanced CIRMP rules, we note that the Department expresses its intentions not to whitelist or blacklist specific vendors and the adherence to the proportionality and practicability principles that currently underscore the SOCI legislative framework. However, this Measure 3 would indeed effectively blacklist vendors.

While we appreciate that the Department has set out considerations that must be had before the Minister could issue a direction, we do not consider this sufficiently curtails the use of this proposed power which would cause huge costs to industry. **For example, at minimum, the current restrictions and considerations on the use of the section 32 directions power under subsections 32(3) and 32(3)-(4) must apply to the proposed vendor directions power.**

Furthermore, due to the significant burdens that will disproportionately affect smaller providers as outlined below, we recommend that where responsible entities of an asset should be able to seek exemptions in the event the direction relates to an asset-class. The exemption model should place the onus on the responsible entity to demonstrate why the direction should not apply to its operations in adherence to the principle of proportionality.

2. ***How would a vendor-specific restriction of this kind interact with your current technology stack, procurement cycles, network/OT architecture, and operational processes? Are there key differences from the scenario that would affect implementation?***

3. ***Are there operational, contractual, supply-chain or technical impediments that could materially affect your ability to comply***

There is a high reliance on only a limited number of vendors for core telecommunications assets, which is compounded for smaller telecommunications providers due to resource constraints. There is also a high level of vendor lock-in due to the nature of technology but also due to contractual obligations and procurement being based on multi-year refresh cycles. We especially consider that sourcing alternative vendors and products may be completely out of budget for smaller providers.

4. ***What internal steps and approvals would be required to comply?***

At minimum, we consider the below internal steps and approvals would be required:

- Network-wide asset inventory and criticality mapping to identify affected equipment and dependencies
- Development of a replacement or remediation plan
- Negotiation of existing contracts with the high-risk vendor
- Undertaking procurement and tendering process
- Governance processes – such as board approval on expenditure and significant technical architecture
- Conducting laboratory and network integration testing
- Staged deployment and cutover windows
- Communicating with customers and stakeholders

5. ***What is a realistic timeline by milestone that maintains service availability and resilience? Identify the top three schedule drivers.***

We consider a realistic timeframe for full deployment and compliance with such a direction would be 24-36 months, broken down below:

- Asset inventory and identification of criticality mapping – 3-6 months
- Design of replacement plan – 3-6 months
- Procurement process – 6-12 months
- Testing – 3 months
- Deployment and migration – 9-12 months

We emphasise that smaller telecommunications operators, such as many of our members, have limited resources and competing priorities (including other regulatory compliance requirements) and will therefore be unable to execute such large-impact network changes in a timely manner.

6. What one-off activities would drive effort/cost? What ongoing activities would persist?

We consider the below activities in particular, would cause considerable cost and burdens for telecommunications providers:

- Capex costs associated with equipment replacement
- Opex costs associated with engineers' efforts in undertaking upskilling/re-skilling, network redesign, testing and deployment
- Contract negotiations which could also result in termination fees or duplication of cost

In relation to ongoing costs, we are primarily concerned about the higher cost base for providers that would result from a reduced trusted vendor pool. We expect that the blacklisting of certain vendors is likely to result in inflated costs for products and associated software maintenance costs which are already a huge cost for industry.

Again, we reiterate that these costs and burdens will be disproportionately felt by smaller providers. Especially in a context where the entire telecommunications sector would be competing for trusted hardware, smaller providers will be most affected by any supply constraints, and inflated costs due to their lack of bargaining power. We are extremely concerned that the use of the proposed power could result in smaller providers being forced to leave the market.

7. What are the likely market and competition implications (e.g., near-term vendor concentration, price effects, supply constraints, interoperability impacts) during transition? Would compliance have material impacts on customers, prices or service quality? Are there cumulative burden issues alongside other obligations (e.g., CIRMP, privacy, sectoral rules)?

We are highly concerned about the competition implications for the telecommunications market. As iterated above, the use of this proposed power will disproportionately affect smaller telecommunications providers and we consider there is a real risk that some providers will no longer be able to operate. In addition, telecommunications is a highly regulated sector and major network changes will give rise to various considerations relating to service delivery and network outages. These considerations and overlapping obligations again cause further burdens for smaller providers. We further note that telecommunications providers are already subject to a higher bar of risk management rules under the *Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025* which many of our members and smaller industry participants have expressed is causing significant regulatory burdens due to their limited resources.

With the telecommunications market already a constrained competitive landscape, we do not consider this potential outcome to be in the interest of the future of Australia's communications landscape. We especially note that smaller carriers often supply niche markets such as local regional or remote areas, and these communities will be most disadvantaged by any decline in market competition.

MEASURE 4 – DELAY CONTINUOUS DISCLOSURE REQUIREMENTS

We support this proposed measure and in addition, recommend its expansion to cover other disclosure obligations including (but not limited to) the below regulatory schemes:

- notifiable data breach scheme under the *Privacy Act 1988*; and
- communications of outage requirements for telecommunications providers under the *Telecommunications (Customer Communications for Outages) Industry Standard 2024.*

We consider there may be other relevant disclosure schemes but due to the compressed consultation timeframe, we have been unable to conduct a comprehensive review of existing disclosure requirements.

Given the existence of other regulatory schemes in addition to the continuous disclosure obligations under the *Corporations Act 2001*, we support Option 2 which would be broader in nature, and would therefore apply to an entity's disclosure obligations under other regulatory schemes.

However, we consider that this measure requires further review and consultation to ensure timeframes are practically feasible as certain schemes will require an entity to notify (whether the public, or affected individuals) by certain timeframes, which may be prior to when the Minister may have directed an entity to not disclose certain information in relation to a cyber-security incident.

Additionally, it would be prudent to introduce safe harbour provisions to provide assurance to industry that entities will not be penalised for failure to make certain notifications due to compliance with this proposed measure.

MEASURE 5 – INCREASED CIVIL PENALTY PROVISIONS

We understand and support the principle of harmonising the penalty units for non-compliance across the SOCI framework, particularly where this would promote consistency and clarity for industry. We also recognise that penalties should be set at an appropriate level that serves as a commensurate and proportionate deterrent to non-compliance, given the seriousness of risks to Australia's national security.

To that end, it is unclear whether there is evidence to suggest that businesses are treating the existing penalty settings as a 'cost of doing business' or that the current maximum of 250 penalty units has proven insufficient to drive compliance. For the purposes of promoting consistency, we consider reducing the maximum penalty units to 250 in respect of Part 2D requirements may be more appropriate in the circumstances.

We are concerned that the proposed significant increase to 2,000 penalty units would again disproportionately affect smaller entities. This may result in more conservative operational decision-making, particularly in the context of lack of regulatory understanding which is common amongst smaller entities. It may also result in increased legal and compliance overheads, diverting already limited resources from activities that would directly improve network security and resilience.

We also note that deterrence and enforcement via penalties is only one component of an effective compliance approach. Industry has greatly appreciated the Department's educative and consultative approach in relation to the SOCI framework reforms, and strongly recommend the Department's continued commitment to providing clear guidance and early and proactive engagement of responsible entities. Particularly due to the prescriptive nature of the Ministerial directions which would greatly affect operations and therefore likely to cause uncertainty and complexity in compliance, we consider providing clarity on the application of Ministerial directions through guidance materials and meaningful engagement with entities as crucial.

We particularly encourage targeted efforts to engage with smaller entities to drive overall security and resilience uplifts across the critical infrastructure landscape so as to reduce the need for extraordinary directions powers, and the risk of inadvertent non-compliance.

Once again, IAA appreciates the opportunity to contribute to the consultation on proposed amendments to the Ministerial Directions Powers in Part 3 of the *Security of Critical Infrastructure Act 2018*. We reiterate our commitment to working with the Department, Government, industry and other stakeholders to ensure uplifts to the security and resilience of Australia's critical infrastructure. To that end, we offer this submission to highlight challenges and issues in relation to the proposed changes with the aim of improving proportionality and effectiveness which we consider important to supporting the objectives of the SOCI framework and therefore Australia's national security. We look forward to continue collaborating on the proposed reforms to ensure the SOCI Act remains fit-for-purpose.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia Ltd (**IAA**) is a not-for-profit member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (WAIA), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations, and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IAA regularly engages with government and regulatory bodies on policy matters affecting the Internet industry. In particular, our advocacy efforts represent the small to medium sized internet service providers in Australia who are often disproportionately disadvantaged by law reform affecting the telecommunications sector. Our advocacy work is guided by the following principles:

We stand for an internet for the common good
We stand for an open internet platform
We stand for measured, effective and practical regulation

IAA is also a licenced telecommunications carrier and provides the IX-Australia service to Corporate and Affiliate members on a not-for-profit basis. It is the longest running carrier neutral Internet Exchange in Australia. Spanning seven states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.