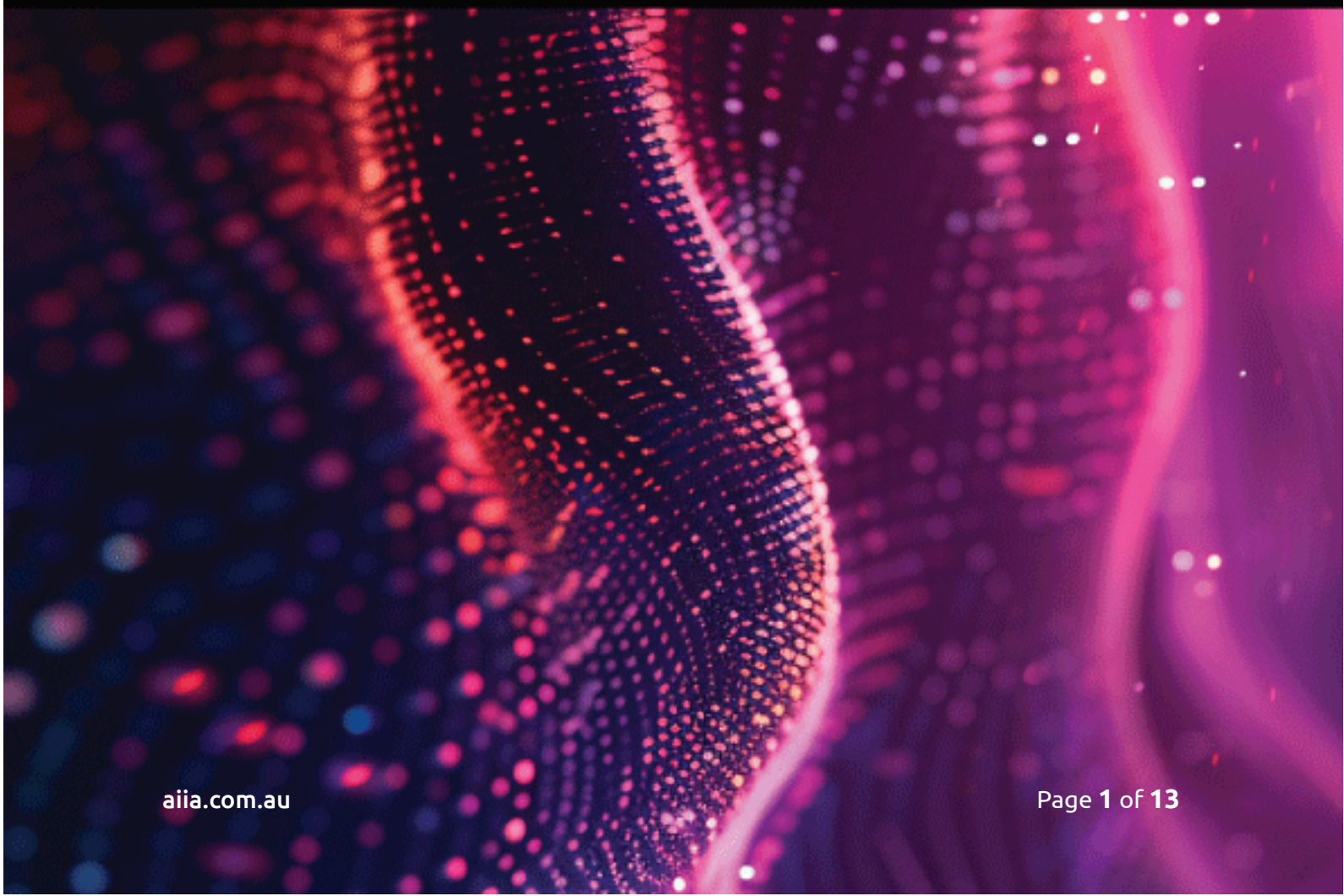
Australian Information Industry Association

Australian Information Industry Association

Submission on

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



About the AIIA

The Australian Information Industry Association (AIIA) is the nation's peak body for those in the digital ecosystem, leading strategic policy and advocacy to shape a thriving digital sector. Through strong engagement with government, industry, and the broader community, the AIIA ensures the voice of its members informs decision-making on technology, innovation, and digital capability.

Membership provides direct access to influential networks, premium events, and opportunities to collaborate on initiatives with the sector's best and brightest to drive industry growth, improve productivity, and secure Australia's place as a global technology leader. AIIA members access real collaboration, real connections, and real outcomes.

Introduction

The Australian Information Industry Association (AIIA) welcomes the opportunity to respond to the Department of Home Affairs' consultation paper on proposed amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure Act 2018 (SOCI Act).

The AIIA acknowledges and supports the Government's objective of ensuring Australia's critical infrastructure remains resilient against an evolving threat environment, including risks arising from foreign ownership, control or influence (FOCI), malicious cyber pre-positioning, and supply chain dependencies. We also recognise that practical experience with Part 3 has surfaced legitimate operational issues that justify targeted reform.[1]

However, the proposed package would significantly expand the scope, reach and consequences of Ministerial directions. Several measures contemplate decisions that could disrupt established commercial arrangements, override existing contractual settings, or impose material technical and governance obligations on entities (and indirectly, their vendors) where there has been no underlying conduct issue on the part of the entity itself. Reforms of this magnitude warrant correspondingly robust safeguards, definitional clarity, and review mechanisms. This submission outlines our principal concerns and recommendations.

[1] Jill Slay, *Independent Review of the Security of Critical Infrastructure Act 2018* (Final Report, Department of Home Affairs, March 2026).

Summary of Recommendations

The AIIA's principal recommendations are summarised below and are explained in more detail in the relevant sections of this submission.

- **Recommendation One:** Incorporate a substantive legislative review mechanism applicable across all Part 3 directions.
- **Recommendation Two:** Recognise vendor and supply chain flow-on effects in legislative design and supporting guidance.
- **Recommendation Three:** Require ASIO advice for entity-specific directions to be tailored to that entity, not generic.
- **Recommendation Four:** Confirm in legislative materials and guidance that section 32 will continue to operate as a genuine last resort.
- **Recommendation Five:** Apply express statutory scoping principles to the Conditions Power.
- **Recommendation Six:** Exclude conditions prohibiting offshore access, support or administration from the proposed Conditions Power.
- **Recommendation Seven:** Introduce a clearly defined framework for identifying "high-risk" vendors, products or services.
- **Recommendation Eight:** Apply enhanced procedural safeguards to class directions under Measure 3.
- **Recommendation Nine:** Address the interaction between any Australian disclosure-delay mechanism and foreign disclosure obligations.
- **Recommendation Ten:** Reconsider the proposed increase in the maximum civil penalty from 250 to 2,000 penalty units.

Absence of a Legislative Appeal Mechanism

A key cross-cutting concern with the proposed measures is the absence of any clearly articulated legislative appeal or merits-review mechanism. The consultation paper confirms that decisions to issue directions would be subject to judicial review, but judicial review is a narrow remedy. It is concerned with the legality of the decision-making process, not the substantive merits of the decision itself, the proportionality of the measures imposed, or whether less intrusive alternatives would have achieved the same outcome.

Given the breadth of the powers being proposed, this is, in our view, an inadequate safeguard. Directions issued under the expanded framework could:

- require an entity to migrate or restructure significant portions of its operating environment;
- compel changes to board composition, voting rights, or governance processes;
- prohibit the use of specified vendors, products, services or technologies across an entire sector by class direction;
- delay public disclosure of a cyber incident, with attendant implications for investors, customers and counterparties; and
- attract civil penalties of up to 2,000 penalty units for non-compliance.

Critically, several of these measures, most notably the proposed vendor-risk direction power in Measure 3, are systemic rather than conduct-based. An entity captured by a class direction may be required to cease using a vendor, restructure contracts, or implement compensating controls without having engaged in any breach of obligation, and without any specific finding of risk attributable to it. The risk being managed sits with the vendor or technology, not with the directed entity.

In these circumstances, judicial review alone does not provide a fair, proportionate or commercially workable safeguard. A directed entity facing significant operational, financial and reputational consequences should have access to a substantive avenue to test the basis and scope of the direction, including the proportionality of the conditions imposed, the adequacy of consultation, the availability of less intrusive alternatives, and the reasonableness of any transition timeframes.

Recommendation One:
The Government should incorporate a substantive legislative review mechanism applicable across all Part 3 directions, capable of considering the merits, proportionality and scope of a direction, and structured to accommodate sensitive intelligence material where necessary.

Flow-On Effects on Vendors and the Technology Industry

A second cross-cutting concern is that the consultation paper is largely framed around the relationship between Government and the directed entity. It does not, in our view, consider the flow-on effects of directions on the broader technology ecosystem, in particular, the vendors, service providers and supply chains that underpin the day-to-day operation of CI assets.

Modern CI entities rely heavily on third-party software, SaaS, cloud, managed services and hardware. A direction issued to a CI entity will frequently translate into requirements that flow through to vendors via commercial contracts, covering matters such as data residency, offshore access, support models, audit rights, segregation of environments, and personnel security. In some cases, vendors may be able to accommodate these requirements through existing or expanded sovereign offerings; in others, they will not, and the practical effect will be to force CI entities to switch vendors, redesign architectures, or absorb material costs.

These flow-on effects are particularly relevant given the Government's express intention that directions will not be published as legislative instruments. Vendors may therefore be required to negotiate complex changes with multiple customers in response to directions whose existence and content they cannot independently verify.

Recommendation Two:
The legislative design and supporting guidance should expressly recognise the role of vendors and supply chains in giving effect to directions. This should include:
(a) a requirement that the Minister consider material flow-on effects on vendors and supply chains as part of any decision to issue or scope a direction;
(b) reasonable transition timeframes that reflect supplier lead times and contract cycles; and
(c) protocols enabling directed entities to share sufficient information with affected vendors, consistent with the SOCI Act's protected information regime, to allow practical compliance.

Measure 1: Amendments to the Existing Directions Power in Section 32

The AIIA understands the practical difficulties identified with the existing Adverse Security Assessment (ASA) and "regulatory exhaustion" pre-conditions in section 32. We are not opposed in principle to recalibrating these guardrails so that the framework remains operable in time-sensitive circumstances. However, we have two specific concerns.

ASIO threat advice must be tailored, not generic

The proposed shift from a formal ASA to "tailored ASIO threat advice" as the intelligence input to a Ministerial direction is presented as a flexibility measure. We accept that flexibility may be appropriate in time-sensitive circumstances, but we are concerned that the proposed formulation does not, on its face, require the ASIO advice to be specific to the entity in question. A direction issued under section 32 may have profound consequences for an individual entity. The intelligence basis for that decision should be commensurately specific.

Generic threat advice (e.g. advice describing a class of risk, a category of vendor, or a jurisdiction) is appropriate to inform sectoral guidance and policy settings. It should not, however, be the sole or primary intelligence input justifying a direction issued to a named entity. Where ASIO advice is the foundation of an entity-specific direction, that advice should be tailored to the specific circumstances of the entity, the nature of the risk it is said to present, and the proposed mitigation.

Recommendation Three:
The legislation should expressly require that, where a Part 3 direction is issued to a specified entity, the ASIO advice relied upon by the Minister must be tailored and specific to that entity and the risk it is said to present. Generic or class-based threat assessments should not, of themselves, satisfy the intelligence threshold for an entity-specific direction.

Section 32 should remain a genuine last resort in practice

The proposed recalibration of the regulatory exhaustion test from a requirement that no other regulatory regime could be used, to a requirement that the Minister consider whether other regimes could more effectively address the risk, lowers the legal threshold. We acknowledge the operational rationale, but the AIIA considers it important that section 32 continues, in practice, to operate as a genuine last resort.

The original guardrails were designed to give industry confidence that SOCI directions would be reserved for circumstances where other levers had genuinely failed. If the legal threshold is softened without corresponding administrative discipline, there is a real risk that directions will be reached for too readily, with corresponding impacts on commercial certainty and investment.

Recommendation Four:
The Government should clarify in the legislative materials, supporting guidance and any explanatory memorandum, that section 32 will continue to operate as a genuine last resort. This commitment should be reinforced by transparent reporting on the use of Part 3 powers (in aggregate and de-identified form where necessary) to Parliament and to industry.

Measure 2: Conditions Power

The AIIA has concerns about the breadth of the proposed Conditions Power and the adequacy of the safeguards as currently described. The illustrative scope of conditions contemplated in the consultation paper is extensive, and the paper provides limited guidance on how individual conditions will be scoped to the minimum necessary in practice.

Breadth of the conditions and inadequate scoping discipline

The illustrative list of conditions set out in the consultation paper is extensive, ranging across access controls, personnel security, board composition, voting restrictions, board committees, cyber security baselines, segregation of systems, audit and reporting obligations. Each of these categories is reasonable in the abstract, but collectively they could amount to a comprehensive override of an entity's governance, operating model and supply chain arrangements.

The paper indicates that conditions would be "tailored, time-bound, and constrained to the minimum necessary," but provides limited guidance on how this scoping discipline will operate in practice. There is no requirement for the Minister to articulate why each individual condition is the least intrusive measure capable of addressing the identified risk; no requirement to consider the cumulative burden of multiple conditions; and no clear pathway for an affected entity to seek narrowing of conditions short of judicial review.

Offshore access prohibitions and impacts on vendors

The AIIA is particularly concerned about the conditions contemplating prohibitions on offshore access, support, or administration for critical systems, and mandated segregation of vendor environments from parent-company or shareholder systems. Many technology vendors and service providers operate global delivery and support models, in which engineering, security operations, customer support and back-office functions are distributed across multiple jurisdictions. These models are not incidental, they are fundamental to how modern software, SaaS and cloud services are delivered, and they enable 24/7 support, follow-the-sun operations, and access to specialised global expertise.

Open trade, including the free flow of data across borders, is central to Australia's digital economy, its trade relationships, and its international competitiveness.[2] Conditions of this kind run directly counter to that policy and to the operational reality of how modern technology services are delivered. To the extent there are specific national security concerns associated with offshore access, those concerns can be addressed through more targeted means already contemplated within the proposed power without resorting to a blanket prohibition on offshore access, support or administration.

Some vendors will be able to accommodate offshore-access prohibitions through existing or expanded sovereign offerings; many will not, particularly smaller and specialist vendors who cannot economically operate parallel Australian-only delivery infrastructure. Conditions that effectively force changes to a vendor's global operating model are unlikely to be a workable or proportionate governance tool in the SOCI context.

CIRMP-relevant data and SaaS vendors

Software and SaaS vendors frequently store or process data that is directly relevant to a CI entity's Critical Infrastructure Risk Management Program (CIRMP), including IT asset inventories, incident response workflows, vulnerability data, and risk registers. Conditions imposed on a CI customer requiring segregation, restricted access or onshore administration of such data could therefore translate directly into requirements on the underlying vendor's platform or service.

This raises practical challenges. A vendor serving multiple CI customers may face different, possibly inconsistent, requirements arising from different directions. Without clear scoping principles, the cumulative effect on vendors could be significant and disproportionate to the risk being managed in any individual case.

Recommendation Five:
The Conditions Power should be subject to express statutory scoping principles requiring the Minister to:
(a) articulate the specific risk each condition is designed to address;
(b) demonstrate why less intrusive measures would be insufficient;
(c) consider the cumulative burden of multiple conditions; and
(d) consider the impact on the entity's supply chain, including foreseeable impacts on vendors and service providers.

[2] Department of Foreign Affairs and Trade, *Digital Trade Strategy* (Australian Government, 2022).

Recommendation Six:
Conditions prohibiting offshore access, support or administration should be excluded from the proposed Conditions Power. Such conditions are inconsistent with the operating models of most modern technology vendors, run counter to Australia's stated commitment to open trade and cross-border data flows, and risk imposing disproportionate cost and disruption on vendors and CI entities alike.

Measure 3: Restrictions on the Use of High-Risk Vendors, Products or Services

Measure 3 contemplates Ministerial directions, including by class, that could restrict, remove, segment or impose compensating controls on the use of specified vendors, products, equipment, services or technologies across an entire sector. The reach of these directions is significant: a single decision could affect multiple CI entities, multiple commercial arrangements, and multiple vendors simultaneously, with consequences that extend well beyond the directly directed parties. We have three principal concerns.

"High-risk" is not defined

The consultation paper uses the term "high-risk vendors, products or services," but does not define it. Nor does it set out the criteria, indicators or process by which a vendor, product or service would be assessed as high-risk for the purposes of issuing a direction. The paper alludes to existing reference points (the Protective Security Policy Framework, the United Kingdom's Telecommunications (Security) Act 2021 framework) but does not commit to any particular methodology, threshold, or process.

This is a significant gap. A direction issued under Measure 3 could, in principle, affect any vendor, product or service used by CI entities, with profound commercial, reputational and operational consequences. Vendors are entitled to understand the basis on which they may be designated as high-risk, the evidence on which such a designation rests, and the avenues available to respond.

The AIIA notes that the consultation paper expressly states that the proposed reforms are intended to provide greater certainty for industry. In our view, in the absence of a clearly articulated framework for identifying high-risk vendors, products or services, Measure 3 as currently described introduces material uncertainty rather than reducing it.

Class directions and systemic flow-on effects

The proposed power expressly contemplates directions being issued to entities "by class." A single decision could therefore sweep across an entire sector, affecting all CI entities using a particular vendor or technology. The flow-on effects on the affected vendor could be severe and immediate, including loss of contracts, asset impairment, reputational

damage, and long-term exclusion from the Australian market, in circumstances where the vendor itself has neither been the subject of the direction nor afforded a clear right to make representations. This concentration of consequence in a single decision warrants a correspondingly robust process.

Contractual disruption and the absence of conduct

As noted in the overarching concerns, a class direction issued under Measure 3 could require CI customers to cease using, restrict, segment or impose compensating controls around a vendor's platform without the directed entity (or the vendor) having engaged in any breach of obligation. The risk being managed is systemic and originates upstream of any conduct by the directed entity. This makes the case for procedural protections, transition flexibility, and a substantive review mechanism considerably stronger than for measures targeted at conduct.

Recommendation Seven:
The legislation should incorporate a clearly defined framework for identifying "high-risk" vendors, products or services, including: (a) published criteria; (b) a transparent process for designation; (c) opportunities for affected vendors to make representations; and (d) clear documentation of the technical and factual basis for any designation. The framework should be developed in consultation with industry.

Recommendation Eight:
Class directions under Measure 3 should be accompanied by enhanced procedural safeguards, including a structured representations process for affected vendors, mandatory consideration of mitigations short of restriction, and transition timeframes that take account of supplier lead times, contract cycles, interoperability testing, and the availability of comparable alternatives.

Measure 4: Delay of Continuous Disclosure Requirements

The AIIA acknowledges that there may be circumstances in which premature public disclosure of a cyber incident could exacerbate national security or systemic economic risk. We wish to highlight an issue that the consultation paper does not, in our view, adequately address: the interaction of any Australian disclosure-delay mechanism with disclosure obligations in other jurisdictions.

Cross-jurisdictional conflicts

Many CI entities operate within global corporate groups, raise capital on foreign exchanges, or are subject to foreign reporting obligations through their customers, counterparties or regulators. Disclosure obligations arise across a range of foreign frameworks, including, for example, the United States Securities and Exchange Commission's cyber-incident disclosure rule (Form 8-K Item 1.05) and the European Union's NIS2 Directive.

An Australian direction or exemption that delays disclosure under the Corporations Act will not, of itself, suspend obligations arising under foreign law. An entity caught between an Australian disclosure delay and a foreign disclosure trigger could face genuine legal conflict. In some cases, the existence of the Australian direction itself may be material information that the entity is required to disclose offshore.

Recommendation Nine:
Before finalising the design of Measure 4, the Government should expressly consider and consult on:
(a) how the proposed mechanism would interact with foreign disclosure obligations; and
(b) what guidance or carve-outs would apply where compliance with an Australian direction or exemption would put an entity in breach of foreign law.

Measure 5: Increased Civil Penalty Provisions

The AIIA notes the proposal to increase the maximum civil penalty for non-compliance with a Part 3 Ministerial direction from 250 to 2,000 penalty units. We have concerns about whether the proposed quantum is proportionate to the scope of the directions power as expanded under this package, and we wish to flag a flow-on concern that has not, in our view, been adequately considered in the consultation paper: the predictable contractual consequences for vendors.

Proportionality of the proposed quantum

The consultation paper justifies the proposed figure by reference to alignment with the penalty settings under Part 2D of the SOCI Act. The Part 2D directions power, however, is materially narrower than the Part 3 power as expanded under these proposals. Part 2D allows the Minister to direct a carrier or carriage service provider not to use or supply a particular carriage service that would be prejudicial to security. The expanded Part 3 power, by contrast, would allow the Minister to require an entity to do or refrain from

doing almost anything, impose ongoing governance conditions, and restrict the use of vendors, products or services on a sector-wide basis. Direct alignment of penalty settings between two powers of materially different scope and consequence may not be apt.

Vendor flow-on contracting risk

An eight-fold increase in the maximum civil penalty will materially change the risk calculus of CI entities when they procure technology and services. CI entities exposed to substantially higher penalties for non-compliance with directions (including directions that may, as discussed above, flow through to vendors via contractual mechanisms) will rationally seek to push compliance risk onto their suppliers.

This is likely to manifest as increasingly stringent contractual and technical requirements imposed on vendors as a condition of continued engagement. Such requirements are not in themselves objectionable, some are reasonable, and some are already common in CI procurement. The concern is one of proportionality and cumulative effect. As penalty exposure rises, customer-side risk transfer is likely to escalate accordingly, with disproportionate impact on smaller and specialist vendors who lack the negotiating leverage of incumbent multinationals. This in turn could narrow the pool of vendors willing or able to serve CI customers, with negative consequences for competition, innovation, and resilience.

Recommendation Ten:
The Government should reconsider the proposed increase in the maximum civil penalty from 250 to 2,000 penalty units. While the AIIA recognises that the existing penalty may be inadequate to deter non-compliance with directions managing serious national security risks, an eight-fold increase calibrated by reference to the narrower Part 2D directions power may be disproportionate to the substantially broader Part 3 power as expanded under these proposals. Any final figure should be supported by a clear and proportionate basis and accompanied by guidance on reasonable contractual risk allocation between CI entities and their vendors.

Conclusion

The AIIA supports the Government's objective of strengthening the resilience of Australia's critical infrastructure. The measures proposed in the consultation paper, however, would significantly expand the scope and consequences of Part 3 directions, with implications that extend beyond directly directed entities to the vendors, service providers and supply chains on which they depend. The legislative design must include corresponding safeguards, definitional clarity, and review mechanisms commensurate with the breadth of the powers being proposed.

The AIIA welcomes the opportunity to engage further with the Department of Home Affairs as the legislative design progresses.