Data Centres Australia
PO Box 42
Highett, Victoria, 3190
contact@datacentres.org.au

Department of Home Affairs
Cyber and Infrastructure Security Centre

Friday 1 May, 2026

Re: Submission to the Proposed Amendments to Ministerial Directions Powers in Part 3 of the *Security of Critical Infrastructure (SOCI) Act 2018*

To the relevant officer,

Data Centres Australia is the peak body for the data centre sector in Australia. We represent data centre developers and operators, and the expanding data centre ecosystem, advancing Australia's national interest in the global race for artificial intelligence infrastructure.

Our members include hyperscale cloud providers, co-location data centre operators, and ecosystem partners and our membership covers 86% of current operational capacity. This diversity of membership is directly relevant to the SOCI Act reforms because the distinction between infrastructure operators and the customers who use that infrastructure is fundamental to how obligations should be assigned.

Data Centres Australia supports the intent of the SOCI Act and the objective of strengthening the security and resilience of Australia's critical infrastructure. Data centres are critical infrastructure, and our members take their security obligations seriously. A strong, clear and enforceable framework protects the sector's reputation, creates a level playing field, and contributes to national security.

However, we have significant concerns about several aspects of the proposed Ministerial Directions reforms. These concerns relate to the breadth and proportionality of the proposed powers and the fundamental question of how obligations are allocated between infrastructure operators and the customers who control the workloads running within those facilities.

This submission draws on feedback from Data Centres Australia members across the spectrum of data centre operations, including hyperscale, co-location and managed services providers. Data Centres Australia is also making a separate submission on the Exposure Draft of the Enhanced CIRMP Rules.

We make ourselves available for further consultation, workshops and briefings as the Department develops its reforms.

Yours sincerely,

[redacted]

[redacted]
Data Centres Australia
[redacted]

Data Centres AUSTRALIA

DATA CENTRES AUSTRALIA:
SUBMISSION TO THE PROPOSED AMENDMENTS TO MINISTERIAL DIRECTIONS POWERS IN PART 3 OF THE *SECURITY OF CRITICAL INFRASTRUCTURE (SOCI) ACT 2018*

Friday 1 May, 2026

Overarching Observations

The operator/customer distinction is fundamental

The single most important issue for the data centre sector in these reforms is the clear delineation of responsibilities between the infrastructure operator and the customer.

In a co-location data centre environment, the operator controls the building, power, cooling, physical security and network connectivity. The customer controls the computing workload, the data, the applications and the cybersecurity posture of their IT environment.

This distinction is not unique to data centres. It mirrors the relationship between a landlord and tenant, or between a utility provider and the end user. The SOCI Act reforms must ensure that obligations fall to the party with the ability to act. Assigning infrastructure operators responsibility for customer workloads, customer data, or customer cybersecurity decisions creates accountability without control, which is both unfair and ineffective.

This concern runs through every aspect of the reforms, from the expanded scope provisions to the Ministerial Directions powers to the enhanced CIRMP requirements. We address it throughout this submission but wish to flag it at the outset as Data Centres Australia's primary concern.

Support for stronger enforcement on a level playing field

Data Centres Australia supports stronger enforcement of SOCI Act obligations, provided enforcement applies consistently across all responsible entities. Members who invest significantly in compliance should not be commercially disadvantaged by competitors who do not. The Independent Review's findings show that some stakeholders are concerned about uneven compliance resonates with our membership.

However, the evidence base for the Independent Review's recommendation to move from a "light touch" approach to a penalty-based framework warrants scrutiny. The Mentimeter and survey data in the Review's appendices show that the dominant themes identified by respondents were complexity, fragmentation and regulatory duplication, not enforcement. When asked to identify the main areas for improvement of the SOCI Act, only seven respondents cited "penalties for non-compliance" and only two suggested "stronger penalties and consequences." The dominant concerns were about simplification, harmonisation and reducing overlap. Data Centres Australia is concerned that a small number of emotive responses may have driven a recommendation that is not proportionate to the evidence.

If true collaboration between government and industry is the objective, moving to a punitive framework may be counterproductive. Entities that have experienced cyber breaches and endured public scrutiny have still shared their learnings at Department of Home Affairs events. This kind of voluntary cooperation seems less likely if the framework is perceived as punitive rather than collaborative.

Data Centres Australia also notes that the Independent Review does not adequately consider the impact of these reforms on productivity, investment attraction or compliance costs, despite the prominence of cost concerns in survey responses. Australia is competing for global data centre investment. Moving the SOCI Act from a collaborative to a punitive framework sends a signal to international investors that must be weighed against the security benefits the reforms are intended to deliver.

Reducing regulatory duplication

Data Centres Australia strongly supports the Independent Review's recommendation to harmonise SOCI Act obligations with other regulatory frameworks including APRA CPS 234, ASIC's cyber resilience requirements, ISO 27001, and the NIST Cybersecurity Framework. Our members already report under multiple overlapping frameworks. A "report once" model for incident reporting and mutual recognition of existing compliance should be a priority.

Data Centres Australia would go further than the Review's recommendation. Rather than simply removing duplication from the SOCI Act, there is an opportunity to position SOCI as unifying legislation. Consideration should be given to pointing other Commonwealth and State legislation to the SOCI Act and requiring conformance with it, rather than maintaining parallel requirements across multiple frameworks. For example, a banking or finance entity with a compliant SOCI-mandated CIRMP should not need to satisfy separate risk management requirements under APRA's CPS 230. Similarly, the Hosting Certification Framework (HCF) administration and reporting could be further substantially incorporated into the SOCI framework rather than operating as a separate process. FIRB requirements that overlap with SOCI obligations should also be considered for consolidation.

The EU has demonstrated that a unified framework can regulate approximately 100,000 entities across 27 member states. Given Australia's relatively mature regulatory framework, a consolidated approach should be achievable and would deliver significant compliance efficiencies for industry while maintaining or improving security outcomes.

If a "report once" model involves a reporting portal, it must be designed in conjunction with industry. Current government portals, including FIRB and DISP systems, are inefficient and create unnecessary administrative burden. A fit-for-purpose portal co-designed with industry would deliver better data quality for government and lower compliance costs for entities.

Bi-directional information sharing

The Independent Review recommends mandating bidirectional information exchange between government and operators. Data Centres Australia supports this in-principle but notes that information sharing between government and industry has historically been one-way. Government briefings often summarise publicly available media reporting and lack sufficient specificity for businesses to make risk-based decisions. If bidirectional sharing is to be mandated, the quality and actionability of government-provided information must improve materially. A mandate that simply maintains the status quo of one-way reporting obligations will not deliver better security outcomes.

Stream 1: Ministerial Directions Reforms

General position

Data Centres Australia acknowledges that Ministerial Directions are intended as a power of last resort. We support the principle that government should have the ability to intervene in serious national security incidents affecting critical infrastructure. However, the extraordinary nature of these powers demands robust safeguards, proportionality, and clear limits on their exercise.

Our overarching concern is that several of the proposed reforms effectively reduce existing safeguards rather than strengthen them. The balance between government power and industry rights must be maintained, particularly given the proposed increase in civil penalties.

Proposal 1: Amendments to existing s32 Directions Power

Data Centres Australia does not support the proposed amendments.

The existing s32 power already includes important safeguards, including the requirement for an Adverse Security Assessment (ASA) and the exhaustion of other regulatory mechanisms before the power is exercised. The proposed amendments would effectively remove or weaken these safeguards.

These safeguards exist to balance the extraordinary nature of the power granted to the Minister. Removing them without adequate replacement would undermine the “last resort” characterisation of the power and create uncertainty for operators about when and how it might be exercised.

Data Centres Australia recommends that the ASA requirement and the exhaustion of other regulatory systems remain as prerequisites to the exercise of the s32 power. Entities subject to directions should have access to merits review of the proposed exercise of the power in its current form.

Proposal 2: New conditions power

Data Centres Australia does not support the introduction of a new conditions power.

Existing CIRMP and Hosting Certification Framework (HCF) processes already provide mechanisms to address the perceived risks. These frameworks should be taken into account in determining whether the conditions power can be exercised. Specifically, if an entity is compliant with its CIRMP and HCF obligations, the conditions power should not be available against that entity.

If, however, a conditions power was to be introduced, Data Centres Australia recommends further safeguards need to be added to ensure the conditions power must be genuinely used as a power of last resort. A detailed examination of measures to streamline the ASA process must be conducted before the ASA requirement is replaced, noting the ASA is an important step to ensuring any directions issued are necessary and remain a power of last resort.

Any condition imposed must materially and measurably uplift the security of the relevant critical infrastructure asset. It must not create or exacerbate any vulnerability or undermine availability or security. It must be appropriately tailored to the specific asset and the responsible entity. It must allow the entity to implement compensating controls in lieu of the specific condition where those controls achieve the same security outcome. And it must be imposed for the shortest possible timeframe to achieve the required security uplift.

Before imposing a 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 government customers.

Ministerial directions into live operational environments must include safeguards to prevent unintended service disruption and consider impacts on customer service level agreements and contractual obligations. The consequences of disrupting a data centre that supports banking, aviation, healthcare or government services extend far beyond the operator.

Transition timeframes must be realistic and commensurate with the impact of the condition. Directors must be protected from allegations of breach of directors' duties, and companies should be immune from loss or damage resulting from the implementation of a direction they were compelled to follow. Entities must be able to appeal on the merits a proposed exercise of the conditions power, and have the condition removed upon implementing appropriate compensating controls.

Proposal 3: Restrictions on high-risk vendors, products or services

Data Centres Australia does not support this proposal.

Restricting or banning the use of products, equipment or services that are already integrated in live data centre infrastructure could have a significant impact on operability and availability. Removal of a product or vendor is not always feasible in a market that is limited by supply and stretched by operational demand, particularly in unforeseen circumstances such as a global pandemic or supply chain disruption. Removing a product or service may also have the inadvertent effect of reducing the availability and integrity of the relevant critical infrastructure asset, or even its security.

Data Centres Australia recommends that government liaise with data centre operators and critical infrastructure owners at the earliest time that vendor concerns arise, so that mitigations can be put in place in an orderly way, including diversifying supply chains away from high-risk vendors. This proactive, collaborative approach will deliver better security outcomes than reactive, compulsory directions that risk operational disruption.

In the event DHA considers a targeted mechanism is necessary to address systemic vendor risks, it must be accompanied by a clear and transparent framework for identifying these risks, designed in partnership with industry.

Where the power is exercised, compensating controls should be permitted in lieu of a specific direction. If compensating controls can demonstrate that the risk is mitigated, the direction should be satisfied.

Industry entities, given their intimate knowledge of their operations, should provide government with a "reasonable timeframe" for compliance, having regard to the complexity of the environment, the hardware or firmware in question, and the implementation of interim compensating controls.

Entities subject to these directions must be protected from liability including vendor claims for breach of contract and customer claims from service degradation or reduced availability. Full merits review of any proposed exercise of this power should be available.

Proposal 4: Time-limited exemption from continuous disclosure rules

Data Centres Australia notes this proposal primarily affects ASX-listed entities. Of the two options presented, Option 2 appears preferable because it is framed as a positive obligation directed by the Minister which provides greater certainty. It also ensures the critical infrastructure regime sits within Home Affairs rather than being extended to the Treasury portfolio. Option 1 provides less certainty because it is framed as a discretion to be elected.

Proposal 5: Increase in civil penalties

Data Centres Australia notes the proposed increase to 2,000 penalty units. Where penalties are increased, the safeguards, review rights and proportionality considerations outlined above in relation to Proposals 1 through 3 become even more important. Higher penalties without adequate safeguards create a coercive framework rather than a collaborative one.

Multi-sector directions

Data Centres Australia notes that the reforms contemplate directions that operate across sector boundaries during multi-sector incidents. This is particularly relevant for data centres, which host workloads across banking, healthcare, government, telecommunications and other critical sectors.

Simultaneous directions to both the data centre operator and the customer could result in conflicting instructions during incidents. Defined coordination mechanisms are needed to prevent confusion and misaligned responses during high-pressure incident scenarios. The reforms should clarify how priority is established when a direction to an operator conflict with a direction to a customer, or with the customer's own regulatory obligations.

Conclusion

Data Centres Australia is concerned about the proposals being put forward. Existing powers provide the necessary safeguards given the extraordinary powers being given to the Minister, and these should not be weakened. Existing processes already provide mechanisms to adequately address the perceived risks. We strongly recommend the Department further consult industry on these changes.

Our key messages to the Department on the proposed Ministerial Directions reforms are:

Maintain the "last resort" character of Ministerial Directions: Existing safeguards should be retained, not weakened. The extraordinary nature of these powers demands proportionality, clear limits, and access to merits review for affected entities.

Ensure obligations align with control: The fundamental distinction between infrastructure operators and customers must be reflected in how directions are issued and applied. Operators cannot be held responsible for risks they cannot manage.

Provide adequate safeguards for entities subject to directions: Protection from liability, realistic transition timeframes, the ability to implement any compensating controls, and access to merits review are essential to ensure the reforms are collaborative rather than coercive.

Engage early on vendor restrictions: Government should liaise with operators at the earliest time that vendor concerns arise, enabling orderly risk mitigation rather than reactive, disruptive directions.

Clarify multi-sector coordination: Defined coordination mechanisms are needed to prevent conflicting directions to operators and customers during multi-sector incidents.

Maintain a collaborative framework: The evidence base for moving to a penalty-focused approach is weak. A punitive framework risks deterring the voluntary cooperation and international investment that strengthen Australia's critical infrastructure.

We look forward to continued engagement with the Department and stand ready to contribute to workshops, briefings and further consultation as the reforms are developed.

Data Centres Australia is also making a separate submission on the Proposed Amendments to Enhance the Critical Infrastructure Risk Management Program Rules (CIRMP Rules).

CONTACT

[redacted]
[redacted]
Data Centres Australia
[redacted]
[redacted]