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 Enhance the Critical Infrastructure Risk Management Program Rules (CIRMP Rules)

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 enhanced CIRMP Rules 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 enhanced CIRMP requirements. These concerns relate to the practical implementation of the requirements, the breadth of supply chain and FOCI obligations, 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 has also made a separate submission on the proposed amendments to Ministerial Directions Powers.

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

Yours sincerely,

[redacted]

[redacted]

Data Centres AUSTRALIA

DATA CENTRES AUSTRALIA:
SUBMISSION TO THE PROPOSED AMENDMENTS TO ENHANCE THE CRITICAL INFRASTRUCTURE RISK MANAGEMENT PROGRAM RULES (CIRMP RULES)

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 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 2: Enhanced CIRMP Rules

General position

As many of the specific scenarios outlined require entity level specificity, Data Centres Australia will respond at a general level. Data Centres Australia supports the objective of uplifting the maturity of risk management programs for critical infrastructure. Many of our members already operate at or above the proposed maturity levels. However, several of the proposed enhanced requirements are overly broad, practically burdensome, and risk imposing obligations on parties that do not have the control or visibility to comply.

Material risks: enhanced requirements (Section 6A)

New risk factors such as “economic stability” and “social stability” are broad and difficult for private companies to assess in isolation without objective benchmarks. The expectations around risk of compromise or impairment due to FOCI risk are also drafted very broadly (“as a result of, or in connection with”), without specification of the degree of causation required. Clear and objective guidance is needed to support compliance, ideally co-developed through the Trusted Information Sharing Network (TISN).

Cyber security: enhanced requirements

The definition of “critical system” is overly broad. The cyber security enhanced requirements should be narrowed to make clear that the obligations apply to systems that directly control the operation or availability of the relevant critical infrastructure asset, and do not extend to all corporate IT systems operated by the regulated entity.

Regarding the effective prohibition on remote access to operational technology control systems and critical business data, the geographic location of a remote accessor is not, in itself, a reliable indicator of security risk. The security of remote access arrangements is determined by the controls applied, not by the physical location of access. These factors should be reframed to focus on the need for robust controls governing any remote or offshore access to critical systems, rather than treating physical location as a determining factor.

Personnel security: enhanced requirements

Data Centres Australia supports AusCheck background checking as a mechanism for vetting critical workers in the critical infrastructure environment. However, clear rules are needed for the application of these requirements to operator staff, third-party vendors and emergency scenarios, particularly where urgent site access is required.

There may be operational difficulties in extending background checking requirements to offshore critical workers particularly for large MNC's, as different jurisdictions have different laws about background checks. More guidance should be published by the Department regarding what constitutes adequate compensating controls for offshore critical workers where specified background checks are unavailable.

The practical implications for hiring timelines, contractor mobilisation and emergency response capability should be carefully considered. Mandatory AusCheck for all personnel with access to critical infrastructure will add time and cost to recruitment in an already constrained and competitive environment. The result is probable cost increases for service contracts.

Supply chain vulnerability mapping

Data Centres Australia supports the principle of understanding and managing supply chain risk. However, the proposed requirement to map risks across the full vendor ecosystem is likely impractical given the global, multi-tier nature of data centre supply chains and the limited visibility operators have beyond their direct vendors.

The supply chain mapping obligations are overly broad and should be focused on higher-risk suppliers only, specifically suppliers that are not themselves subject to Australian critical infrastructure regulation and who supply components, systems or services that are directly integrated in the critical infrastructure asset's functions.

The vendor assessment obligations are also very broad and require extensive resources to be used in an untargeted manner by entities that may not be equipped to undertake them effectively. Not all entities will be able to make an effective assessment of foreign laws, restrictions, sanctions and other impediments across their entire vendor base.

Data Centres Australia recommends that vendor assessment obligations should apply only in respect of specified vendors identified by the government. The government should bear the onus of identifying risky vendors, rather than requiring entities to assess all their vendors on a speculative basis. This approach would be more targeted, more effective, and less burdensome.

Realistic implementation timeframes are essential. Supply chain and FOCI requirements represent a significant operational uplift and rushed or ineffective compliance outcomes benefit no one.

FOCI risk management

Extending FOCI requirements across vendors and potentially customers introduce significant complexity. In co-location environments, operators may need to request ownership and supply chain information from customers to complete their own FOCI risk assessments. This creates commercial friction, may slow customer onboarding, and imposes obligations that sit outside the operator's influence.

Data Centres Australia recommends that FOCI obligations be clearly limited to what the operator can reasonably control and assess, with guidance on what level of customer due diligence is expected and what constitutes adequate compliance where customers decline to provide information.

Physical security: enhanced requirements

The physical security enhanced requirements in section 11A could be read as requiring detailed physical security information to be documented in a CIRMP. Concentrating detailed physical security information in a single document would present a security risk. There should be flexibility in how physical security information is documented to avoid single-artefact concentration risk.

The operator/customer boundary in CIRMP

This is the most critical implementation issue for the data centre sector.

In co-location environments, the operator controls the physical infrastructure: building, power, cooling, physical security, network connectivity. The customer controls the IT workload: servers, applications, data, cybersecurity configuration. Risk ownership is shared, but it is not equal, and the allocation of responsibility must reflect the allocation of control.

CIRMP obligations must align with control and ability to act. Generic SOCI frameworks will not apply consistently across different data centre designs, operating models and customer profiles. Industry-specific guidance is essential to ensure consistent, practical application across the sector.

Data Centres Australia recommends that the Department consult with the data centre industry to develop specific guidance on how CIRMP obligations apply in co-location environments, including clear demarcation of which risks and obligations fall to the operator, and which fall to the customer.

External assurance

Data Centres Australia does not support a shift from board self-attestation to mandatory external assurance in its current form. Multiple controls on directors and boards already exist under the SOCI Act, ASIC directors' duties, and other regulatory frameworks. Introducing a requirement for external assurance providers risks creating an additional compliance industry without commensurate security benefit.

An obvious starting point for recognising a strong security posture is where multiple regulators already have visibility of the same entity. Where departments canvass other areas of government and find nothing adverse, this should be recognised as evidence of compliance maturity rather than requiring a separate, costly assurance process.

If external assurance is pursued, requirements need clarity on scope, responsibility and frequency. Assurance frameworks should align with existing standards where relevant, and care must be taken to avoid duplicate audits, unclear ownership and increased compliance cost with limited additional benefit.

Incident reporting expansion

Data Centres Australia notes the Review's recommendation to expand incident reporting to cover "all types of outages" including offshore operations. Data Centres Australia does not support this expansion without further detail and consultation. Reporting every outage, regardless of cause or materiality, would create a massive compliance burden without meaningful improvement in national security posture. The extra-territorial application of Australian reporting requirements to offshore operations raises additional legal and practical complexities that have not been adequately considered. Incident reporting should remain focused on events that have a material impact on the availability, integrity or security of the critical infrastructure asset.

Conclusion

Data Centres Australia supports the objective of uplifting the maturity of risk management programs for critical infrastructure. Our members take their obligations seriously and many already operate at or above the proposed maturity levels.

Our key messages to the Department on the Enhanced CIRMP Rules are:

Ensure obligations align with control. The fundamental distinction between infrastructure operators and customers must be reflected throughout the enhanced CIRMP requirements. Operators cannot be held responsible for risks they cannot manage. Industry-specific guidance for co-location environments is essential.

Focus supply chain and FOCI obligations on identified risks. Broad, untargeted mapping requirements impose significant burden without commensurate security benefit. Government should bear the onus of identifying high-risk vendors, with entities then required to manage those identified risks.

Allow realistic implementation timeframes. The enhanced CIRMP requirements represent a significant operational uplift. Rushed compliance outcomes benefit no one. Industry consultation on implementation timelines is essential.

Reduce regulatory duplication. Go beyond harmonisation to position SOCI as unifying legislation that other frameworks point to. Implement a "report once" model with a fit-for-purpose portal co-designed with industry. Our members already report under multiple overlapping frameworks, and the compliance burden is significant.

Ensure information sharing is genuinely bidirectional. If government mandates information sharing from industry, the quality and actionability of information flowing back to industry must improve materially.

Retain board self-attestation. The shift to mandatory external assurance risks creating a compliance industry without commensurate security benefit. Existing accountability mechanisms are adequate.

Keep incident reporting focused. Expanding reporting to cover all outages including offshore operations would create a massive compliance burden without meaningful improvement in national security posture.

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 has also made a separate submission on the Proposed Amendments to Ministerial Directions Powers in Part 3 of the *Security of Critical Infrastructure (SOCI) Act 2018*.

CONTACT