BCA
Business Council of Australia

Enhancements to the Critical Infrastructure Risk Management Program Rules under the SOCI Act

BCA submission

February 2026

Contents

1. Executive summary

The Business Council of Australia (BCA) welcomes the opportunity to provide a submission on proposed amendments to the Critical Infrastructure Risk Management Program (CIRMP) Rules for high-risk asset classes.

The BCA represents and advocates for some of Australia's largest employers, operating across all sectors of the economy. Our members include critical infrastructure operators that have a strong interest in regulatory settings that support productivity, security and long-term economic growth.

We support a targeted uplift to the CIRMP Rules where it delivers a clear and proportionate reduction in risk. Measures such as strengthening cyber maturity are sensible and aligned with the current threat environment.

However, several proposed requirements – particularly around cyber security, foreign ownership and personnel screening – are not calibrated to the operational realities of many critical infrastructure operators and risk imposing cost and delay without a commensurate security benefit.

In particular, the energy sector is operating through a complex and time critical transition to lower emissions. Regulatory settings that constrain access to essential technology, skilled labour or established supply chains will directly increase costs and extend delivery timelines.

Overall, government should ensure CIRMP amendments are proportionate, risk-targeted, and calibrated to avoid imposing unnecessary cost and delay on critical infrastructure operators.

2. Key recommendations

Recommendation 1.

Government should clarify and recalibrate cyber uplift requirements (including segregation and three-month isolation capability) so they are achievable in modern cloud-connected environments and account for long technology renewal cycles.

Recommendation 2.

Government should allow continued use of vendors where substitution is not viable, provided defined compensating controls are applied via clear guidance on additional security measures.

Recommendation 3.

Government should establish clear benchmarks and extend timeframes for the FOCI framework to ensure consistent, practical and proportionate implementation.

Recommendation 4.

Government should avoid mandating AusCheck for all critical workers, but if implemented should apply a risk-tiered approach, enable third-party administration, clarify offshore requirements, and ensure processing times are under 20 working days.

Recommendation 5.

Government should provide clear guidance on the scope, depth and frequency of supply chain mapping requirements.

Recommendation 6.

Government should adopt a staged implementation approach, prioritising higher risks by 30 June 2028 and allowing a further 12–18 months for lower-risk requirements.

3. Detail

3.1 Cyber security uplift

The proposal to move from a cyber framework maturity level 1 to level 2 should be about targeting real risks. However, even if taking a triaging approach to addressing risks, uplifting maturity is already difficult in environments built on outsourced "build and run" models and global SaaS platforms, where long-term contracts are not designed to flex around specific Australian requirements.

Similarly, different controls and assets are unable to have their maturity uplifted at the same pace. Some assets will already be on a decommission path, and high-cost cyber uplift efforts would use resources that may be better spent elsewhere. Government should consider allowing organisations to set maturity targets by risk, control domain or asset, recognising that improvement will often be uneven across a system.

The proposal for "practical" network segregation also runs into the reality of how modern critical infrastructure is built. Today's environments are highly distributed and deeply interconnected, often sitting on public cloud platforms. Full isolation or air-gapping is effectively unachievable. Many modern critical infrastructure systems depend on tens of thousands of daily interactions with external systems and partners. If systems were isolated, they would not have the instructions, data, or coordination needed to function in any meaningful way. The proposed requirement to operate independently for three months in the event of isolation is similarly unrealistic.

Obligations to mitigate new risks from AI deployment, offshore remote access to critical data and legacy hardware and software make sense but require further clarification. Components of critical infrastructure assets are subject to long renewal cycles (including for security) of up to 10 years, sometimes more in the cases of operational technology and offshore providers. Changing these systems rapidly – or addressing new requirements to on-shore them – would present complex and costly contract re-negotiations for many critical infrastructure operators.

Recommendation 1.

Government should clarify and recalibrate cyber uplift requirements (including segregation and three-month isolation capability) so they are achievable in modern cloud-connected environments and account for long technology renewal cycles.

3.2 Vendors of concern and foreign ownership, control or influence (FOCI)

The BCA recognises the risks of undue foreign ownership, control or influence in critical infrastructure. However, the proposed approach to vendors of concern does not sufficiently account for the structure of the global original equipment manufacturer (OEM) market. In several critical technology domains there are limited or no commercially or operationally viable alternatives. A framework that effectively disqualifies these vendors would be unworkable and, in some cases, would leave no compliant options available.

Where substitution is not commercially or operationally feasible, the framework should explicitly permit the continued use of such vendors, provided the critical infrastructure owner implements appropriate compensating controls. To support this approach, Government should issue clear and practical guidance on what constitutes sufficient controls. Without that clarity, regulated entities are likely to adopt overly conservative interpretations of regulatory expectations, potentially resulting in disproportionate costs and operational disruption without a commensurate improvement in security outcomes.

Recommendation 2.

Government should allow continued use of vendors where substitution is not viable, provided defined compensating controls are applied via clear guidance on additional security measures.

3.3 FOCI framework more broadly

The proposed FOCI requirements are ambiguous and place responsibility on businesses to make challenging geopolitical risk judgements. It may also lead to inconsistent assessments (and therefore outcomes) across the sector – and possibly inconsistent with government assessments.

Although the Australian Government provides welcome guidance on these issues from time to time, a narrower framework with clear benchmarks would improve consistency, reduce duplication of effort, and better align industry assessments with government risk tolerance.

The proposal that responsible entities would have to minimise or eliminate material risks associated with foreign ownership or influence "as far as reasonably practicable" within six months of the amended CIRMP Rules commencing is problematic, especially in circumstances where there are complex, multi-year contractual arrangements. A longer timeframe with a triaging approach would be more realistic.

Recommendation 4: Government should establish clear benchmarks and extend timeframes for the FOCI framework to ensure consistent, practical and proportionate implementation.

Recommendation 3.

Government should establish clear benchmarks and extend timeframes for the FOCI framework to ensure consistent, practical and proportionate implementation.

3.4 Strengthened background checking and AusCheck

Mandating AusCheck checks for all critical workers would be resource intensive and create material recruitment and mobilisation delays. The current indicative six-week AusCheck assessment window is misaligned with standard onboarding timelines. It means critical infrastructure owners would have difficulty fulfilling workforce needs.

Also, AusCheck has significant limitations: it examines only a point in time, excludes psychological and behavioural attributes and is restricted to on-shore critical workers. We argue that AusCheck should not be mandated and instead businesses should be able to prove (as they do now) through other means that they are meeting their critical worker obligations.

However, if adopted, this proposal should:

- be risk tiered, allowing entities to define the highest risk roles to which checks apply,
- allow contractors to manage checks independently,
- permit the use of third-party administrators,
- provide clear guidance for offshore personnel, and
- be adequately resourced to ensure turnaround times of fewer than 20 working days – anything longer will materially impact workforce availability and increase reliance on interim risk workarounds.

Recommendation 4.

Government should avoid mandating AusCheck for all critical workers, but if implemented should apply a risk-tiered approach, enable third-party administration, clarify offshore requirements, and ensure processing times are under 20 working days.

3.5 Supply chain mapping

As described above, modern critical infrastructure networks are very complex. The proposal that a responsible entity should discover and assess supply chain vulnerabilities and mitigating controls, and where possible, include details regarding supplier diversification and redundancy planning, would likely be a large and costly endeavour.

There is no definition of "supply chain" in the *Security of Critical Infrastructure Act 2018* or current CIRMP Rules. The *Guidance for the Critical Infrastructure Risk Management Program* document does contains some pointers to help describe a "supply chain". However, if the expectation is detailed mapping, it would require detailed guidance. This should include the expected scope, depth and frequency of mapping to avoid open-ended and duplicative compliance activity.

Recommendation 5.

Government should provide clear guidance on the scope, depth and frequency of supply chain mapping requirements.

3.6 Timelines

Many of the proposals would be complex, expensive, and time consuming. This means that the proposed compliance deadline of 30 June 2028 is unrealistic and would become a "rush to failure".

The impact of changes will ultimately be borne through channels such as higher costs for customers or changes to investment, operating and maintenance costs. By directing investment into the highest risks first, a risk-based, staged implementation would minimise these effects and better balance security with affordability and availability.

The BCA recommends a staged approached for implementation, where higher risks are addressed with priority by 30 June 2028, and with lower risks addressed in the following 12 to 18 months.

Along with critical infrastructure operators, a staged approach would also ease the burden on the Federal Government, which would similarly need to be ready by 30 June 2028 to adequately administer significantly expanded CIRMP requirements in a timely and accurate manner.

Finally, the *Addendum to the proposed amendments to enhance the CIRMP Rules* proposes a new requirement for a physical security plan. The BCA supports this inclusion, but notes that it would increase the compliance burden, further supporting a staged implementation approach.

Recommendation 6.

Government should adopt a staged implementation approach, prioritising higher risks by 30 June 2028 and allowing a further 12–18 months for lower-risk requirements.

3.7 Conclusion

The BCA supports a strong and resilient critical infrastructure framework. To be effective, any proposed amendments must be risk weighted, clear in their expectations, and grounded in commercial and operational realities. Adjusting the proposals in the areas outlined above would materially improve their workability while preserving the underlying security intent.

BCA

Business Council of Australia

BUSINESS COUNCIL OF AUSTRALIA
GPO Box 1472
Melbourne 3001
T 03 8664 2664
www.bca.com.au