CISO Lens Pty Ltd
PO Box 6406
North Sydney, NSW 2059
Australia
www.cisolens.com

13 February 2026

Critical Infrastructure Security Centre
Department of Home Affairs

Submission on proposed amendments to enhance the Critical Infrastructure Risk Management Program Rules (CIRMP Rules)

CISO Lens welcomes the opportunity to make a submission to the Department of Home Affairs regarding proposed amendments to enhance the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 (CIRMP Rules).

CISO Lens is a strategic information sharing and analysis community that fosters collaboration among cyber security executives and operational leaders from Australia's largest and most complex organisations. Our mission is to help our members deliver outstanding security outcomes for their organisations and the communities they serve. We hold a deep understanding of the cyber security risks, issues, and opportunities they face, and advocate for greater collaboration between government and the private sector to improve Australia's cyber security posture.

Collectively, our member organisations:

- Represent about 54 per cent of the market cap value of the ASX All Ordinaries index.
- Employ more than 1.5 million people, mostly based in Australia.
- Operated with a combined annual security budget of more than $2.7 billion in FY24.
- Are responsible for between 35-40 per cent of security spend in the Australia / New Zealand region.

We recognise and appreciate the need for continued evolution of Australia's critical infrastructure security measures. We operate in a highly volatile and rapidly changing global threat landscape, particularly in the cyber security domain, and the need for commensurate protections is well understood. Our members take their requirements under the CIRMP Rules very seriously, and work hard to continually enhance the protection of critical assets under their control.

Consultation with CISO Lens members impacted by the proposed reforms has identified several items for the Department's consideration. These items are presented in the table below. It is important to note that our feedback is drawn from consideration of cyber security risks, issues and opportunities associated with the proposed reforms, and do not necessarily reflect the opinions of other hazard owners within organisations subject to CIRMP Rules.

Please contact me directly via [redacted] if you would like to discuss any aspect of this submission.

Yours truly,

[redacted]

David Cullen
Director, National Advocacy and Uplift

FEEDBACK ON PROPOSED REFORMS

Reform Item	Comment
All-hazard 1: Consideration of specified risk advice	It is currently proposed that responsible entities will have 12 months from the identification of specified risk advice to consider the advice, identify whether it poses a material risk to the availability or function of their asset, and minimise or eliminate the material risks, as far as reasonably practicable. Noting the rapidly evolving global cyber threat environment and the persistent threat to critical infrastructure and essential services, we anticipate there will almost certainly be a future need for the Department to designate cyber security intelligence as specified risk advice, to assist with protecting critical infrastructure assets from imminent or active nationally significant cyber threats. This may include designating *'Act Now'* cyber security alerts from the Australian Signals Directorate. Noting that a 12-month window to consider and act on specified risk advice does not align with the speed and velocity of contemporary cyber threats, particularly those requiring immediate attention to protect critical infrastructure assets, we recommend the Department explore the adoption of a tiered action model akin to: • Immediate action required – must be considered and, if posing a risk to the availability or function of their asset, actioned as far as reasonably practicable within 72 hours • Priority – must be considered and, if posing a risk to the availability or function of their asset, actioned as far as reasonably practicable within 30 days • Routine – consider the advice, identify whether it poses a material risk to the availability or function of their asset, and minimise or eliminate the material risks, as far as reasonably practicable within 12-months. If adopted, we further recommend the Department specify risk advice for immediate action (i.e., 72 hours) only in the most extreme circumstances, such as intelligence regarding a credible imminent or active threat to critical infrastructure assets across multiple sectors and/or jurisdictions, which if materialised would result in activation of Australia's national crisis management arrangements and require coordination at Tier 3 or Tier 4 of the Australian Government Crisis Management Framework.
All-hazard 2: All-hazard material risks	The Department raises valid concerns regarding risks associated with foreign ownership, control and influence (FOCI) of critical

- foreign ownership, control and influence	assets. Our members have a mature understanding of these risks, and work is already occurring within large organisations to improve FOCI risk identification, analysis and management. If the Department proceeds with this enhanced requirement, our members would benefit from greater access to government insights about the specific countries, vendors and technologies of concern, in order to simplify the management of FOCI risk. It is common for members to provide us with feedback that highlights the difficulty they experience in sourcing official information about specific countries, vendors and technologies of concern, which is essential to their FOCI risk assessment process.
Cyber 1: Cyber security framework uplift *and* **Cyber 2: Critical systems network protection**	While the need for improved maturity (aligned to a recognised framework) and enhanced network segmentation is well appreciated—and broadly supported as an important risk management approach—our members note the timeframe and costs associated with lifting controls from maturity level 1 to maturity level 2, and adopting the required network segmentation, will challenge many organisations. Specifically, concerns exist this timeline is likely out of reach for many smaller and mid-sized regulated entities, particularly those who already experience difficulty securing budget and organisational support to adopt baseline controls. Our members also expressed concern about whether the domestic cyber security market has sufficient resources to support all organisations requiring external assistance to implement the reforms. Members are concerned that a limited pool of experts could drive higher service prices, placing added cost pressures on impacted organisations. Consideration should be given to the use of a staged, risk-based (tiered) implementation timeline for compliance. Members also cited specific items for the Department to consider. <u>Enhanced maturity of third-party managed hardware and software</u> Where relevant hardware (incl. OT) and software (incl. SaaS) is operated by third parties, it could be very difficult for regulated entities to meet the enhanced maturity obligations where their managed service providers are reluctant to invest in necessary upgrades. For instance, some very large critical infrastructure entities rely heavily on custom built automation and robotics to manage their inventory. These services are implemented and managed by third-parties on behalf of Australian organisations, and are critical assets for the purpose of SOCI Act and the CIRMP. Where it is necessary to enhance the maturity of controls applied to these services (such

	as stronger MFA, backups and logging), members anticipate that vendors will almost certainly push those costs back to customers, which may then flow down to consumers. In extreme cases, managed service providers may also refuse to improve the maturity of controls, with limited options for diversification available to their customers. Consideration should be given to how this matter might be addressed through the proposed enhancements. <u>Operational independence – 3 months isolation</u> Also of interest was the proposed requirement for ensuring critical systems are operationally independent from other IT systems and networks to the greatest extent possible, such that they can be isolated for a period of 3 months while maintaining critical services. We have received feedback that raises questions over the potential for many regulated entities to meet this requirement. For instance: • Some entities' IT systems communicate tens of thousands of times daily with the systems of suppliers and transport providers in order to purchase and deliver their products into the supply chain. If isolated, a business BCP process to replicate this interaction over a sustained period is largely unrealistic. • Most systems form a chain of interactions to enact critical business processes. Isolated components on their own will not have the instructions/data needed to perform their function. At a technical level, many critical systems are highly dependent on centralised technology services and service providers, not least the public cloud which hosts almost all business applications.
Cyber 3: Multi-factor authentication (MFA)	Our members appreciate the importance and value of MFA as a cyber security control, and request the Department offer entities flexibility in how this requirement is implemented (tied to their internal threat and risk assessments).
Cyber 4: Enhancing cyber material risks	Our members cite a variety of projects and programs already underway within their organisations to identify and manage risks associated with legacy software and technology; new and emerging technologies (including Artificial Intelligence), and offshore access to systems and data. Feedback on the proposed reforms suggests the rules should remain at the process/system level – i.e., ensure a process and system exists to manage emerging risks – as opposed to individual requirements relating to each new and emerging technology or material risk.

	On mitigating risks from offshore remote access to critical data, feedback from members indicates arrangements with offshore providers would usually be on a multi-year contractual basis. Changing these rapidly, or requirements to on-shore to mitigate risk, would be commercially problematic and there would be substantial business risk given entities would be transitioning technology support to an entirely different team in a different location. On mitigating risks from legacy (unsupported) hardware/software, our members note that many organisations have large installed asset bases of IT equipment, some of which is knowingly unsupported. Large and mature organisations are already heavily selective in what they let fall into this category, so there is an acceptable balance between risk and available funding. Similarly, there are some software platforms where the risk of them being unsupported for a time is unavoidable for a variety of reasons. Any enhanced requirement that restricts the use of unsupported hardware or software should be further explored with industry prior to the adoption of new regulation.
Supply Chain 1: Supply chain vulnerability mapping	Although most large and complex organisations in Australia will likely have a detailed understanding of their supply chain and related dependencies (built in support of their business continuity and resilience programs), the proposed reforms will support further maturity of these programs, and drive uplift among less mature regulated entities.
Supply Chain 2: Vendors of concern	This work serves as an extension of Supply Chain 1 and All-hazard 2.
Personnel 1: Personnel security plan	We support the Department's focus on improved management of cyber (and other) risks arising from compromised credentials and exploitation resulting from personnel travel, both official and personal; and exposure of physical and digital critical assets from visiting officials and delegations.
Personnel 2: Strengthened background checking *and* **Personnel 3: Enhancing personnel material risks**	We support efforts to improve the screening of workers to proactively identify and manage any personnel security risks, and the management of identified personnel material risks, that may impact the confidentiality, integrity or availability of critical assets and related systems or data. However, we note there are limitations regarding the range of risk indicators that can be detected via the AusCheck program, as we understand it is limited to a point in time, excludes psychological and behavioural attributes and is restricted to on-shore critical workers. Notwithstanding these limitations, where the AusCheck program is to be used, we encourage the Department to consider a stronger position on this item, including consideration of a continuous checking regime, whereby persons screened for work in relation to critical assets are subject to regular AusCheck screening, rather than at 5-year intervals.

	We note the Australian Criminal Intelligence Commission (ACIC) is working collaboratively with Commonwealth, state and territory stakeholders, including screening units and police agencies, to scope, design and trial a National Continuous Checking Capability (NCCC).

[Submission ends]