Australian Government
Department of Home Affairs

Consultation on the Exposure Draft of the *Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules*

The Minister for Home Affairs undertook public consultation on the Exposure Draft of the Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules between 25 March and 1 May 2026. The consultation information set out below outlines the feedback that was received as part of this consultation process.

Engagement

During the consultation period, the Department of Home Affairs:

- published the Exposure Draft on its website – inviting submissions to the minister
- provided a copy of the Exposure Draft to all First Ministers, inviting submissions to the minister
- hosted 7 online engagement sessions, addressing more than 640 attendees from the public and across the Trusted Information Sharing Network (TISN).

Engagement summary: 25 March 2026 – 1 May 2026	
Total number of online engagements (industry and all levels of government)	7
Total number of attendees at online engagements	640+
TISN engagements	2
Total number of attendees at TISN engagements	536
Public online engagements	1
Total number of attendees at public online townhalls	88
Targeted engagement with utility regulators	1
Total number of attendees of utility regulators	1
Targeted stakeholder engagement	3
Total number of attendees	15+

Submissions

The Minister received and considered 27 written submissions during this consultation period.

These submissions have been published on the Department of Home Affairs website, except those which specifically requested confidentiality.

Consolidated summary from both engagements and submissions

Feedback received	How feedback was addressed	Justification
Submissions broadly supported uplifting the obligations. Several suggestions were provided regarding the implementation timeframe, including: - staged/progressive implementation - extended grace periods, and - exemption mechanisms.	The Department has considered feedback concerning implementation timeframes. To address feedback the Department has aligned grace period timeframes into two batches. In some instances, grace periods have been lengthened and in some, shortened. The Department has aligned compliance for all material risks proposed in the enhanced CIRMPs to 12 months. For all other measures, the Department has aligned grace period timeframes to 24 months. A 12-month grace period applies to enhanced material risks: ○ **Section 6A – Additional material risks**. The grace period for section 6A has had an extension of 6 months from what was proposed in the Exposure Draft. ○ **Subsection 8A(2) – Cyber and information security hazard material risks**. The grace periods for subsection 8A(2) have had a reduction of 6 months from what was proposed in the Exposure Draft. ○ **Subsection 9A(2) – Personnel hazard material risks**. The grace periods for subsection9A(2) have had a reduction of 6 months from what was proposed in the Exposure Draft A 24-month grace period applies to all other measures: ○ **Sections 8A, other than 8A(2) - Cyber and information security hazard – enhanced requirements.** The grace period have not changed since the Exposure Draft. ○ **Section 8B – Credential compromise hazard.** This measure was consulted on under Section 8A in the Exposure Draft; therefore the grace period has not changed.	The Department acknowledges the impact these proposed reforms have on critical infrastructure stakeholders, including the cost and for some measures, technical complexity of achieving the obligations. However, given the degradation of the national security environment, the proposed reforms are essential to ensure the ongoing availability, integrity, reliability and confidentiality of these high-risk critical infrastructure assets. In order to mitigate against the extant and emerging risks facing critical infrastructure, the maximum grace periods for these measures are 24 months. The alterations made to the Grace Periods acknowledge the impact these reforms will have on critical infrastructure stakeholders. For example, cost and – in some instances – the technical complexity of satisfying on obligation. To streamline expectations on affected stakeholders, the Department has refined the proposed grace periods. This has seen all material risks set to 12 months, and all other measures set to 24 measures.

Consolidated summary from both engagements and submissions

	○ **Section 8C – Lateral movement hazard**. This measure was consulted on under Section 8A in the Exposure Draft; therefore the grace period has not changed. ○ **Section 9A, other than 9A(2) – Personnel hazards – enhanced requirements.** The grace period has not changed since the Exposure Draft. ○ **Section 10A – Supply chain hazards – enhanced requirements**. The grace period has been extended by 6 months from what was proposed in the Exposure Draft) **Section 11A – Physical security hazards and natural security hazards**. The grace period for section 11A has had an extension of 6 months from what was proposed in the Exposure Draft	
Stakeholders expressed strong support to maintain principle-based approach of the CIRMP, ensuring obligations are risk-based, proportionate and grounded in the 'as far as is reasonably practicable' principle. Stakeholders consistently provided feedback that obligations should be aligned with what entities can reasonably control and influence.	The Rules have maintained a principle-based approach, with revisions from the Exposure Draft continuing to prioritise flexibility rather than prescriptive requirements. Where previously consulted, more prescriptive obligations have been retained, reflective of the risk environment we are operating in. Where obligations are prescriptive (for example, implementing phishing-resistant multi-factor authentication), the Rules have provisions for alternative compensating controls, including for additional measures following consultation of the Exposure Draft. This ensures entities can meet the intent of the requirements where prescriptive measures may not be suitable, such as technological limitations associated with legacy systems. This approach seeks to ensure the CIRMP Rules remain proportionate to the risk profile and operational context of each asset, while still delivering the level of security uplift required to safeguard critical infrastructure.	Stakeholders operate across a highly diverse range of sectors, asset types and operational environments, with varying levels of maturity, capability and system constraints. The Department acknowledges the benefits of the CIRMP Rules remaining principle-based, and the measures proposed are designed to reflect this. The Department's decision to apply these obligations to select high-risk asst classes re-confirms the commitment to ensuring any regulatory reform is risk-informed and proportionate; these proposed enhancements are directed toward high-risk sectors only. There are, however, some hazards which can be mitigated in a limited number of ways. For example, preventing lateral movement of an adversary from an IT environment to an OT environment (the method employed by Volt Typhoon) can only be mitigated through the practical segregation of those two environments. In the event that an entity cannot practically segregate these environments, the Rules require that they identify alternate risk mitigations.

Consolidated summary from both engagements and submissions

		This approach, which is replicated throughout the enhanced CIRMP, ensures the obligations are aligned with what entities can reasonably control and influence.
Submissions consistently requested additional guidance, practical examples and/or templates to support implementation of the requirements.	At the time of publishing this document, best-practice guidance is being developed. This guidance: ○ is being co-designed with experts (including partners across the Commonwealth, Standards Australia, and expert advisory groups in the Trusted Information Sharing Network) ○ will provide detailed, best practice guidance and clear expectations for continuing and enhanced CIRMP obligations ○ will include practical examples, definitions ○ is being consulted iteratively across the cross-sector channel of the Trusted Information Sharing Network; and ○ is expected to be released in August 2026.	Clear, detailed guidance supporting implementation of, and ongoing compliance with, obligations provided within these Rules. Accordingly, the goal is to align the release of the best practice guidance with the Rules taking effect. Industry is encouraged to participate in fora – such as the Trusted Information Sharing Network – to engage with other regulated entities. Doing so provides industry with opportunities to benefitting from, and add to, insights and approaches to identifying and mitigating risks.
Submissions raised concerns regarding costs (upfront and going) diverting finite capability from approved capital and programs, particularly with limited availability for specialist cyber skills. Many affected asset classes are subject to fixed budget and funding cycles. This limits access to additional funding required to implement security uplift measures. Multiple stakeholders called for engagement with pricing regulators.	Independent impact analysis was conducted, to ensure the Rules are proportionate and that related cost implications for specific assets are properly understood. This thorough analysis concluded that benefits of the Rules outweigh the associated regulatory costs for affected asset classes. The Department has engaged with pricing regulators throughout this reform process and will continue to do so to provide understanding of the enhanced CIRMP obligations and the threat landscape necessitating their introduction. The Department is intending to use best-practice guidance to provide clear expectations on what and how entities should implement the enhanced CIRMP Rules for their asset, but note the obligation remains principles based.	A thorough impact analysis was undertaken by an independent third party, ***1 and One.*** This analysis was used to test the proportionality of the measures and to better understand the financial and operational implications across affected sectors. This work provides assurance that the enhanced CIRMP Rules are calibrated to deliver a security uplift while remaining proportionate to the level of risk. In parallel, continued engagement with pricing regulators supports a shared understanding of the reforms and their implications, including how costs may be considered within existing regulatory and funding settings. The Department notes that the Commonwealth provides a range of support and advice to industry, particularly regarding cyber security uplift, through the Australian Cyber Security Centre.

Consolidated summary from both engagements and submissions

Submissions raised concerns about duplicating requirements with federal, state and sector specific legislation and regimes.	In developing these Rules, relevant Commonwealth, state, territory and sector-specific stakeholders have been engaged to minimise regulatory duplication wherever possible. The Government has accepted, in principle, the recommendations of the Independent Review of the Security of Critical Infrastructure Act 2018. This includes a recommendation to remove legislative duplication where possible.	Given the broad, nation-wide remit of the SOCI Act, there are some instances of legislative duplication. Work to identify and reduce duplication as well as improve regulatory harmonisation is ongoing. As it stands, the SOCI Act does not allow for carve-outs or exemptions for specific obligations.
Submissions emphasised the importance of maintaining an outcomes-focused, risk-based approach to multi-factor authentication (MFA) and critical systems network segregation, with flexibility in how security objectives are achieved. Submissions highlighted support for recognising alternative or compensating controls for MFA where needed, and for adopting a more principles-based approach to network segregation requirements.	To maintain an outcomes-focused approach, new hazard vectors for MFA and network segregation measures have been created: *Credential Compromise* and *Lateral Movement*. While these measures are now organised under distinct hazard vectors, there is no change to their substantive content as presented in the Exposure Draft. This refinement provides greater clarity on the risks the measures are designed to address, and to better articulate risk-based expectations for industry. This structure seeks to support a more coherent and transparent framework by aligning measures with the threat actor behaviours they aim to mitigate. The Enhanced CIRMP Rules explicitly recognise that, where there is a technical limitation which prevents MFA or network segregation (for example, due to legacy hardware), entities must – in their CIRMP – include the reasonable steps they've taken to minimise or eliminate the material risks associated with the relevant hazard.	An outcomes-focused, risk-based approach is essential for maintaining the intent of these Rules. This approach has been maintained whilst responding to the degrading security environment. Creating two new hazard vectors – Credential Compromise and Lateral Movement – demonstrates both the crucial role flexibility has in this regulatory setting and reflects the significance of the risks posed by said vectors. Real-world examples such as *Scattered Spider* and *Volt Typhoon* demonstrate the need for entities to mitigate such hazards. This strengthens the connection between the actions required of entities and the purpose of minimising or mitigating material risks to critical infrastructure assets. This approach improves the clarity, coherence and enforceability of the Rules, while preserving the original policy intent and maintaining flexibility for entities in how outcomes are achieved.
Submissions raised concerns about Government's capacity and readiness to facilitate increased background checks through the AusCheck program in a timely manner.	Following this feedback, the Explanatory Statement on the Enhanced CIRMP has been updated to explicitly address the policy intent where a circumstance arises that an AusCheck background check or relevant security clearance has not yet been obtained, due to processing times. This now provides that entities may assess suitability as an interim measure through 9A (3)(a)(ii) and (b).	Noting concerns regarding AusCheck processing times, the Home Affairs Annual Report 24-25, states that over 86% of AusCheck background checks for applicants with no disclosable court outcomes were completed within 20 days. For those with disclosable court outcomes, over 90% were completed within 40 business days.

Consolidated summary from both engagements and submissions

Submissions also called for all clearance levels with an element of intelligence checking (including NV2 and Positive Vetting) to be listed as an acceptable background check.	Additionally, the grace period for this measure has been extended from 18 to 24 months. This reflects the onboarding required for entities prior to commencing the use of AusCheck. The Trusted Information Sharing Network will be used to engage with entities on the AusCheck process and timeframes. The Department has amended the relevant provisions to expressly recognise that Australian Government issued security clearances with an intelligence check are accepted.	As such, AusCheck processing times are not expected to be a significant issue. The Explanatory Statement has been amended to provide comfort to industry.
Feedback raised concerns about supply chain and Foreign Ownership Control and Influence (FOCI) measures, particularly around the practical challenges including multi-tier supply chains, upstream ownership visibility and timelines for implementation.	The Department will clarify expectations on the scale of supply chain mapping and FOCI vendor assessments through best-practice guidance. This will include practical examples, templates and links to existing resources, such as Foreign Ownership, Control or Influence Risk Assessment Guidance to assist industry in applying proportionate and risk-based approaches. This guidance is being developed in consultation with relevant supply chain experts to ensure it is practical across different asset classes, including with the Office of Supply Chain Resilience and the Supply Chain Expert Advisory Group, as well as wider consultation with Trusted Information Sharing Network members. Additionally, the grace period for this measure has been extended from 18 to 24 months. This timeframe is intended to better support entities addressing the complexity of these requirements and achieve an appropriate level of risk mitigation in a timely manner.	These obligations may be burdensome to industry. However, recent global shocks, and a worsening geo-political environment, make it necessary for critical infrastructure entities to identify and mitigate the extant and emerging risks across their supply chain and FOCI vulnerabilities. Of note, obligations regarding supply chain mapping and vendors of concern are limited to major suppliers. Meaning those with a significant influence over the security of the asset. This is considered proportionate to the associated risks.
A small percentage of feedback called for the enhanced CIRMP Rules to address physical theft/sabotage, excavation/ground disturbance examples, and there were some suggestions to include counter-unmanned aircraft systems posture expectations for high-risk assets.	There have been no material changes to the enhanced CIRMP Rules as a result of this feedback. The CIRMP framework requires responsible entities to adopt a comprehensive, risk-based approach, including the identification and management of material risks beyond those expressly outlined in the Rules. It is neither practical nor desirable to prescribe all potential risks within the legislative framework, as doing so would limit flexibility and reduce the effectiveness of the regime in responding to an evolving threat environment.	It is likely there are material risks which are not addressed in the Rules – those mentioned in the Rules do not equate to an exhaustive list of material risks facing critical infrastructure assets. However, the CIRMP framework requires entities to identify and mitigate material risks – they do not need to be detailed in the CIRMP Rules to be addressed. With regards to the theft/sabotage, the Department has been working in partnership with the Australian Institute of Criminology on a research project regarding 'Crime Impacting Critical Infrastructure in Australia' and has

Consolidated summary from both engagements and submissions

	The Department will continue to raise awareness of relevant and emerging risks and threats through established channels, including the Trusted Information Sharing Network (TISN), TISN briefings, and guidance published on the Cyber and Infrastructure Security Centre (CISC) website.	been engaging extensively with stakeholders throughout. Once complete, the Department will review the recommendations, and consider reform, where appropriate. The Department recently publicly consulted on the Drone Security Public Consultation Paper 2026. This paper identified six potential areas of reforms to manage drone security outcomes.