Submission to the Department of Home Affairs' Consultation on Proposed Enhancements to the Critical Infrastructure Risk Management Program Rules

13 February 2026

Introduction and Executive Summary

Global Shield Australia welcomes the Department of Home Affairs' (the **Department**) proposed enhancements to the Critical Infrastructure Risk Management Program (**CIRMP**) rules[1] and the opportunity to provide a submission on the proposed changes.

Global Shield Australia is a non-profit policy advocacy organisation dedicated to reducing global catastrophic risk. We support governments to enact and effectively implement policies that prevent and prepare for all forms of risk, including in relation to critical infrastructure.

The Department's proposed enhanced CIRMP rules will help safeguard Australia's critical infrastructure against new and evolving sources of risk. Global Shield Australia is particularly supportive of the proposals to:

(a) **Require entities to map their supply chains and critical systems to identify critical vulnerabilities and minimise or eliminate related material risks**.[2] The proposed coverage of *physical and digital (or cyber)* supply chains, including AI supply chains, will be key to ensuring the effectiveness of this enhancement, along with clear guidance and support for industry on how this should be done.

(b) **Enable the Department to require entities to consider specified risk advice from government, identify whether there is a material risk for their asset, and minimise or eliminate that risk as far as reasonably practicable.**[3] This will help formalise the relevance and application of Australian Government determinations and directions, and ensure entities are integrating these into their risk management considerations.

(c) **Identify and introduce cyber and information hazard material risks into the CIRMP rules** to ensure entities integrate these into their consideration and planning.[4] This is an important recognition of the changing nature of the key material risks facing Australia's critical infrastructure entities.

[1] *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023.*
[2] Department of Home Affairs, *Consultation Paper: Proposed amendments to enhance the Critical Infrastructure Risk Management Program Rules (CIRMP Rules)* (December 2025) (**Consultation Paper**), 14.
[3] Ibid 6.
[4] Ibid 12-13.

We have also identified three areas where the proposed enhancements could be amended to ensure the enhanced CIRMP rules operate effectively, particularly in relation to AI risk. We recommend that:

1. **The enhanced CIRMP rules be applied to data storage or processing sector assets, at least where these host or are used to train advanced AI models.**
2. **The new cyber and information hazard specific material risks should include risks associated with hosting or training advanced AI models in Australian data centres, in addition to risks arising from AI deployment or use by other assets.**
3. **There is clear guidance and support for industry regarding mapping of digital supply chains, including AI supply chains, to support their compliance with the new supply chain mapping requirement.**

These recommendations would help ensure the CIRMP rules are future-proofed and remain fit for purpose in a period of increasing risk for Australia's critical infrastructure.

Contact: australia@globalshieldpolicy.org

Recommendations

A. Data storage and processing assets should be subject to the enhanced CIRMP rules

The Department has proposed that the enhanced CIRMP rules will only apply to a specific list of proposed sectors and asset classes,[5] this includes assets in the energy, communications, water and sewerage, and transport sectors. However, the Consultation Paper does not propose including data storage or processing assets within the scope of the enhanced rules.

As Global Shield Australia has argued elsewhere,[6] at present the *Security of Critical Infrastructure Act's* (**SOCI Act**) coverage of data storage and processing assets is inappropriately narrow and likely fails to capture key pieces of Australia's critical infrastructure. This risk will only increase given the government's focus on attracting investment in hyperscale data centres to train and host advanced AI models.

While the issue of SOCI Act coverage is outside the scope of this consultation, it is unclear why the enhanced CIRMP rules should not apply to data storage or processing assets given their centrality to Australia's economy and security, exposure to major threats and hazards (including those the enhanced CIRMP rules are designed to address), and the likelihood of their increasing importance to Australian society in the future.

To remedy this, **Global Shield Australia recommends that data storage and processing assets be subject to the proposed enhanced CIRMP rules,** at least where such assets are used for:

(a) Training general-purpose advanced AI models, whether Australian or foreign developed; or

(b) Hosting advanced AI models that are integrated into or servicing critical infrastructure assets.

Capturing these assets under the enhanced CIRMP rules would reflect their growing importance to Australia's economic and national security. By acting now, Australia will also be better positioned to address future risk and can avoid playing catch-up as AI becomes more integrated across our economy.

[5] *Consultation Paper*, 4.
[6] Global Shield Australia, *Submission to the Consultation on the Independent Review of the Security of Critical Infrastructure Act 2018* (December 2025) (**Global Shield Australia Submission**) 11.

B. The enhancements to the CIRMP material risks should include risks associated with the hosting or training of advanced AI models

Global Shield Australia supports the Department's proposal to "*identify and introduce cyber and information hazard specific material risks*" that entities will need to reflect in their CIRMPs.[7] As set out in the Consultation Paper, this will include a requirement to consider the potential impacts of deploying "*advanced and emerging technology*" and the use of that technology by "*malicious and state-sponsored actors*", which in particular includes AI technologies and vulnerabilities.[8]

This is consistent with Global Shield Australia's previous recommendation that the material risks in the CIRMP rules need associated guidance and clarification in relation to AI-specific risk.[9] This will help to ensure CIRMPs are future-proofed and that entities are guarding against modern threats.

However, the current focus in the Consultation Paper appears to be on impacts arising from the deployment and use of advanced and emerging technology.[10] As identified in our previous submission, to maximise the effectiveness of these enhancements, **they should also include impacts that could arise from the *training* and *hosting* of advanced AI models by data centre assets.**[11]

Hosting and training advanced AI models involves unique and specific risks, beyond traditional cyber and information hazard risks. This includes risks arising from their intensive power and cooling demands, use of sensitive training data, highly targeted and valuable model weights, and need for enhanced human oversight to avoid unintended or unpredictable output or actions by the AI model or system. These specific risk vectors should be clearly identified as part of the proposed enhancements to the CIRMP rules' material risks to ensure they are being addressed in CIRMPs of relevant data centre assets.

[7] *Consultation Paper*, 12.
[8] Ibid.
[9] Global Shield Australia Submission, 13.
[10] *Consultation Paper*, 12.
[11] Global Shield Australia Submission, 12-13.

C. Supply chain vulnerability mapping should include digital and AI supply chains

Global Shield Australia also supports the proposed requirement for entities to map their major supplier and critical system supply chains, including the application of this requirement across both physical *and* cyber supply chains.[12] Such mapping is crucial to ensuring entities understand their exposure to supply chain risk and thus are able to take steps to mitigate that risk.

In implementing this new requirement, **Global Shield Australia recommends the Department ensure there is clear guidance and support on mapping software and AI supply chains,** which present distinct challenges.

The supply chain complexities in AI tools and systems are less visible and more difficult to interrogate, including due to the:

1. Opacity of the inputs, data sources, and training used to develop an AI model, with ramifications for how the model operates and its potential failure modes.
2. Concentration of AI capabilities among a small number of foreign providers, limiting the potential to source alternatives and creating potential foreign ownership, control and influence (**FOCI**) risk depending on where the models are hosted or trained.[13]›
3. Multiple nodes in a typical AI supply chain, including training data providers, base model developers, hosting infrastructure operators, and application overlay designers.

The novel and rapidly advancing nature of these systems means that guidance and examples, including best practices and standards, will be key to uplifting industry in its assessment of these supply chains. This includes in relation to what can be reasonably expected from AI service providers and what controls are appropriate in response to varying levels and sources of risk.

Conclusion

The proposed enhancements to the CIRMP rules represent a key opportunity to strengthen the implementation of the SOCI Act and ensure Australia's critical infrastructure assets are prepared for an increasingly complex threat environment. Our recommendations aim at maximising the effectiveness of these changes and ensuring the SOCI Act regime is able to effectively realise its objectives. Global Shield Australia looks forward to continuing to engage with the Department on these important issues in the future.

Contact: australia@globalshieldpolicy.org

[12] *Consultation Paper*, 14.
[13] Noting this risk should also be considered as part of the FOCI elements of the enhanced CIRP Rules.