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

1 May 2026

Introduction and Executive Summary

Global Shield Australia welcomes the opportunity to provide a submission to the Department of Home Affairs' (the **Department**) Consultation on the Exposure Draft of the Critical Infrastructure Risk Management Program (**CIRMP**) Rules (**Exposure Draft**).

Global Shield Australia is a non-profit policy advocacy organisation dedicated to reducing global catastrophic risk. We take an all-hazards approach to risk reduction, supporting governments to enact and effectively implement policies that reduce and prepare for all forms of catastrophic risk.

The *Security of Critical Infrastructure Act 2018* (**SOCI Act**) regulatory framework is a key tool for ensuring Australia is protected against a range of catastrophic threats and has the powers necessary to respond in a catastrophic crisis. Its risk management obligations, in particular, are an important method for safeguarding Australia's safety and security in an increasingly volatile threat environment.

The Exposure Draft presents a necessary uplift in standards for critical infrastructure (**CI**) assets, and we support the Department's continued principles-based approach to regulation. We are particularly supportive of the proposed new Section 6A, which would require responsible entities for specified CI assets to consider impairments that "*could prejudice the social stability, economic stability, national security or defence of Australia*" as a material risk for the purpose of their CIRMP. This recognises the foundational role these assets play in Australia's overall security.

Our submission makes two recommendations to strengthen the Exposure Draft:

> **Recommendation 1** identifies a potential drafting issue in the proposed Section 8A(2)(d) that may be read as framing deployment of new technology as a risk to be minimised, rather than addressing risks associated with such deployment. We propose an amendment that preserves the policy intent while correcting this inconsistency, along with a clarificatory amendment to expand Section 8A(2)(d) to cover the *hosting* of such technology in addition to just deployment.
>
> **Recommendation 2** proposes an additional Note to Section 10A(3) to clarify that the new supply chain mapping obligation encompasses risks of compromise through the supply chain, not only risks of outage.

We also take this opportunity to again emphasise that the growing integration of artificial intelligence (**AI**) systems across CI assets, and AI itself becoming CI, means that the scope of the SOCI Act and the enhanced CIRMP Rules should be reconsidered to ensure that the SOCI Act framework is addressing key threats to Australia.

Recommendations

Recommendation 1 — Clarify the drafting of cyber and information security hazards material risk

Global Shield Australia supports the requirement in the proposed new Section 8A(2)(d) and (e) that relevant CI entities must account for risks associated with the "*deployment of advanced, novel and emerging technologies*" and the "*use of advanced, novel and emerging technology against the asset, in a manner that could prejudice the social stability, economic stability, national security or defence of Australia*".

However, we note that the drafting of sub-paragraph (d) is not consistent with the other sub-paragraphs, which identify negative outcomes or unacceptable practices that must be "*minimise*[d] *or eliminate*[d]".

While the deployment or hosting of advanced technologies (such as frontier AI systems) will involve substantial material risks (as we identified in our prior submissions), it will also be necessary to defend against modern threats and hazards. Indeed, sub-paragraph (c) of the new Section 8A(2) highlights the need for entities to replace legacy systems. This will often involve deploying advanced, novel or emerging technologies.

We also note that, particularly if the enhanced CIRMP Rules ultimately cover data centres (as per our comments below), it will be important to ensure that relevant entities also consider the material risks associated with *hosting* advanced, novel, or emerging technologies, not just their deployment.

Thus, to ensure that the proposed Section 8A(2)(d) is clear and effective, we propose the following amendments drawing on the language in Section 8A(2)(e):

> **Proposed amendment to s8A(2)(d) — amend:**
>
> *(d) the development, deployment or hosting of advanced, novel or emerging technology, in a manner that could prejudice the social stability, economic stability, national security or defence of Australia;*

These amendments preserve the core policy intent of the proposed change, while ensuring the drafting clearly targets the potential harm rather than modernisation itself.

The guidance to be released in association with the enhanced CIRMP Rules should also explicitly set out the AI-related risks within the scope of Section 8A(2)(d) and (e) and best practice for addressing them. This includes risks from a lack of human oversight, poisoned or compromised training data, and unpredictable or uncontrolled systems.

Recommendation 2 — Clarifying the extent of supply chain mapping obligation

Global Shield Australia is supportive of the proposed new requirement for entities to undertake supply chain mapping of their physical and cyber risks in Section 10A(2)-(3).

We note that in addition to potential outages caused by supply chain vulnerabilities, a significant supply chain risk for CI assets is the potential compromise of CI systems or data. Supply chains are an established access point for adversaries to critical infrastructure — as demonstrated by incidents such as the Volt Typhoon campaign referenced in the Exposure Draft. While this risk is likely covered by Section 10(A), it may not be clear to regulated entities, particularly given the focus on outages in sub-paragraph (b) and the current Note's focus on diversification, redundancy planning, recovery, resilience and restoration processes.

Thus, we recommend that an additional Note be included in this Section to clarify this intent:

> **Proposed amendment to s10A(3) — insert:**
>
> *Note: Vulnerabilities and risks for the purpose of paragraph (3)(a) may include, but are not limited to, risks of compromise to or within a supplier that could lead to unauthorised access to, degradation of, or interference with a CI asset's system or data.*

Additional Consideration — Data centres and AI systems

Data storage and processing assets are excluded from the proposed enhanced CIRMP Rules in the Exposure Draft. While Global Shield Australia recognises that expansion of the enhanced CIRMP Rules to other asset classes is not being considered in these reforms, we continue to urge the Department to review how the SOCI Act and the enhanced CIRMP Rules could apply to AI models and data centres in the future.

As the Exposure Draft notes, many submissions recommended the inclusion of additional asset classes under the enhanced CIRMP Rules. The Independent Review of the SOCI Act also identified the need for the Department to consider "*the impact of AI, quantum, physical threat vectors and the role of Operational Technology (OT) Cybersecurity as they relate to the SOCI Act*".

As argued by Global Shield Australia in our submissions to the Independent Review of the SOCI Act and the Consultation on enhancements to the CIRMP Rules, the inclusion of AI and data centre assets is essential for Australia's ongoing security, particularly as AI becomes more integrated across CI assets, and as AI and data centres hosting AI become increasingly central to basic societal functioning. This would also be consistent with Expectation 1 of the Government's Expectations of Data Centres and AI Infrastructure Developers, which states that data centre operators "*should protect sensitive and personal data, prepare for threats and disruptions, and limit physical and digital access to their data centres to those with a right to it.*"

As such, we encourage the Department to consider ensuring that the enhanced CIRMP Rules cover data storage and processing assets to the maximum extent possible under the current legislative framework. One way to prepare the enhanced CIRMP Rules to address this is by amending the proposed Section 4A(1) as follows:

> **Proposed amendment to s4A(1) — insert:**
>
> *(j) a critical data storage or processing asset.*

Global Shield Australia also recognises that many data centres may already be covered by the Hosting Certification Framework (**HCF**) and thus may be exempted from the requirement to maintain a CIRMP under the SOCI Act. For such assets, it will be important to ensure that the HCF matches and exceeds the requirements of the enhanced CIRMP Rules.

Conclusion

Global Shield Australia supports the Exposure Draft and the Department's continued work to uplift the security of Australia's critical infrastructure in a complex and diverse threat environment. We look forward to continuing to work with the Department as these risks evolve to ensure Australia's regulatory response keeps pace.

Contact: australia@globalshieldpolicy.org