



Submission to the Department of Home Affairs' Consultation on Proposed Amendments to the Ministerial Directions Powers in Part 3 of the *Security of Critical Infrastructure Act 2018*

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 Proposed Amendments to the Ministerial Directions Powers in Part 3 of the *Security of Critical Infrastructure Act 2018* (**SOCI Act**).

[Global Shield Australia](#) is an independent, non-profit policy advocacy organisation dedicated to reducing global catastrophic risk. We take an all-hazards approach to risk reduction, supporting governments to effectively implement policies that prevent and prepare for all forms of catastrophic risk. Global Shield Australia has actively engaged in the implementation and reviews of the SOCI Act framework, including as a member of the Department's Resilience Expert Advisory Group, through the recent Independent Review of the SOCI Act, and recent consultations on the Critical Infrastructure Risk Management Program (**CIRMP**) Rules.

The powers set out in Parts 3 and 3A of the SOCI Act will be central to Australia effectively preparing for and responding to a range of catastrophic crises. As such, Global Shield Australia has previously argued for improvements to the Ministerial Directions Powers so that they can be relied on in a crisis. Our past recommendations include: minimising procedural and legal complexity, providing clear guidance to industry, and undertaking regular testing of the use of these powers against credible risk scenarios.

Global Shield Australia is strongly supportive of the proposed amendments to the Ministerial Directions Powers in Part 3 of the SOCI Act. These will ensure the powers remain fit for purpose in an evolving and more volatile threat environment, and that they can be effectively utilised when needed. Our submission covers proposed Measures 1 and 3 in the Consultation Paper.

Contact: australia@globalshieldpolicy.org

Comments on proposed measures

Measure 1 – Amendments to the existing directions power in section 32

Global Shield Australia strongly supports the proposed amendments to the directions powers in section 32 of the SOCI Act. The Part 3 directions powers could play a powerful role in Australia's preparation for catastrophic and cascading crises. The utility of these powers depends upon their ability to be exercised quickly, effectively and with legal clarity. The proposed approach to Measure 1 is a meaningful step towards this objective.

We support the replacement of the current adverse security assessment (**ASA**) requirement with one to obtain tailored Australian Security Intelligence Organisation (**ASIO**) advice, and also the recalibration of the regulatory exhaustion requirement. These changes will materially reduce the risk that these directions cannot be effectively exercised when needed, and avoid unnecessary legal and procedural challenges in their use.

Further enhancements to Measure 1

While supportive of the current proposed changes in Measure 1, Global Shield Australia notes two additional areas where further improvements are possible.

Aligning the scope of Part 3 with the scope of Part 3A

First, section 32's scope is limited to situations where the Minister is satisfied that there is a risk to "security" as defined in the *Australian Security Intelligence Organisation Act 1979 (ASIO Act)*.¹

This covers specific threats to Australia, namely espionage, sabotage, politically-motivated violence, promotion of communal violence, attacks on Australia's defence system, acts of foreign interference, and threats to our territorial or border integrity.²

This narrow scope reflects the original language of section 32 when it was first enacted. It is out of step with the modern threat environment and subsequent reforms to the SOCI Act. For example, the SOCI Act's Part 3A powers apply where there is a material risk that an incident has or is likely to seriously prejudice "*the social or economic stability of Australia or its people*", "*the defence of Australia*" or "*Australia's national security*".

While recognising that the Part 3A powers are designed for use in more immediate and potentially extreme scenarios than section 32, the current gap in scope means that significant threats fall outside of the scope of the section 32 direction powers, such as:

- Criminal cyber attacks for financial gain;

¹ SOCI Act, s 32(1).

² *Australian Security Intelligence Organisation Act 1979*, s 4.



- Cascading and systemic failures from non-hostile events (such as the 2024 CrowdStrike incident or space weather incidents);
- Supply chain vulnerabilities or fragilities that are not appropriately mitigated;
- Non-hostile shocks to the food and grocery sector, including biosecurity challenges or climatic impacts; and
- Novel systemic risks from emerging technologies, including AI systems.

Extending the scope of any coercive power over private entities requires careful consideration. However, given the length of time since the enactment of section 32 and subsequent legislative changes, now is an appropriate time to ensure the section's scope remains fit-for-purpose and consistent with the current SOCI Act framework.

We recognise that ASIO's tailored advice under section 32(3)(c) may not be able to directly address threats outside the ASIO Act's definition of security. However, the proposed shift away from adverse security assessment provides the flexibility needed to manage this. Where the Minister is considering issuing section 32 directions in circumstances outside of ASIO's direct remit, ASIO's advice on potential national security implications would still be informative even if it is not determinative. Over time, it may also be worth revisiting the procedural architecture around inputs into this decision to ensure the Minister is supported by the most relevant advice across the full range of threats the directions power could be used to address.

As such, we recommend the Department consider harmonising section 32 and Part 3A by amending section 32(1) to align with section 35AB(1)(c).

Providing clear guidance for industry and regularly testing these powers **Second, while the proposed changes in Measure 1 will reduce friction to using the powers set out in section 32, their ability to address the “time-sensitive threats” referred to in the Consultation Paper will depend on advanced preparation by government and industry. As such, we recommend the Department complement Measure 1 with published guidance and regular testing of these powers.**

The Department should publish clear guidance to industry on how and when the Part 3 powers may be used. This includes sanitised scenarios, decision criteria, and indicative timeframes for action. This would support entities to comply with Part 3 directions, reducing the potential for surprise or contestation at critical decision points. This would also reassure industry that these powers will be exercised responsibly, and help to reduce costs at the time they are used by ensuring there has been sufficient warning and preparation.

Guidance would also support the Minister to meet the preconditions found in section 32(3)(a) and (b). Under section 32(3)(a) the Minister must be satisfied that a direction is “reasonably necessary” for addressing the identified risk. Clear guidance on how a Part 3 direction interacts with entities' existing obligations under other regulatory frameworks would assist with this assessment by



ensuring that less intrusive alternatives have been considered. Under section 32(3)(b) the Minister must be satisfied that “reasonable steps have been taken to negotiate in good faith” with the relevant entity. This requirement, in particular, would benefit from operational clarity. Guidance on matters such as information sharing arrangements, the treatment of costs incurred, regulatory overlap, and potential engagement timeframes would help ensure industry is ready to negotiate if and when it is needed. Guidance of this kind would not constrain the Minister’s discretion to make use of the section 32 powers; instead, it would ensure industry is ready when the power is exercised.

This guidance should also be accompanied by a regular program of exercises testing the end-to-end use of Part 3 powers against credible scenarios, particularly those requiring urgent action. These exercises should involve relevant government agencies, industry representatives, and civil society where appropriate. Their findings should also inform iterative refinement of the published guidance and ultimately the SOCI Act regulatory framework itself.

Measure 3 – Restrictions on the use of high-risk vendors, products or services

Global Shield is strongly supportive of the proposed new power to enable restrictions on the use of high-risk vendors, products or services. This power is particularly important to formalise existing voluntary advice and guidance to the CI industry around these issues. The ability to issue class-wide directions is key to avoiding duplicative, inconsistent and cumbersome interventions that need to be applied across assets and sectors.

Further enhancements to Measure 3

While Global Shield Australia supports the substance of Measure 3, we urge the Department to ensure that, in drafting this new power and supporting material, the concept of “*high-risk vendor product or service*” is not unduly narrowed.

Measure 3 in the Consultation Paper discusses high-risk vendors with a particular focus on foreign ownership, control or influence (FOCI) risks. While the proposal itself refers more broadly to vendors, products, services or technology that “*poses a material risk that is prejudicial to national security*”, it is critical that this is not drafted narrowly to only focus on FOCI risk or to a narrow definition of national security.

While FOCI-related risks are a key threat to Australia’s critical infrastructure, a product or service can pose a material (and indeed potentially catastrophic) risk to Australia for reasons unrelated to FOCI. Systemic vulnerabilities within a product could arise from its design, testing or internal safeguards. This concern is particularly relevant to advanced AI systems, which are becoming an increasingly important part of Australia’s critical infrastructure sector. An AI system may present a material risk that requires addressing, not because of its country of origin, but due to a range of reasons, including:



- Inadequate training data quality, integrity or provenance processes;
- Insufficient pre-deployment evaluation or testing;
- Vulnerability to prompt injection, jailbreaks or similar exploits;
- Inadequate safeguards in high-risk or high-consequence situations, including in relation to following user instructions; and
- Opacity in model behaviour and decision-making.

As such, Global Shield Australia recommends that the drafting of the Measure 3 power, and any supporting explanatory material, expressly contemplate that a vendor, product or service may be deemed restricted wherever it poses a material risk to Australia's stability, defence or national security. This could make use of a similar test to that used in section 35AB(1)(c) of the SOCI Act (as discussed above).

Conclusion

Global Shield Australia strongly supports the proposed amendments to the Ministerial Directions Powers. They are a key opportunity to ensure the SOCI Act framework remains fit for purpose in a complex and rapidly evolving threat environment. We look forward to continuing to work with the Department to ensure the SOCI Act powers are not only legally available but operationally ready when Australia needs them.

Contact: australia@globalshieldpolicy.org