SUBMISSION TO THE CONSULTATION ON THE

Independent Review of the Security of Critical Infrastructure Act 2018

Prepared for the Department of Home Affairs

20 December 2025

globalshieldpolicy.org

Introduction

Global Shield Australia welcomes the opportunity to provide a submission to the Department of Home Affairs' (the **Department**) Consultation on the Independent Review 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 preparedness, supporting governments to enact and effectively implement policies that prevent and prepare for all forms of risk.

This submission focuses on the fourth question raised by the Independent Reviewer, namely "*are there new or emergent threats the SOCI Act is unable to manage in its current form*?". Our review has identified four key areas in which the SOCI Act regime needs to adapt to keep pace with modern threats and hazards.

First, **the effective implementation of the SOCI Act requires a national and systemic assessment of critical infrastructure risk**. As such, a new statutory requirement to prepare and publish a regular National Critical Infrastructure Risk Assessment should be added to the SOCI Act. The Assessment should focus on systemic, catastrophic and cascading threats and hazards to Australia's critical infrastructure.

Second, **the SOCI Act's most serious powers and authorities (the so-called 'last resort' powers) are untested and need to be made operationally ready.** This requires investment in comprehensive planning around when and how these powers would be used, communicating this planning to industry, and undertaking regular testing of the powers through exercises with industry and across government.

Third, **the SOCI Act regime needs to be modernised for the AI-era.** Data centres hosting AI models need to be effectively covered by SOCI, risk management program requirements need to be clarified or updated to capture AI hazards as material risks, and a pathway to covering AI models once they become critical infrastructure in their own right is needed.

Fourth, the **Systems of National Significance (SoNS) regime must evolve to an all-hazards footing in line with the 2024 reforms to the SOCI Act.** Enhanced resilience obligations for SoNS should be added to the Act in addition to the existing enhanced cyber security obligations.

Given the expanded scope of the SOCI Act and Critical Infrastructure Security Centre's (**CISC**) growing responsibilities, including its shift in regulatory posture towards compliance activities, adequately supporting industry to meet its obligations will also require a corresponding increase in CISC's budget and resourcing.

These recommendations are intended to preserve the SOCI Act's core strengths while ensuring it remains fit for purpose as Australia's critical infrastructure becomes more interconnected, integrated with AI systems, and the risk environment deteriorates.

We would welcome the opportunity to further brief the Independent Reviewer or Department on these matters in more detail.

Contact: australia@globalshieldpolicy.org

Table of Contents

A. Context

The Independent Review of the SOCI Act comes at a time of increasing risk, volatility, and disruption, with credible indicators showing that global catastrophic risk is increasing.[1] Catastrophic risk is the risk of events or incidents occurring that would significantly harm Australia's security, economy or society in a manner that is beyond our existing response capabilities. Under the Australian Government Crisis Management Framework, these are termed "*extreme or catastrophic crises*" and require the highest levels of Commonwealth coordination to respond to.[2]

Specific sources of catastrophic risk include nuclear conflict, severe climate change, pandemics, cyberattacks, and AI misuse or malfunctions. Australia is particularly exposed to these hazards given our reliance on international supply chains, contested strategic environment, and increasing dependence on foreign-run or foreign-regulated AI systems. A catastrophic incident arising from any of these sources has the potential to disable or degrade multiple critical infrastructure sectors and services simultaneously and result in cascading failures.

The Independent Review is an important opportunity to ensure that the SOCI Act and its implementation are reducing Australia's exposure to catastrophic risk and increasing the resilience of our critical infrastructure to all forms of hazards.

B. Creating a National View of Critical Infrastructure Risk

The SOCI Act places substantial obligations on critical infrastructure owners and operators to assess and manage risk to their individual assets. These obligations, and the information the government receives as a result, should provide a solid foundation for ensuring national-level, systemic risk is identified, assessed, and addressed. However, there is no direct requirement on the Commonwealth to be acting to ensure that Australia has true, system-wide risk management in place and communicated publicly.[3]

While each individual asset owner might have plans in place to deal with specific hazards to their asset, it is only the Commonwealth that is able to manage the potential for *concurrent* or *cascading* disruptions across assets and sectors. Similarly, only the Commonwealth can evaluate the overall risk exposure of Australia's critical infrastructure, prioritise key threats and hazards, and communicate this back to industry.

In the absence of the government undertaking such work:

---

[1] RAND, *Understanding and Managing Global Catastrophic Risk* (2024); and Global Challenges Foundations, *Global Catastrophic Risk Report 2026* (2025).
[2] Department of Prime Minister and Cabinet, *Australian Government Crisis Management Framework* (September 2025).
[3] Australian Payments Network, *Submission to Consultation on Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy* (5 September 2025) 3-4.

(a) Critical infrastructure owners and operators have a limited view of the government's assessment of national or system-level risk and how hazards should be prioritised;

(b) Investment in addressing risk is vulnerable to shifting or unclear priorities, and may not be targeted at the most pressing sources of risk; and

(c) Cross-sector vulnerabilities and dependencies lack systemic mapping or assessment.

At present, the CISC's Annual Risk Review usefully communicates the Government's general view of the threat and hazard environment facing critical infrastructure, including some ranking of sources of risk by plausibility and damage. However, there is no statutory requirement for a regular, forward-looking assessment of risk to Australia's critical infrastructure to guide individual Critical Infrastructure Risk Management Programs (**CIRMPs**).

As specialised cybersecurity consultancy TrustedImpact has noted in previous consultations:

> *Senior Government leaders should have direct access to a consolidated 'cyber risk register' that provides factual insight into the common and most critical issues faced by Commonwealth organisation on an aggregated level so that they can be mitigated much better than what exists today.*
>
> *… if there was a mechanism to identify the MOST IMPORTANT [sic] risks faced by the Commonwealth on an aggregated basis, then one could build a working model that appropriately focuses on the major risks facing our Government today (for one application of the 'model'). This is one more reason why we believe the suggestion to develop a 'federal-level' composite cyber risk management framework would be of considerable value.*[4]

While this comment focuses on cyber risk, the same principle holds true for all threats and hazards that put Australia's critical infrastructure at risk.

Approaches in other jurisdictions

Other jurisdictions have also gone further in articulating a national view of risk. The United Kingdom's National Risk Register[5] is a public facing version of the government's internal National Security Risk Assessment. It includes 89 risks across 9 risk themes, assessing their likelihood and impact across a range of scenarios, including reasonable worst-case scenarios. The assessments are specific and able to be compared across risks (see Figure 1). This allows for analysis and prioritisation of responses and mitigations.

[4] TrustedImpact, *Policy Discussion Paper - Input for Consideration* (August 2025) 4, 5.
[5] UK Government, *National Risk Register 2025* (January 2025).

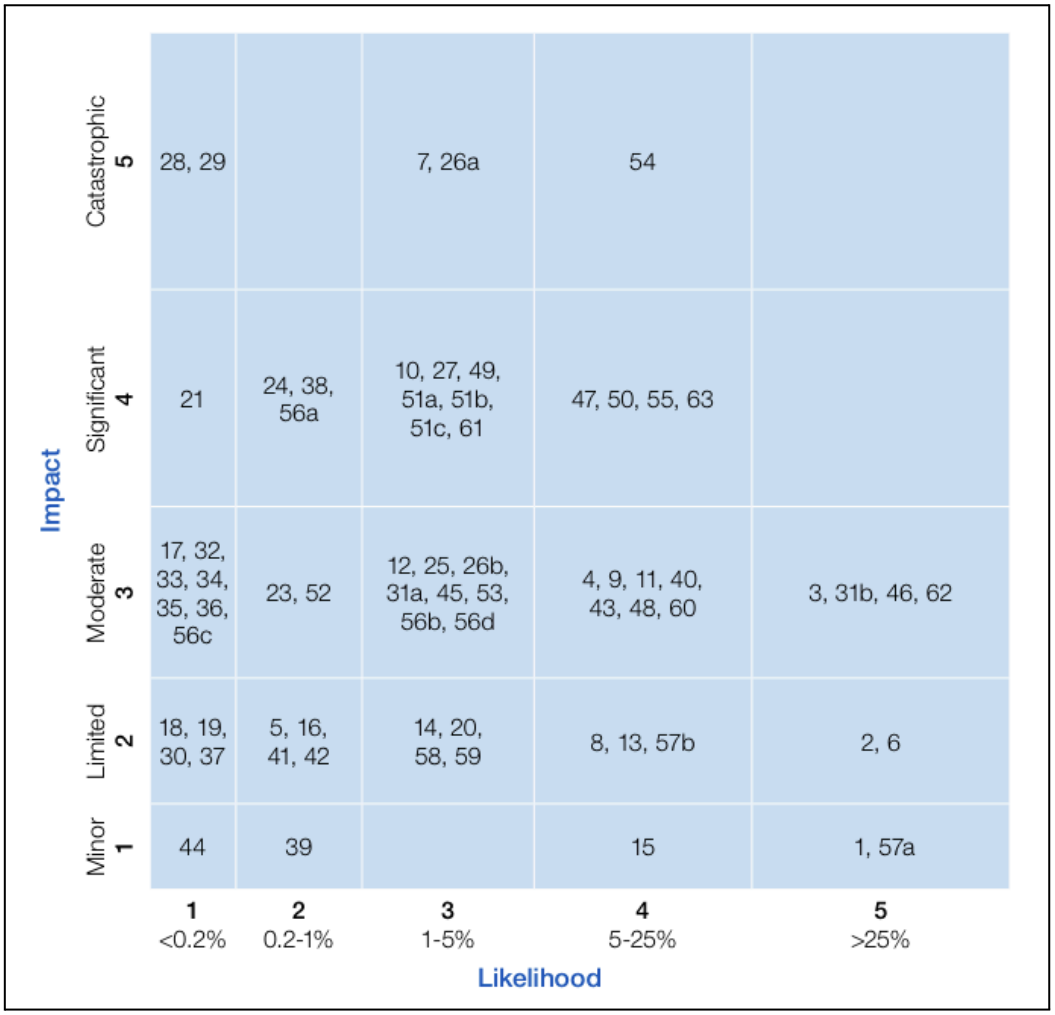

Figure 1. Risk assessment matrix from the United Kingdom's National Risk Register. Each number refers to a specific risk (e.g. 1 is an international terrorist attack with strategic implications, 54 is a pandemic, and 44 is an earthquake).

In the United States, the 2022 *Global Catastrophic Risk Management Act* mandated an assessment of global catastrophic and existential risk over the next 30 years and updating of Federal Interagency Operational Plans to "*ensure the health, safety, and general welfare of the civilian population affected by catastrophic incidents*".[6]

An Australian National Critical Infrastructure Risk Assessment

Learning from these other jurisdictions and the issues identified above, **Australia should build upon the CISC's Annual Risk Review to deliver a comprehensive, systemic, and structured assessment of Australia's critical infrastructure risk**. Such an assessment should:

[6] See Title 6, Sections 821-825 of the US Code, at 6 USC CHAPTER 2, SUBCHAPTER II, Part F: Global Catastrophic Risk Management. See also RAND, *Understanding and Managing Global Catastrophic Risk*, (2024).

(a) Focus specifically on systemic, catastrophic and cascading disruptions, which the Commonwealth is uniquely placed to assess;

(b) Integrate data from CIRMPs, intelligence sources, cross-government analysis and experts; and

(c) Be produced in both classified and unclassified versions, with the latter communicated to the private sector and broader public.

This would bolster Australia's national preparedness and resilience, provide a clear signal to boards and critical infrastructure owners and operators, and help ensure that individual CIRMPs are focused on the most pressing threats and hazards.

While a National Critical Infrastructure Risk Assessment (**NCIRA**) could be delivered as part of the Department's existing functions, elevating it to a statutory footing would provide additional guarantees around its performance, visibility, and contents. It would also enable current CIRMP obligations to incorporate reference to the NCIRA as a mandatory reference point for critical infrastructure owners and operators. Creating such a statutory obligation could be achieved through amendments to Part 7, Division 4 (Periodic reports, reviews and rules, etc) of the SOCI Act) as set out in **Annex A**.

Summary of Recommendations

1. **Establish a statutory National Critical Infrastructure Risk Assessment.** Amend the SOCI Act to require the Secretary of Home Affairs to prepare, at least every three years, a National Critical Infrastructure Risk Assessment that focuses on systemic, catastrophic and cascading threats and hazards to Australia's critical infrastructure. The assessment should be prepared in both classified and unclassified versions.

C. Operationalising SOCI's Last Resort Powers

As Global Shield Australia has previously highlighted:

> … *reforms to the SOCI Act provide[d] the Government with important authorities to prepare for and respond to a national crisis or catastrophic incident…. The last resort powers, in particular, are powerful and necessary tools for enhancing the preparedness and resilience of Australia's critical infrastructure. However, more can be done to increase understanding and certainty in relation to when, why, and how the government might decide to use these powers.*[7]

The 'last resort' powers in Part 3A of the SOCI Act empower the Minister for Home Affairs to respond to serious critical infrastructure incidents. This includes by gathering information from entities, directing action by entities, and authorising the Australian Signals Directorate to intervene. The 2024 SOCI Act reforms expanded some of these powers to cover all-hazards incidents, rather than just cyber security incidents.

These powers are significant governmental authorities, intentionally designed for use only in the most serious scenarios. They will be rarely exercised, with the hope being that less invasive provisions of the SOCI Act regime will mean it is not necessary for Part 3A to be explicitly relied upon. However, in a truly catastrophic scenario, which seriously prejudices Australia's social or economic stability, national security or defence, the government must be ready to make use of these powers and industry must similarly be prepared.

As such, there is a need to ensure the government is operationally ready to exercise these powers when required and that industry has clarity on when and how these powers would be used (and their role and rights in such circumstances).

The need for operational readiness

A lack of operational readiness poses a significant risk to the SOCI Act last resort powers being able to be an effective tool in a crisis.

(a) **Any crisis that necessitates the use of the last resort powers will happen at speed and require rapid decision-making and coordination.** A pre-established operational framework and plan is key to ensuring valuable time is not lost to deliberating over procedures and legal disputes.

(b) **The last resort powers overlap or intersect with a broad range of other Commonwealth and State and Territory powers.** During a crisis, there will also be multiple other regulators and authorities all seeking to act simultaneously (for example, financial regulators, health regulators, and telecommunications regulators, as well as agencies specific to the threat, such as biosecurity agencies or emergency management

[7] Global Shield Australia, *Submission to the Department of Home Affairs' Consultation on Horizon 2 of the 2023-2030 Australian Cyber Security Strategy* (29 August 2025) 4.

agencies). Without clear operational protocols, the risk of confusion, duplication, or conflict is substantial.

The recent expansion of Part 3A to cover all-hazards, which Global Shield Australia is strongly supportive of, also makes the above considerations more acute. The broader scope of Part 3A means the range of potential scenarios that might require these powers to be triggered is far greater. They include threats such as natural disasters, supply chain disruptions, and physical attacks. These each involve different factors and considerations that need to be accounted for, ways in which the powers could be used, and stakeholders who would need to understand their application.

Furthermore, without regular testing of the last resort powers in realistic scenarios, the government will not be able to identify gaps or unintended consequences that need to be remedied.

Industry needs clarity

Previous consultations by the Department, including when these powers were introduced, have also revealed concern regarding if, when, and how the government plans to use the last resort powers and the need for clear guidance:

(a) The Active Cyber Defence Alliance has noted the need for the government to "*articulate* [how these powers]...*will operate in a practical sense*" and that they need "*to be accompanied with policy guidance on the rights and responsibility of private sector actors*";[8]

(b) Exabeam has suggested that while the powers themselves are well understood "*the precise thresholds that would trigger government intervention are less clear to industry, which can create uncertainty*";[9]

(c) The Australian Banking Association has indicated the need for "[c]*lear guidance on how Government will engage with industry in the event of a crisis scenario, including sequencing of Government engagement, the identity of the key engagement points, and identification of expected benefits and outcomes.*" The Association has also called for "[c]*ontinued cross-industry exercises to build and refine understanding of how this guidance will operate in practice*";[10]

(d) The Water Services Association of Australia has said that "*additional clarification is required to identify the appropriate triggers for such action, the parameters under which such power may be exercised, the role of the entity during this period, and the implications for all parties arising from such an event*";[11] and

[8] Active Cyber Defence Alliance, *2023-2030 Cyber Security Strategy Horizon 2 Consultation* (26 August 2025) 12-13.
[9] Exabeam, *Submission to Consultation on Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy* (29 August 2025) 51.
[10] Australian Banking Association, *Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy* (29 August 2025) 3-4.
[11] Water Services Association of Australia, *Protecting Critical Infrastructure and Systems of National Significance – Consultation Paper, August 2020* (16 September 2020) 32.

(e) The Cyber Security Cooperative Research Centre submitted that "*greater clarity is needed regarding the proposed Government Assistance regime. These powers, what they mean, how they will be used and by whom needs to be clearly articulated. This will involve close consultation with industry and other stakeholders to ensure the regime is both clearly understood and proportionate*".[12]

Use of the last resort powers will necessarily mean deep engagement with industry and specific entities. If those engaged do not understand their obligations, rights and protections, this will slow their response or create unnecessary barriers to compliance that would hinder the effective use of these powers. While there will naturally be security sensitivities to protect, these should not entirely prevent appropriate engagement with industry (including security cleared staff members and through the Trust Information Sharing Network).

Closing the operational readiness gap

The following three actions would help to address the gap between legislative authority and operational readiness. All of these are actionable by the Department and Government and would not require new legislation or amendment to the existing regulatory regime.

First, **the Department should prepare and distribute an up-to-date and all-hazards operational framework for when and how the SOCI Act's last resort powers would be used**. This should include:

(a) Guidance on the circumstances and threat indicators that would lead to the Government considering using last resort powers;

(b) Clear procedures for how decisions would be made and by whom, including consideration of legislated consultation requirements and timeframes;

(c) Defined coordination mechanisms for engaging with relevant other agencies and governments;

(d) Articulation of the interaction of the last resort powers with sector-specific regulatory frameworks and authorities, prepared in consultation with other agencies to address overlaps and conflicts in advance;

(e) Clear statements of the legal rights and protections for entities subject to the last resort powers, including in relation to compensation and the limitations on use of information gained by government; and

(f) Procedures for when and how the use of the powers would be terminated and transitioned back to normal operations, including any remediation that may be required with the entities concerned.

This work should involve classified and public versions of the framework and be informed by deep consultation with industry.

[12] Cyber Security Cooperative Research Centre, *Submission: Security Legislation Amendment (Critical Infrastructure) Bill 2020 – Exposure Draft and Explanatory Document* (27 November 2020) 10.

Second, **the Department should establish a regular program of tabletop exercises and scenario testing involving both government agencies and critical infrastructure entities.** These must explicitly test the ability of the Commonwealth to activate and use the last resort powers across a range of sectors and crisis events (including catastrophic, compounding and cascading crises). They should involve relevant Commonwealth agencies, State and Territory governments, and private sector stakeholders. The outcomes from this work should be used to refine the operational framework, clarify roles, and identify changes needed to the underlying SOCI Act regime.

Third, **industry must be engaged on how the last resort powers would be used and contribute to the operational framework around their use**. Unclassified guidance should be published for critical infrastructure owners and operators setting out the relevant elements of the last powers operational framework, providing examples of when and how these might be triggered, and setting expectations on entities before, during and after an intervention. Classified guidance can also be provided through appropriate channels. This should also include clear information on the rights, responsibilities and protections of industry when the last resort powers are used.

Summary of Recommendations

2. **Prepare an operational framework for utilising the SOCI Act's last resort powers.** The Department should develop a comprehensive operational framework for the last resort powers. This framework should be developed in consultation with industry and be produced in both classified and unclassified versions.

3. **Undertake regular exercises and scenario testing of the last resort powers,** including using catastrophic, compounding, and cascading crisis scenarios. Outcomes should be used to refine the operational framework and identify necessary amendments to the SOCI Act regime.

4. **Engage with industry on how the last resort powers would be used in a crisis.** The Department should publish guidance for critical infrastructure owners and operators setting out key elements of the operational framework. Industry should be involved in co-designing the Department's planning and guidance through consultation processes and ongoing dialogue.

D. Modernising the SOCI Regime for the AI-era

As recognised by the Minister for Industry and Innovation in Australia's National AI Plan, AI is "*reshaping the global economy and transforming how Australians work, learn and connect with one another*".[13] The same Plan also articulates the Government's objective to "*support Australia to build an AI-enabled economy that is more competitive, productive and resilient*". Achieving this objective will mean a far greater reliance on AI by Australian businesses and ordinary Australians. It will also expose Australia to new threats and hazards that need to be managed.

With the Government opting to rely on existing sector-specific regulatory regimes to manage AI adoption, the SOCI Act is the primary framework for managing AI-related critical infrastructure risk. This is particularly urgent given the Government's drive to facilitate investment in this sector, including through initiatives such as hyperscale data centers to host frontier AI models for training and deployment.

This means the SOCI Act regulatory regime needs to be ready to:

(a) Address the risk associated with frontier AI models being hosted and trained in Australian data centres; and

(b) Prepare for when AI models and services are essential to Australian society and thus become critical infrastructure themselves.

AI is becoming critical infrastructure

AI is evolving from a productivity-enhancing tool to a foundational piece of Australia's infrastructure. This transition is not unprecedented. Telecommunications followed a similar path from novelty to convenience to necessity. Today, Australia cannot function without reliable telecommunications. A nationwide telecommunications outage would be catastrophic, paralysing emergency services, financial systems, supply chains, and government operations within hours. AI is on a similar path, and it is moving much faster.

When does AI become critical infrastructure?

While frontier AI models might not be critical infrastructure for Australia today, there is a clear pathway towards this occurring:

Stage 1 (past)	AI is an optional but useful tool. Businesses and users experiment with AI applications, but adoption is limited and consequences of failure are minimal.
Stage 2 (now)	Businesses must integrate AI to remain competitive. Ordinary Australians increasingly rely on AI-enabled services in daily life.

[13] Department of Industry, Science and Resources, *National AI Plan* (2025) 5.

Stage 3 (near future)	AI is embedded in the operation of critical infrastructure across most sectors. Business and government decision-making is augmented by AI tools. Failure of a major AI system causes significant disruption, but alternatives exist and recovery is measured in days.
Stage 4 (medium term future)	AI is as essential as telecommunications or electricity. Society is severely hampered or unable to function during outages or malfunctions of major AI systems. Recovery requires weeks or months. No ready alternatives exist.

Australia is currently transitioning from Stage 2 to Stage 3 under the above schema. AI is increasingly being deployed into operational technology, business-critical systems, and customer-facing services. Our regulatory regime needs to prepare for the next move to Stage 4, before it occurs.

AI as critical infrastructure creates unique threats and hazards, including:

(a) **Concentration risk:** A small number of frontier AI providers dominate the market, meaning a small number of models will likely power a range of services and sectors. This means an issue in one model could rapidly cascade across the economy, similar to the disruption seen by the CloudStrike and Cloudflare outages;[14]

(b) **Deeper integration:** Unlike software that runs alongside business operations, AI is increasingly informing or making operational decisions with less human oversight; and

(c) **Opaque failure modes:** When software such as CrowdStrike fails, it crashes visibly. When an AI system malfunctions, it may continue operating while producing subtly incorrect outputs – a 'silent failure' that can persist for hours or days before detection.

Addressing the gaps in the SOCI Act regime

At present, the SOCI Act framework does not clearly capture Australia's emerging dependency on AI nor provide a clear pathway for managing the transition to AI becoming critical infrastructure. This is evident across two key 'gaps' in the current regime.

Gap 1: Data centres training and hosting frontier AI models are not appropriately covered by the SOCI Act

Section 8D of the SOCI Act recognises the "*critical data storage and processing sector*" as a critical infrastructure sector. However, a data storage or processing asset is only captured under the Act where it is used wholly or primarily to provide services to government bodies or other critical infrastructure entities, and where those services relate to "*business critical data*".[15]

[14] Al Jazeera, *CrowdStrike IT outage causes chaos, disrupting airlines, banks, media* (19 July 2024).
[15] SOCI Act, Section 12F(1) and (2).

This customer- and data-type test is increasingly out of step with where key sources of risk now lie. This test may fail to capture the hyperscale data centres now being built to train and host frontier AI models. As a result, highly capable AI systems – which are likely to be relied upon by Australians at scale and increasingly integrated into critical infrastructure – may fall outside the SOCI regime, regardless of their technical sophistication, systemic importance, or relevance to national security.

For example, a Sydney data centre might train and host an advanced AI model that is later used to support critical functions across Australia, including energy grid management, hospital operations, and financial fraud detection. The same model could also power consumer facing applications and services for small businesses. Despite the importance of the resulting model to Australian society, the data centre may fall outside the scope of the SOCI Act. During training, its primary customer would be the AI developer; during deployment, it is unlikely to be considered as providing services "*wholly or primarily*" to critical infrastructure entities given its broader user base.

Furthermore, even where existing AI data centres are subject to SOCI Act requirements, the CIRMP requirements may not adequately account for AI-specific risk. Section 6 of the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 (**CIRMP Rules**) specifies what "*material risks*" entities need to address in a CIRMP under sub-section 30AH(8) of the SOCI Act. It covers hazards such as stoppages or slowdowns in an asset, substantive loss of access to an asset, and interference or remote access to the asset.

However, hosting or training AI models involves unique hazards specific to AI. This includes the potential for loss of control of the frontier AI model itself (where the model behaves in ways its operators cannot predict, monitor or constrain). Absent clear guidance, these hazards may not be identified or addressed under existing CIRMPs, leaving these data centres exposed.

To address the gap identified in this section:

(a) The **SOCI Act should be amended so that data centres used to train general purpose frontier AI models, or serve such AI models to customers, are themselves treated as critical infrastructure**. This should apply regardless of which customers these data centres serve and whether or not they handle "*business critical data*". The coverage of data centres could be limited by reference to certain sizes of models trained, compute used, and/or the potential consequences that disruption or malfunction of the model could have.

Further, where particular data centres are training or hosting AI models that are especially consequential to Australia's stability, defence or national security, consideration should be given to their designation as a SoNS to enable the application of enhanced obligations commensurate with their importance;

(b) **Guidance for data centre CIRMPs should be updated to clarify how existing categories of material risk apply specifically in relation to training and hosting**

frontier AI models. Alternatively, the CIRMP Rules should be updated to explicitly capture the specific threats and hazards associated with such data centres.

Gap 2: Frontier AI models themselves will need to be covered by SOCI

Regulating data centres will help to address some of the risk associated with advanced AI. However, ultimately, the AI models themselves will need to be covered by the SOCI Act as given their transition into critical infrastructure.

Users, businesses and critical infrastructure operators using and integrating frontier AI are reliant on the AI model being capable, accurate, safe, and secure, and this is separate to the need to ensure the safety and security of the physical data centre hosting the model.

AI model providers themselves therefore need to have risk management programs in place to guard against AI-specific vulnerabilities and hazards. This includes to mitigate potential hazards such as:

(a) **Training data poisoning:** corrupt or biased data being used to train the model resulting in hidden instructions or behaviours that lie dormant until activated;

(b) **Model backdoors:** hidden functions being embedded in the model that activate only under specific conditions, allowing unauthorised control or manipulation;

(c) **Data exfiltration risks:** model weights being stolen by malicious actors; and

(d) **Loss of control:** advanced AI models behaving in ways their operators cannot reliably predict, monitor, or constrain.

Covering AI models as critical infrastructure assets is also consistent with the broader need to transition the SOCI regime to focus on *services* being provided rather than just *assets* that provide such services.

Determining when any AI model meets the criteria for coverage under the SOCI Act will depend on whether its disruption would have a sufficiently severe impact on Australia's economic or social stability, national security, or defence.[16] Practical indicators for when this occurs could include: systemic dependency on a model (how many essential services and Australians rely on it), low substitutability (moving to different models or services would be difficult or impossible), recovery time in the case of a disruption, and the scale of the consequence of an outage or malfunction.

[16] The 2023 Critical Infrastructure Resilience Strategy (February 2023) defines critical infrastructure as "*those physical facilities, systems, assets, supply chains, information technologies and communication networks which, if destroyed, degraded, compromised or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of Australia as a nation or its states or territories, or affect Australia's ability to conduct national defence and ensure national security.*"

Advanced AI models are clearly on track to meet each of these indicators. Once they do, it will be key to ensure the SOCI Act regime is prepared to regulate them.[17]

To address the gap identified in this section **a clear pathway to covering frontier AI models and AI services under the SOCI Act is needed,** to ensure they are appropriately managing risk and are regulated as critical infrastructure once they function as critical inputs to essential service delivery or the broader functioning of the Australian community**.**

Designing and implementing the integration of frontier AI into the SOCI Act regime should be done through structured consultation and co-design with industry on, for example, definitions, thresholds, and which SOCI Act obligations are appropriate for model developers and providers (as distinct from hosting facilities) and what new or modified provisions might be also be necessary.

For example, once frontier AI models are captured by the SOCI Act, the notification of cyber security incidents regime in Part 2B should be amended to require providers of such models to also notify when their AI system is used to cause serious harm (such as by enabling cyberattacks on Australian critical infrastructure).

Summary of Recommendations

5. **Bring frontier AI training and hosting data centres clearly within the SOCI Act.** The SOCI Act should treat data centres used to train or serve general-purpose frontier-scale AI models as critical infrastructure, regardless of the customers served or whether they handle "*business critical data*". Coverage could be limited based on model size, compute used, or the potential consequences of disruption or malfunction. Data centres hosting AI models that are especially consequential to Australia's stability, defence, or national security could be designated as SoNS.

6. **Update CIRMP guidance (and/or amend the relevant Rules) to ensure that AI-specific hazards are captured as material risks for AI data centre assets.**

7. **Create a clear pathway to cover frontier AI models and AI services as critical infrastructure under the SOCI Act**. This will also require new or modified SOCI Act obligations in light of the unique nature of these systems. For example, the notification of cyber security incidents regime in Part 2B of the SOCI Act should be amended to require providers of such models to also notify when their AI system is used to cause serious harm.

[17] Consideration should also be given to designating AI models that are wholly or primarily used to process "*business critical data*" or perform critical business functions of critical infrastructure assets as critical infrastructure assets through amendments to Section 12F(2) of the SOCI Act (similar to existing obligations regarding data storage and processing assets that store business critical data).

E. Evolving Systems of National Significance into an All-Hazards Regime

The SOCI Act's SoNS regime recognises that some critical infrastructure assets are particularly crucial to Australia. The Secretary of the Department is able to apply "*enhanced cyber security obligations*" (**ECSOs**) to this subset of assets, including requirements to develop cyber incident response plans, undertake cyber exercises and vulnerability assessments, and provide system information to the government. The SoNS regime is explicitly focused on cyber security risk. The CISC has stated, for example, that SoNS incident response plans are "*not intended to address hazards more generally*".[18]

The focus on cyber risks made sense in the context in which the SoNS regime was introduced.[19] However, given the increasing range of threats and hazards facing critical infrastructure assets and the recent reforms to ensure the SOCI Act addresses all hazards,[20] the narrow focus on cyber requires reconsideration.

In the current operating environment, SoNS need to be prepared for a wide range of disruptions and incidents, not just those arising from a cyber security incident. The CISC's 2025 Annual Risk Review identified sources of risk across cyber, supply chain, physical and natural, and personnel hazards.[21] Non-cyber disruptions can also easily generate consequences comparable to a cyber incident.

As such, **consideration should be given to amending the SoNS regime to also include 'Enhanced Resilience Obligations' or 'Enhanced Risk Management Obligations'.** These would be focused on ensuring continuity of service delivery during severe disruptions from all sources of hazard. These new obligations could reflect many of the existing ECSOs. For example, they could allow for the Secretary to require a SoNS entity to maintain an all-hazards services continuity plan, define maximum acceptable outages, plan and demonstrate capability to operate for minimum time periods during severe upstream disruptions (such as loss of key suppliers or services), and undertake regular all-hazard exercises.

Consideration should also be given to obliging SoNS to report non-cyber incidents that have a significant impact upon the provision of their services. Ultimately, this could also be expanded to all critical infrastructure assets, to align with the broader SOCI Act move to all-hazards preparedness.[22]

---

[18] Critical Infrastructure Security Centre, *CISC Factsheet - Systems of National Significance Enhanced Cyber Security Obligations* (April 2025) 2.
[19] Department of Home Affairs, *Explanatory Document - Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020* (2020) 5.
[20] Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (29 November 2024).
[21] Critical Infrastructure Security Centre, *Critical Infrastructure Annual Risk Review* (November 2025).
[22] See e.g. European Parliament and Council, *Directive (EU) 2022/2557 on the Resilience of Critical Entities*, 14 December 2022, Article 15, which requires Member States to ensure that critical entities notify incidents that "*significantly disrupt or have the potential to significantly disrupt the provision of essential services*".

Summary of Recommendation

8. **Expand the SoNS regime to include all-hazards resilience obligations.** Following consultation with industry, amend the SOCI Act to enable the application of Enhanced Resilience Obligations to SoNS in addition to the existing ECSO, covering all hazards not just cyber risk. Consideration should also be given to requiring notification of non-cyber incidents by SoNS, and eventually all critical infrastructure assets.

Conclusion

Australia's critical infrastructure is becoming more interconnected and more exposed to potential high-impact disruptions, including catastrophic scenarios that could cascade across sectors. The 2024 reforms to the SOCI Act were an important step to ensuring the regime remains relevant to emerging challenges, but further refinement is needed to ensure the framework remains operationally effective as dependencies deepen, risk increases, and AI systems are transformed into critical infrastructure in their own right.

This submission sets out concrete and practical reforms to strengthen national preparedness. Together, these measures would preserve the SOCI Act's strengths while improving clarity, readiness, and continuity of essential functions under severe disruption. Recognising that these reforms will require effort from both government and industry, Global Shield Australia also recommends that the Department consider expanding the budget and resourcing of the CISC to enable it to effectively implement its enhanced authorities under the SOCI Act and support critical infrastructure operators and owners to meet their obligations.

Global Shield Australia would also welcome the opportunity to meet with, brief, or otherwise engage further with the Independent Reviewer and the Department on the recommendations in this submission.

Contact: australia@globalshieldpolicy.org

Annex A: Amendments to the SOCI Act regarding a National Critical Infrastructure Risk Assessment

Draft amendments to Part 7, Division 4 of the SOCI Act to mandate the preparation of a regular National Critical Infrastructure Risk Assessment.

Part 7, Division 4—Period reports, reviews and rules, etc.

60A National Critical Infrastructure Risk Assessment

(1) The Secretary must, at least once every 3 years, cause to be prepared a written assessment of all hazards and threats that pose a material risk to Australia's critical infrastructure.

(2) An assessment under subsection (1) is to be known as a National Critical Infrastructure Risk Assessment.

(3) Without limiting subsection (1), the National Critical Infrastructure Risk Assessment must:

(a) Identify and describe all material hazards and threats that would, if they materialised, significantly disrupt the availability, integrity, reliability or security of the critical infrastructure services (whether in one sector or across multiple sectors);

(b) Assess the likelihood and impact of each material hazard and threat identified;

(c) Consider vulnerabilities and interdependencies across critical infrastructure assets, sectors, and supply chains, including domestic and international supply chain dependencies that may contribute to cascading failures;

(d) Consider, follow, or reflect any other matter or procedure prescribed by the rules.

(4) The Secretary must give the Minister the National Critical Infrastructure Risk Assessment as soon as practicable after it is completed.

(5) The Minister must cause copies of the National Critical Infrastructure Risk Assessment, or a declassified version of the assessment, to be tabled in each House of Parliament within 15 sitting days of that House after he or she receives the assessment.