Consultation on the Independent Review of the Security of Critical Infrastructure Act (2018)

Authors: [redacted]

Organisation: Vaesec

Public Submission

December 2025

Summary

It is the fundamental position of this submission that the Security of Critical Infrastructure Act (2018) (SOCI) is a positive and necessary government initiative.

Under current conditions, the barriers to targeted attack on Australia's critical infrastructure will remain structurally low in terms of cost, capability, and access for motivated threat actors. In this context, SOCI will not meaningfully improve security through additional preventative obligations alone. Rather, a deliberate regulatory shift toward detection, containment, and consequence management practices is required.

The effectiveness of existing SOCI obligations is constrained by five persistent points of friction for responsible entities:

- submitting operational, control, and influence information;
- accessing actionable context specific threat guidance;
- handling and sharing protected information;
- security vetting of critical workers; and
- access to specialised SOCI expertise.

SOCI has built a foundation for risk visibility, information sharing, and preventative risk mitigation for critical infrastructure entities. To remain effective where disruption is likely to be inevitable, this foundation now should be advanced in two main ways:

- streamlined to reduce friction; and
- deliberately extended to include obligations that position responsible entities to respond to and recover from all-hazard disruptions.

Disclaimer

This submission does not represent, and must not be construed as representing, the views, opinions, compliance status, or risk posture of any specific responsible entity, regulated entity, or stakeholder.

Nothing in this submission constitutes or should be interpreted as an assessment of the compliance position of any specific entity or SOCI sector.

Acknowledgements

We are grateful for the opportunity to contribute to this public consultation.

This submission has been prepared with the anonymous review and input of industry stakeholders to support the continued evolution of SOCI. It has been informed by a broad range of collective experiences designing, implementing, and uplifting end-to-end SOCI compliance programs across multiple responsible entities and SOCI sectors.

Question 1

Is SOCI achieving its intended objectives?

SOCI forms a core industry-centric defensive pillar within Australia's broader national security framework. It is designed to safeguard the continuity of the essential services Australians depend upon by uplifting the baseline security and resilience of Australia's critical infrastructure, spanning 11 sectors and 22 asset classes. In doing so, SOCI intends to mitigate persistent security fragility amid an escalating risk environment driven by both domestic and international threat actors.

Australia's Critical Infrastructure Resilience Strategy 2023 was established to respond to increasing industry susceptibility to a wider range of potential hazards, increasing technological advances and interconnectivity, and increasing geopolitical volatility. These trends are persisting:

- Australia's National Terrorism Threat Level remains at Probable, indicating a greater than 50% chance of an onshore attack or planned attack. This projection is evidenced by declining social cohesion and trust in democratic processes that materialised in the recent Bondi Beach attack.
- Australia is facing a dynamic, diverse, and degraded security environment with multifaceted, merging, intersecting, concurrent and cascading threats. Sabotage is emerging as a distinct threat, with foreign regimes attempting to pre-position cyber access as part of establishing a persistent capability to exploit Australia's critical infrastructure.

To date, SOCI has uplifted material risk awareness, accountability, and senior-level engagement across responsible entities. Mandatory annual Risk Management Program (RMP) reporting for most asset classes has resulted in security and resilience matters receiving more sustained attention at executive and Board levels. Operational progress within responsible entities on meeting SOCI obligations varies across hazard domains but is generally sustained, incremental and in good faith. However, responsible entities are increasingly confronting the reality that uplift is capital-intensive, slow to deliver, and unlikely to meaningfully mitigate exposure.

In our professional opinion, critical assets remain inherently vulnerable to low-complexity and disproportionately high-impact attacks. Basic kinetic attacks could disable critical electricity asset

components, exhaust critical spares, and impose prolonged restoration times. Basic forced entry attacks could disable critical telecommunication asset components and disrupt connectivity for large geographical regions. Basic vehicular or contamination attacks could sabotage critical water asset supply to large population centres. Basic social engineering attacks could expose critical higher education research to misuse. Basic trespass could sabotage critical gas assets isolated on remote properties. Australia's critical infrastructure is inherently vulnerable to attack, and the cost of mitigation is often prohibitive.

As a result, the barriers to targeted attack on Australia's critical infrastructure will remain structurally low in cost, capability, and access for a motivated individual or group. SOCI's requirement to mitigate or eliminate material risks is fundamentally sound, but constrained by cost, legacy design, and structural realities. In response, responsible entities are increasingly defaulting to cautious compliance in anticipation of SOCI enforcement or the occurrence of a major incident. In this context, SOCI's continued effectiveness depends not on expanding preventative obligations, but on a deliberate shift toward requiring detection, containment, and consequence management practices. It is in Australia's interest that this shift occurs before significant pressure is applied by one or more persistent threat actors.

Question 2

Is SOCI functioning as intended?

This submission intends to highlight three areas of friction where we believe SOCI is currently not functioning as intended:

- **Mandatory information reporting:** SOCI requires responsible entities to submit and maintain a range of operational, control, and influence information with government. The intent of these requirements, to provide government with visibility of industry context and interconnectedness, is valid and important. In practice, however, the reporting forms are dynamic, manual, repetitive, and open-ended, making it burdensome for responsible entities. Submissions are also one-sided, often without validation or feedback, creating uncertainty as to whether information has been provided correctly. As a result, the process is difficult for responsible entities and is likely constraining the currency, consistency, and usefulness of the information for the government.
- **Critical worker vetting:** SOCI requires responsible entities subject to a RMP obligation to identify critical workers and restrict access to critical components to individuals assessed as suitable. While the intent of this requirement is sound, its implementation has proven challenging in practice. In the absence of a standardised vetting scheme, responsible entities are required to define and administer appropriate security vetting through lengthy workforce consultation, legal review, and union engagement processes. This has resulted in fragmented practices across responsible entities and introduced complexity where critical components are shared or a responsible entity is reliant on third-party operators.

- **Protected information usage:** The legislative intent to restrict the use of information which if exposed could compromise the security of critical infrastructure or Australia more broadly is sound and necessary. While SOCI establishes mechanisms for permitting the disclosure of protected information for legitimate purposes, uncertainty in how these provisions should be applied in practice persists. This uncertainty is creating friction that delays or discourages information sharing in instances where such sharing would support the mitigation of shared material risks and promote collaboration between interconnected entities and major suppliers.

Question 3

Is SOCI having unintended consequences?

This submission intends to highlight two areas of friction where we believe SOCI is currently having unintended consequences:

- **Limited specialised expertise:** SOCI introduces a dense and broad set of interrelated concepts. Examples include critical infrastructure asset, critical component, critical worker, critical supplier, major supplier, protected information, operator, relevant information, operational information, business critical data, material risks, hazards, data storage system, data storage or processing service, direct interest holder, control and influence information, significant impact, and relevant impact. These concepts require contextual interpretation, asset-specific judgement, and an understanding of legislative intent to meaningfully unpack. This demands deep SOCI experience and legal expertise that is currently scarce in the market and cost-prohibitive for smaller entities.
- **Threat intelligence asymmetry:** Responsible entities largely receive general intelligence and risk guidance to support adoption of SOCI obligations. This tends to inform equally broad preventative uplift that is costly, slow, and diffused. This dilutes investment effectiveness and inflates cost. The result is a persistent mismatch between the precision of threats and the broadness of preventative mitigations. Responsible entities require more responsive, specific, and actionable threat guidance.

Question 4

Are there new or emergent threats the SOCI Act is unable to manage in its current form?

It is the position of this submission that SOCI should continue to remain agnostic to specific threats in its obligations and rules. We believe government should continue to provide guidance on new and emergent threats for entities to consider through the existing established forums.

Attachment A – Recommendations

To further support this independent review, find below a list of proposed recommendations derived from points raised within this submission:

- Extend the scope of Mandatory Cyber Incident Reporting (MCIR) requirements to include any significant or relevant impact regardless of hazard domain. This is to say cyber incidents are not the only incidents that should require reporting.
- Expand the RMP rules to specify requirements for detection, containment, and management of the consequences of a realised impact regardless of hazard domain.
- Provide clear avenues for responsible entities to access government support and capability, including during an incident, without significant risk of punitive penalties.
- Extend the scope of the Systems of National Significance (SoNS) framework to preparedness exercises and vulnerability testing across all hazard domains. This could be supported by greater application of obligations under the framework.
- Simplify how responsible entities submit and maintain the currency of operational, control, and influence information with the government.
- Commence SOCI compliance enforcement with a focus on identifying critical vulnerabilities and issuing specific remediation directions, not punitive penalties. This could be supported by requiring responsible entities to seek external assurance.
- Standardise and centralise critical worker security vetting requirements across all relevant asset classes. This would be supported by removing the need for responsible entities to self-administer checks. AusCheck already provides an established, scalable, and consistent model aligned to comparatively security-sensitive aviation and maritime roles.
- Explore ways to meaningfully bolster the availability of SOCI-specific expertise.