SOCI Act Independent Review Submission

Name: [redacted]
Organisation: MPS People Security Risk Management Pty Ltd (MPS People Security)
Website: https://mpspeoplesecurity.com.au

About the Submitter

MPS People Security provides professional personnel security and insider risk management services, including security training for SOCI entities, industry, and government. We support organisations to strengthen governance, personnel security, and insider risk management.

We have:

- Engaged extensively with SOCI Act entities across food and grocery, energy, and defence supply chain sectors.
- Been invited by the Department of Treasury Insider Threat Forum to present our Insider Threat Framework to 75 entities, demonstrating our leadership in this space.
- Partnered with Dr Eric Shaw, a globally recognised expert in insider threat psychology and mitigation, to deliver specialised advice and training. Dr Shaw's work has shaped insider threat programs internationally.
- Contributed to a new Australian Standard for Personnel Security, reinforcing our commitment to best practice and national resilience.

200-Word Summary

The SOCI Act is directionally sound and has raised awareness of critical infrastructure security obligations. However, it is not consistently achieving its objectives due to a 'light touch' compliance posture and lack of regulatory capacity to review CIRMPs. This results in weak assurance, poor practices, and minimal uplift in personnel security and insider risk management.

Proposed reforms are scheduled to be mandated by 30 June 2028, following an Australia-wide educational SOCI Act roadshow in 2025. Given escalating geopolitical risks and persistent insider threat vulnerabilities, this timeline is inadequate and leaves critical sectors exposed for years.

Feedback from SOCI entities and forums confirms systemic challenges: boards and executives resist insider threat programs because they are not mandated; some entities prioritise profit over security; practitioners lack resources and guidance. Insider threats

remain a primary pathway for sabotage, espionage, and operational disruption.

We recommend accelerating implementation, maintaining a broad SOCI scope, introducing the CIRMP and reporting requirements by 30 June 2026, as initially planned, adopting risk-based personnel security aligned to AS4811:2022, and strengthening regulatory assurance.

Responses to the Four Questions

1) Is the SOCI Act achieving its intended objectives?

Assessment: Partially. The Act has encouraged formalised security governance and risk management planning. Positive security obligations have driven some uplift, particularly where boards treat the framework as a strategic risk issue rather than a compliance exercise.

Key Gaps:

- - CIRMPs often lack actionable, tested controls and are produced as administrative artefacts.
- - Personnel security and insider risk are not treated as core security controls, despite being the primary pathway for sabotage and espionage.
- - Insider threat practitioners report they do not know how to implement programs, have no allocated resources, and feel unsupported.

Recommendation: Re-centre the Act on measurable risk reduction and assurance, including scenario-based testing, continuous improvement, and risk-tiered personnel security aligned to AS4811:2022.

2) Is the SOCI Act functioning as intended?

Assessment: Not consistently. The principles-based framework works when supported by credible oversight and clear guidance. In practice, regulatory capacity constraints and limited engagement with industry specialists has resulted in inconsistent and very minimal uplift.

Additional Insight: Regulators have indicated at industry forums that they lack resources to review CIRMPs, signalling weak compliance expectations.

Recommendation:

- - Establish a scalable assurance model (risk-based sampling, independent audits, maturity assessments).
- - Create a transparent practitioner forum spanning personnel, cyber, physical, and supply chain security.

3) Is the SOCI Act having any unintended consequences?

Assessment: Yes. Compliance cost without proportionate benefit is a significant risk, particularly if personnel security obligations become overly standardised.

Unintended Consequences:

- - Misallocation of resources away from high-risk roles.
- - Reduced focus on elevated access and coercion exposure.
- - Cost pass-through to essential services, impacting consumers through higher cost of living expenses
- - Some SOCI entities admit profit comes first and prefer to 'deal with fallout' rather than invest in prevention.

Recommendation: Mandate role- and access-based personnel security controls with clear risk tiers, aligned to AS4811:2022, and avoid incentivising a paperwork-first culture.

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

Assessment: Yes. The threat landscape has evolved faster than SOCI Act implementation maturity. ASIO warns of foreign adversaries exploiting vulnerabilities and coercing individuals in critical infrastructure roles.

Emerging Threats:

- - Insider-enabled compromise (malicious, coerced, negligent insiders).
- - Blended threats combining cyber, physical, and supply chain vectors.
- - Geopolitical escalation and foreign interference.
- - SOCI entities face interconnected risks, meaning a catastrophic attack on one sector can trigger cascading impacts across multiple sectors, amplifying disruption and national security vulnerabilities.

Recommendation: Strengthen legislative and compliance settings for personnel security programs, including governance, behavioural risk awareness, and tested response pathways. Build regulatory capability for meaningful CIRMP review and define transparent criteria for best practice.

Recommendation: Integrated risk assessments across all critical infrastructure sectors to identify cascading impact scenarios, joint incident response protocols and shared contingency planning to ensure rapid, coordinated action during a catastrophic event.

Legislative Context

The SOCI Act was legislated in 2018. An Australia-wide educational SOCI Act roadshow was undertaken in 2025, with a proposed mandate for SOCI entities to submit their CIRMP reports to Home Affairs. It is now proposed to further extend the mandate to 30 June 2028.

Given escalating geopolitical risks and insider threat vulnerabilities, this timeline is inadequate. Australia cannot afford a prolonged exposure window; reforms must be accelerated to ensure resilience.

Recommendations Summary

- To safeguard Australia's resilience, reforms must be accelerated and broadened with a clear sense of urgency. The proposed extension to 2028 for mandated CIRMP reporting leaves critical sectors exposed for too long. We recommend maintaining the full scope of the SOCI Act, introducing mandatory insider threat programmes and reporting requirements without delay, and embedding risk-based personnel security controls aligned with AS4811:2022. These measures must be supported by increased regulatory resources to enable timely and meaningful CIRMP reviews, robust assurance mechanisms, and cross-sector coordination. Accelerating these reforms is essential to address escalating geopolitical threats and insider risk.

- **Recommendations Summary**
  - Accelerate mandate for CIRMP submission and insider threat programs before 2028.
  - Maintain broad SOCI Act scope beyond energy, transport, and water.
  - Introduce mandatory insider threat program and reporting requirements.
  - Adopt risk-based personnel security aligned to AS4811:2022.
  - Strengthen regulatory assurance through audits, maturity assessments, and practitioner forums.
  - Build capability for meaningful CIRMP review and define transparent criteria for compliance.