Submission to the Independent Review of the *Security of Critical Infrastructure Act 2018*

Pentagram Advisory Pty Ltd

8 December 2025

Executive Summary

Pentagram Advisory Pty Ltd (Pentagram) welcomes the opportunity to contribute to the Independent Review of the *Security of Critical Infrastructure Act 2018* (SOCI Act). Through extensive advisory work with SOCI-regulated entities across multiple sectors, Pentagram has observed that while the SOCI Act has raised national awareness of critical infrastructure risks and established an essential regulatory framework, significant challenges persist in practical implementation, particularly across personnel security, supply chain security, enterprise governance, and interpretation of the Critical Infrastructure Risk Management Program (CIRMP) requirements.

The SOCI Act is achieving several of its objectives; however, it is not yet fully achieving its most important purpose: ensuring responsible entities identify, assess, and manage material risks to the availability, integrity, reliability, and confidentiality of Australia's critical infrastructure assets.

Key issues identified through Pentagram's work include:

- Low self-identification and low CIRMP reporting rates, suggesting many entities have not recognised their obligations.
- Disproportionate focus on cyber hazards, due to the clear availability of cyber standards, its established 'place' in entities, and the absence of comparable guidance for other hazard vectors.
- Misalignment between CIRMP expectations and the protective security culture available in private sector environments, given the Protective Security Policy Framework (PSPF) origins of the CIRMP framework.
- Legacy reliance on AusCheck background checking, which is not designed for contemporary insider threat risk or SOCI personnel hazard obligations.
- Limited enterprise governance integration, with Boards lacking full visibility of SOCI risks.
- Significant resourcing imbalance, where cyber teams are comparatively well-staffed while personnel security, supply chain security, and protective security teams are minimal or absent.

- Procedural SOCI audits that validate compliance artefacts rather than the effectiveness or completeness of the CIRMP to uplift security performance and outcomes, creating a potential illusion of compliance.

Pentagram considers that clearer guidance for the three non-cyber hazards, contemporary personnel assurance frameworks, stronger enterprise governance integration, and a shift from procedural to substantive audit approaches are required for the SOCI Act to fully achieve its national security outcomes.

1. Context

Pentagram was established in May 2024 to provide strategic protective security and SOCI advisory services to Australian critical infrastructure entities.

Pentagram's co-founders have held senior positions across the Attorney-General's Department, the Department of Home Affairs (Home Affairs), Defence, the Department of Infrastructure and Transport, and the Australian Intelligence Community.

Pentagram has advised entities in the Aviation, Communications, Energy, Finance, Health, Water and Sewerage sectors and collaborates with organisations in Defence Industry, Higher Education and Research, Space Technology, and Transport, including Systems of National Significance.

Pentagram is also committed to national uplift through no-cost workshops, expert articles, podcasts, community-of-practice events, and SOCI-aligned eLearning programs.

2. Introduction

The SOCI Act represents a significant evolution in how Australia manages national critical infrastructure security risks. The SOCI Act adopts an all-hazards, principles- and outcomes-based approach requiring responsible entities to identify and mitigate risks across cyber and information security, personnel, supply chain, physical and natural hazard vectors.

However, many entities find the CIRMP difficult to operationalise due to:

- nil or limited protective security expertise
- underdeveloped personnel and supply chain security practices
- lack of clarity regarding proportionality of mitigation versus consequence
- resourcing constraints
- lack of education and training
- misalignment between Australian Government's PSPF-inspired expectations and private-sector operating environments
- ability to comprehend how CIRMP 'fits' into existing business processes and systems spanning operations and governance.

The result is uneven uplift, with cyber programs advancing far ahead of other hazard vectors, perhaps uplifting in a cyber silo rather than enabling uplift of other hazards.

3. Purpose of the SOCI Act

Section 3 of the SOCI Act outlines five objectives, including strengthening transparency, facilitating cooperation, requiring risk identification and mitigation, and enabling government response to significant incidents.

The SOCI Act and the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023* (CIRMP Rules) operationalise risk management obligations through four hazard vectors and require responsible entities to maintain a CIRMP appropriate to their operational context.

While the conceptual model is sound, it implicitly assumes a level of protective security culture comparable to that in Australian Government agencies. This assumption does not hold across much of the private sector, where protective security is not embedded, insider threat is not well understood, and supply chain assurance is still maturing.

In supplementary guidance, Home Affairs has stated that the purpose of the SOCI Act is to strengthen Australia's national security by protecting critical infrastructure from espionage, sabotage, coercion, and other forms of interference that could degrade essential services or undermine sovereign resilience. The Act requires owners and operators of critical infrastructure assets to take positive security obligations proportionate to their operational context and provides the Australian Government with the information and powers necessary to manage and respond to threats affecting national interests.

This reinforces that the SOCI framework is fundamentally a national security mechanism rather than an administrative compliance regime, and that effective implementation depends on a strong organisational understanding of security risk, protective security principles, and the role of critical infrastructure in Australia's economic and social stability. Also, there is a presumption that the private sector will view threat, such as espionage or sabotage, as a Commonwealth entity might.

4. Pentagram's SOCI market observations

Drawing on Pentagram's advisory service engagements and contact with SOCI entities and their employees Pentagram offers, from its vantage point, the following observations about the performance of the SOCI Act.

4.1 Lack of guidance or standards for non-cyber hazards

Clear expectations exist for the Cyber and Information Security hazard through nominated frameworks. No equivalent guidance exists for Personnel, Supply Chain, or Physical and Natural hazards. This results in:

- inconsistent implementation
- confusion about what constitutes adequate or proportionate mitigation

- overreliance on cyber uplift as a proxy for overall security maturity
- underdeveloped personnel and supply chain security programs.

Entities repeatedly express that cyber is clear "because the standard is clear", while the other hazards lack a reference point. Home Affairs has publicly noted it does not intend to nominate equivalent frameworks for the remaining hazards. This has left entities uncertain about what "good" looks like and contributed to significant variation in CIRMP maturity.

4.2 AusCheck has assumed a 'default' setting for background checking

Background checking is recommended rather than mandated under the SOCI Act, with AusCheck offered as the Commonwealth option if background checking is undertaken. Many SOCI entities remain in a compliance mindset and, therefore, default to AusCheck rather than determining what background checking or workforce screening model best meets their operational context and personnel security risk profile.

AusCheck assessments underpin the Aviation and Maritime Security Identification Card (ASIC and MSIC) schemes and were designed to detect unlawful interference, primarily terrorism and serious and organised crime, not contemporary insider threat vectors, supply chain infiltration, cyber-enabled manipulation, or remote-access vulnerabilities.

Contemporary personnel assurance requires far more than legacy point-in-time checks, including:

- role- and risk-based pre-employment screening
- whole-of-person assessment
- behavioural monitoring
- continuous suitability assessment
- supplier personnel assurance
- ongoing threat awareness.

Overreliance on AusCheck provides false assurance, particularly as it is rooted in the early 2000s counter-terrorism settings and has not evolved to address the contemporary threat landscape that SOCI entities now traverse.

4.3 Cyber and Information Security hazard dominates the hazard types

Given the ubiquity and central role of information technology in operating critical infrastructure assets, cyber naturally receives the greatest attention and resources. Chief Information Security Officers (CISOs) are often treated as the enterprise's default protective security lead, even though their expertise is centered on cyber.

This creates systemic imbalance:

- the cyber hazard consumes resources
- personnel and supply chain security remain underdeveloped
- entities attempt to "buy" cyber threat mitigation rather than achieving it through integrated personnel and supply chain security

- personnel security performance remains a limiting factor in cyber resilience.

Balanced protective security performance requires integrating cyber with personnel security and supply chain security, not treating them as separate domains.

4.4 Gap between Home Affairs' advice and 'real world' solutions is keenly felt by SOCI entities

Home Affairs frequently emphasises that mitigation measures must be tailored to each entity's "operational context". While well-intentioned, many SOCI entities report that this principle does not translate into practical, achievable, or affordable solutions.

Entities consistently seek:

- clearer guidance
- examples of proportionate mitigation
- realistic pathways toward maturity
- clarity about minimum expectations.

The gap between high-level principles and real-world implementation remains one of the most significant barriers to the CIRMP security maturity.

4.5 Governance frameworks and indicative standards are lacking

This observation is reflected in entity feedback to Home Affairs and echoed in Pentagram's engagements. SOCI entities appreciate that the Cyber and Information Security hazard nominates five frameworks with an identified target level. They seek equivalent certainty for Personnel Security, Supply Chain, and Physical and Natural hazards.

However, Home Affairs has confirmed it does not plan to nominate guidance akin to that for the cyber domain.

The impact is that:

- Cyber is relatively well-governed
- Personnel, Supply Chain, and Physical/Natural hazards are less well-governed and less governable
- Personnel security remains the least well-supported hazard due to legal constraints (e.g. Privacy Act), cultural sensitivities, and workplace resistance to changes needed for effective mitigation

The absence of indicative standards contributes directly to inconsistent CIRMP quality.

4.6 Home Affairs as advisor and regulator can deter SOCI entities from seeking its advice

Pentagram has been asked by clients to approach Home Affairs on their behalf, without disclosing their identity, because the client feared negative regulatory consequences. This indicates that the dual role of advisor and regulator can create hesitancy in seeking

clarification or assistance, working against the collaborative intent of the SOCI framework.

4.7 Insider threat is not well understood

The Personnel Security hazard is integral to mitigating the other three hazards. It transcends the "critical worker" definition and includes the behaviours, motivations, and access pathways of all employees, contractors, and suppliers.
Insider threat is dynamic because:

- people can adapt, deceive, and conceal
- motivations evolve rapidly due to internal or external pressures
- malicious insiders exploit trust, access, and privileges.

Many SOCI entities underestimate the scope and behavioural complexity of insider threat. Pentagram notes that beyond cyber exploitation from outside, an adversary's next best option is to coerce or recruit an insider to achieve information collection or disruption objectives.

4.8 Insider Threat Program is not well understood

The SOCI Act and the CIRMP Rules do not use the term "insider threat program", yet such a program is the practical mechanism by which entities meet section 9 of the CIRMP Rules for mitigating personnel hazards.

Most SOCI entities:

- equate personnel security with background checks
- do not have structured insider threat programs
- lack behavioural reporting frameworks
- do not conduct continuous evaluation or suitability assessments
- focus only on "critical workers", not the broader set of personnel with access pathways.

4.9 Personnel security hazard is not well understood

Entities often struggle with:

- identifying who their critical workers (and their alternates) actually are
- managing personnel risks within supply chains
- distinguishing between eligibility, suitability, and ongoing assessment
- embedding personnel security governance into the enterprise risk management framework (ERMF) processes.

Personnel security remains the least mature hazard domain.

4.10 Supply chain hazard is not well understood

Home Affairs has indicated in its 2024–2025 engagements that supply chain hazards, along with personnel hazards, are the least understood by entities undergoing audits or regulatory dialogue.

Common shortcomings include:

- limited visibility of upstream and downstream dependencies
- procurement-driven rather than risk-driven processes
- insufficient supplier assurance
- lack of understanding of third-party personnel risks.

4.11 Procedural SOCI audits versus substantive CIRMP effectiveness assessments

Current SOCI audits conducted by Home Affairs are predominantly procedural, verifying the existence of artefacts such as registers, policies, and CIRMP documentation. These audits do not assess:

- the quality of risk identification
- whether material risks are accurately analysed
- whether mitigation strategies are proportionate and effective
- whether personnel and supply chain hazards have been meaningfully considered
- whether mitigation measures are operationalised
- whether CIRMP governance is mature or integrated into the ERMF.

A CIRMP may therefore pass a procedural audit while still being ineffective in protecting the asset.

This can create false assurance for regulators and entities. Substantive effectiveness assessments, requiring deep operational understanding, are necessary for the SOCI Act to function as intended.

5. Findings

1. The SOCI Act is conceptually sound but not yet fully achieving its objective of ensuring material risks are identified and mitigated.
2. The absence of guidance for non-cyber hazards results in inconsistent implementation maturity.
3. CIRMP requirements assume PSPF-like protective security capability, which is not present in most private sector entities.
4. Reliance on AusCheck leads to inadequate personnel hazard mitigation.
5. Enterprise governance integration is limited, leaving significant visibility gaps for Boards.
6. SOCI implementation is hindered by workforce and capability imbalances.
7. Many entities still treat SOCI as a compliance exercise rather than a national security responsibility.
8. The current audit program is largely procedural and may create false assurance by validating compliance artefacts rather than evaluating CIRMP effectiveness.

6. Pentagram's response to the Review's questions

Q1. Is the SOCI Act achieving its intended objectives?

Partially.

Using the purpose of the SOCI Act as outlined earlier in this submission, Pentagram contends that the Act is achieving, to varying degrees, most of its intended objectives, particularly those where the SOCI framework seeks to improve, facilitate, impose, or provide, which are principally Commonwealth-driven actions.

However, the most important objective, requiring responsible entities for critical infrastructure assets to identify and manage risks relating to those assets, is not yet being fully realised.

Pentagram bases this assessment on three factors:

1. Limited penetration and uptake of the CIRMP regime across the SOCI market.

Home Affairs reported that in 2024 it received 457 CIRMP annual attestations from approximately 831 critical infrastructure entities, and the 2025 figure has not yet been released. This low response rate, when compared to the expected total number of responsible entities (likely in the thousands), suggests that the SOCI obligations have not yet sufficiently penetrated the market.

2. Many entities lack the foundational enterprise security risk assessment (ESRA) necessary to fulfil SOCI obligations.

Pentagram's client engagements reveal that many entities do not have an ESRA in place and therefore cannot reliably:

- recognise their critical assets
- identify relevant threats
- understand vulnerabilities
- determine proportionate and effective mitigation strategies.

The ESRA is the foundation of an effective CIRMP. Without it, entities cannot meaningfully identify or manage risks across all hazard vectors.

3. Additional factors observed across industry

Pentagram's assessment is further supported by:

- capability gaps affecting personnel, supply chain, and physical hazard domains
- a cultural and structural mismatch between PSPF-derived expectations and private-sector resourcing models
- the absence of standards or indicative frameworks for non-cyber hazards

- a predominantly procedural audit model that validates documentation rather than assessing CIRMP effectiveness.

Q2. Is the SOCI Act functioning as intended?

Functionally yes; practically uneven. Sector maturity varies significantly.

Pentagram's assessment is that the SOCI Act is functioning as intended in some areas, particularly where the requirements are clear and directly actionable. For example:

- some (but not all) critical infrastructure entities have identified that they are subject to the SOCI Act
- some SOCI entities have met, or are in the process of meeting, their Positive Security Obligations (PSOs)
- some SOCI entities have improved the security of their critical asset(s) by identifying and mitigating risks aligned with the PSOs and the CIRMP framework.

However, there remains ongoing confusion among entities regarding their obligations, how to implement them, and what level of risk mitigation maturity is sought by Home Affairs. This contributes to uneven implementation and highly variable CIRMP quality across sectors.

If the SOCI Act is intended to foster an embedded culture of protective security across all critical infrastructure sectors, a culture akin to that found in Commonwealth entities such as the intelligence community or Defence, Pentagram does not observe evidence that such a culture has taken root broadly. It may be emerging within a small number of SOCI entities but this is not yet widespread or demonstrably effective.

Pentagram therefore assesses that while the mechanisms of the SOCI Act are functioning, practical implementation remains uneven, and without stronger guidance, capability development, and governance integration, uplift is likely to remain inconsistent across the SOCI landscape.

Q3. Is the SOCI Act having any unintended consequences?

Yes.

Pentagram has observed several unintended consequences arising from the implementation of the SOCI Act.

1. Overreliance on AusCheck background check, leading to suboptimal personnel security outcomes

The reference to background checking within the SOCI framework, combined with the promotion of AusCheck background check, has unintentionally encouraged entities to treat AusCheck as the default or preferred option.

This results in:

- reliance on a check not designed for contemporary insider threat or supply chain risk
- false reassurance that an AusCheck background checking result equates to effective personnel security vetting
- reduced investment in tailored, context-specific background checking.

This dynamic increases the likelihood of personnel security gaps and, in some cases, insider threat risks.

2. Misinterpretation of procedural audits as indicators of actual security effectiveness

Because SOCI audits focus on documentation and artefacts, many entities assume that "passing" an audit means they have adequately mitigated their risks. This unintended consequence can create false confidence and divert attention away from substantive improvements in protective security.

3. Skewed resource allocation driven by clarity rather than risk

The clarity of cyber standards compared to other hazards has unintentionally led some entities to over-invest in cyber uplift while under-investing in personnel and supply chain security. Although this overlaps with capability issues, the unintended aspect is that entities prioritise what is easiest to understand, not necessarily what is most critical to their risk profile.

Q4. Are there new or emergent threats the SOCI Act is unable to manage in its current form?

Yes.

Artificial Intelligence (AI) may evolve to be a non-human source of harm that will need to be treated in ways analogous to human-based insider threats. In particular, if Artificial General Intelligence (AGI) is deployed – current estimates are for AGI to be realised in two to ten years – then AI / AGI will need to be addressed through the dual lenses of cyber and personnel security. These technologies may therefore require new or adapted mitigation approaches that treat AI/AGI risks through both cyber and personnel security lenses.

7. Conclusion

The SOCI Act has elevated national and international partners and allies' expectations for critical infrastructure risk management but its implementation and workplace security culture messaging remain challenging for many entities to operationalise.

The lack of non-cyber hazard guidance, reliance on outdated background checking, operational-culture mismatch with PSPF expectations, limited governance integration, and procedural audit approaches all constrain effective uplift.

For the SOCI Act to fulfil its national security purpose, responsible entities need clearer guidance, stronger protective security capability, contemporary personnel assurance frameworks, and audits that assess not only procedural compliance but the effectiveness and appropriateness of the CIRMP in real operational contexts.

However, there are limitations in the advice and support that the Commonwealth overall, and Home Affairs as the regulator, can provide to operationalise this government security policy in the context of private sector for-profit entities. Accordingly, Home Affairs should consider how best to collaborate with private sector providers to uplift initial security posture and enable the ongoing security maturity performance of SOCI entities.

Pentagram remains committed to supporting the uplift of Australia's critical infrastructure resilience.

[redacted]

[redacted]

Pentagram Advisory Pty Ltd

[redacted]

[redacted]

Pentagram Advisory Pty Ltd