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

Pentagram Advisory Pty Ltd

19 December 2025

Dear Dr. Slay,

Pentagram Advisory Pty Ltd (Pentagram) welcomes the opportunity to provide this supplementary submission to the Independent Review of the *Security of Critical Infrastructure Act 2018* (SOCI Act). This submission focuses specifically on the role of protective security education in enabling effective implementation of the SOCI Act.

Protective security education to critical infrastructure sector

The Commonwealth government does not provide protective security education or training to critical infrastructure entities subject to the *Security of Critical Infrastructure Act 2018* (SOCI Act). While the Department of Home Affairs (Home Affairs) publishes guidance material, runs the Trusted Information Sharing Network (TISN), and performs an essential regulatory function, it is necessarily limited in the extent to which it can provide practical, entity-specific guidance on how to interpret and operationalise the SOCI Act and subordinate rules obligations.

Home Affairs' role as regulator means it is not positioned to deliver the type of applied skills-based education required to translate legislative requirements into effective security practice, particularly for the unique operational context of any responsible entity subject to the SOCI Act. This creates an education and capability gap between the SOCI legislation and its implementation within the diverse operational, commercial, and risk environments of SOCI entities.

Education as a prerequisite for effective SOCI implementation

Pentagram's experience since 2022 indicates that many SOCI entities struggle not with intent or willingness to comply, but with:

- understanding the evolving threat environment relevant to critical infrastructure,
- developing the in-house professional skills required to conduct fit-for-purpose security risk assessments, and
- translating CIRMP obligations into proportionate, defensible, and business-aligned controls.

The effective implementation of the SOCI Act obligations depends fundamentally on:

- an informed understanding of contemporary threat actors, methods, and vulnerabilities,
- professional competence in security risk assessment methodologies, particularly for personnel and supply chain hazards, where capability is generally less mature than for cyber, information, physical security or natural hazards, and
- the integration of security risks to critical infrastructure into the organisation's enterprise risk management (ERM) framework as a subset of overall enterprise governance.

Where security risks associated with critical infrastructure are not assessed using recognised risk methodologies, or are treated as compliance artefacts rather than enterprise risks, they are unlikely to be visible to senior executives or Boards. This undermines the intent of the SOCI Act, which relies on informed governance, investment prioritisation, and accountability at the highest levels of an organisation.

CIRMP, Board visibility, and risk-based decision-making

A CIRMP that is not underpinned by skilled risk assessment and a clear understanding of threats is unlikely to:

- meaningfully inform Board-level decision-making,
- support defensible annual CIRMP attestations, and
- drive sustained improvement in security maturity and resilience.

Conversely, SOCI-aligned education enables entities to:

- understand why specific threats matter to their business
- assess security risks in a way that is consistent with enterprise risk appetite and tolerance
- document decisions and residual risk in a defensible manner, and
- position security as an enabler of resilience and continuity, rather than as a stand-alone compliance burden.

Consideration for the Review

Accordingly, Pentagram encourages the Review to consider making comment on:

- the need for SOCI-aligned protective security education, spanning the needs of a security practitioner to a director, as a critical enabler of effective SOCI implementation and protection of critical infrastructure assets and operations,
- the role of professional skills and specialist advice in security risk assessment, threat analysis, and operationalising the SOCI Act in achieving the objectives of the SOCI Act,
- the need for specialist advice to determine SOCI Act Critical Infrastructure Risk Management Program (CIRMP) effectiveness and maturity, and
- the benefits of embedding critical infrastructure security risks within enterprise risk management and Board-level governance frameworks.

Improved access to, and recognition of, SOCI-aligned education would support stronger security outcomes for critical assets and operations, while also delivering tangible business benefits through improved decision-making, prioritisation of investment, and organisational resilience.

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

Pentagram Advisory Pty Ltd

Pentagram Advisory Pty Ltd