SUBMISSION

Home Affairs – Independent Review of the Security of Critical Infrastructure Act 2018

17 December 2025

The Association of Superannuation Funds of Australia Limited
[redacted]

W www.superannuation.asn.au

ABN 29 002 786 290 CAN 002 786 290

File: 2025/40

Dr Jill Slay
Independent Reviewer
Statutory Review of the Security of Critical Infrastructure Act
3 Molonglo Dr, Canberra Airport ACT 2609
Sent via email: SOCI.Independent.Review@homeaffairs.gov.au

17 December 2025

Dear Dr Slay,

Home Affairs – Independent Review of the Security of Critical Infrastructure Act 2018 (Cth)

The Association of Superannuation Funds of Australia (ASFA) is pleased to provide this submission Home Affairs on your consultation in relation to the Independent Review of the *Security of Critical Infrastructure Act 2018* (Cth)(the SoCI Act).[1]

About ASFA

ASFA, the voice of super, has been operating since 1962 and is the peak policy, research and advocacy body for Australia's superannuation industry. ASFA represents the APRA regulated superannuation industry with over 100 organisations as members from corporate, industry, retail and public sector funds, and service providers. We develop policy through collaboration with our diverse membership base and use our deep technical expertise and research capabilities to assist in advancing outcomes for Australians.

We unite the superannuation community, supporting our members with research, advocacy, education and collaboration to help Australians enjoy a dignified retirement. We promote effective practice and advocate for efficiency, sustainability and trust in our world-class retirement income system.

ASFA's Opening Comments

ASFA is strongly committed to ensuring that Australia's Security of Critical Infrastructure (SoCI) framework functions effectively to protect superannuation fund members and their retirement savings.

We have previously made submissions in relation to recent amendments to the SoCI Act. These include:

1. ASFA's 29 February 2024 submission to the Department of Home Affairs consultation on Legislative Reforms required under the 2023–2030 Australian Cyber Security Strategy.[2]

2. ASFA's 25 October 2024 submission to the Parliamentary Joint Committee on Intelligence and Security's inquiry into the Cyber Security Legislative Package. This included recommendations in relation to changes made to the SoCI Act in the package.[3]

- We attach this submission in full as **Attachment B** to this submission, to assist the Independent Review.

[1] Home Affairs, *Consultation on the Independent Review of the Security of Critical Infrastructure Act 2018* (2025).
[2] ASFA Submission to the Department on Legislative Reforms required under the 2023–2030 Australian Cyber Security Strategy (29 February 2024).
[3] ASFA Submission to the Parliamentary Joint Committee on Intelligence and Security – Cyber Security Legislative Package 2024 (25 October 2024).

3. ASFA's 14 February 2025 submission to the Department, in relation to your Consultation on Subordinate Legislation under the Cyber Security Act and Security of Critical Infrastructure Act 2018 (SOCI Act).[4]

We note that the core questions asked by the Independent Review, being conducted by Dr Jill Slay AM pursuant to section 60 of the Act, are as outlined below. They relate to if the SOCI Act is:[5]

1. achieving its intended objectives

    - ASFA notes that, for financial institutions regulated under APRA, a clear alignment and expectation should be articulated with expectation defined under the SoCI Act around applicability and reporting of incidents.

    - Additionally, the focus should also be on operational testing of controls (for effectiveness) to provide assurance that those measures will work in crises. This expectation currently is not articulated clearly in the Act.

    - While the threshold for applicability is for superannuation funds above $20 billion, it leaves a gap for mid-size funds and financial organisation who are close to this threshold but do not need to comply with SoCI.

    - Perhaps additional guidance is required to provide coverage for those organisations (under the threshold) on how they can manage the operational resilience and cyber risk or another alternate regulation applied to them (e.g. APRA) that achieves similar outcomes to SoCI.

2. functioning as intended

3. having any unintended consequences

    - Where the Act relies on other regulations (such as those issued by APRA) to manage the cyber or resilience related risks, this should be mentioned explicitly in the Act. This would facilitate compliance.

4. are there new or emergent threats the SOCI Act is unable to manage in its current form.

    - Consideration should be given to the risks to the regulated entity's critical assets from emerging threats such as AI, Quantum Cryptography, Quantum Computing and third party reliance.
    - This should be articulated and expectations defined from Critical Incident Risk Management Plan (CIRMP) perspective.
    - These are the new areas that a currently not defined in SoCI and should be addressed.
    - Regulated entity's threat assessments to address emerging threats should also be tied to their CIRMP.

[4] ASFA Submission to the Department on Consultation on Subordinate Legislation to the Cyber Security Act and Security of Critical Infrastructure Act 2018 (SOCI Act)(14 February 2025).
[5] Home Affairs, *Consultation on the Independent Review of the Security of Critical Infrastructure Act 2018* (2025).

ASFA intends to answer these questions wholistically, by outlining our proposed reforms to the SoCI Act, that would help it to better achieve its objective, function as intended and address emergent threats without unintended consequences.

Our detailed recommendations are outlined in **Attachment A**, and are consistent with the proposals contained in our 25 October 2024 submission, as outlined above.

If you have any questions on our recommendations or would like to discuss them further, please feel free to reach out to [redacted] via [redacted] or [redacted].

Yours sincerely

[redacted]

[redacted]

Attachment A – ASFA's Detailed Comments and Recommendations

Background

ASFA notes that the SoCI Act applies to the superannuation sector by virtue of section 8E(1)(4)(b) of the Act, which indicates that the Act applies to a 'critical superannuation asset'.[6]

Pursuant to the relevant Rules made under the SoCI Act, 'critical superannuation assets' are Registrable Superannuation Entity (RSE) licensees that hold total assets over $20 billion.[7]

This means that RSE licensees holding assets under $20 billion are not subject to the relevant obligations.

With respect to the current functioning and effectiveness of the SoCI Act, ASFA makes the following recommendations.

Recommendations

Recommendation 1 – Further clarification of definitions

In relation to section 9(7) of the Act, ASFA has the following recommendations.

- ASFA seeks more detailed guidance in relation to how the terms 'business critical data', 'hazard' and 'material risk' should be applied. The provision of examples would assist.

- We note the term 'business critical data' is defined in section 5 of the SOCI Act. We also note the term 'critical data storage or processing asset' is defined in section 12F of the SOCI Act.

- However, these provisions have yet to be interpreted by a court, so guidance with examples would help provide certainty regarding how these provisions are to be interpreted.

- Consistent with our previous submission, the phrase 'information related to any research and development of a critical infrastructure asset' should be removed from the definition of 'business critical data' in section 5 of the SOCI Act. This is because, in the superannuation context, this would include benign demographic and aggregate data used for the modelling of retirement products.[8]

- Consideration should also be given to having sector-specific definitions of 'business critical data', rather than one across the board definition, so the unique characteristics of each industry can be handled as necessary.[9]

Recommendation 2 – Clarification of consequence management powers

ASFA notes amendments in the Cyber Security Legislative Package created new consequence management powers, whereby the Minister may authorize the Secretary to do any of the following under the SOCI Act, as summarised in section 35AA of the Act

1. give information-gathering directions to regulated entities under (see section 35AK);
2. give action directions to regulated entities (see section 35AQ);
3. give intervention requests to an authorised agency (see section 35AX).

These powers are extraordinarily broad. For example, under section 35AQ, the Secretary can:

---

[6] This means that the obligations which attach to the 'financial services and markets sector' under section 8D(c) of the Act also apply to 'critical superannuation assets', as defined under section 12J.

[7] Department of Home Affairs, Critical Infrastructure Security Centre, 'SOCI Act 2018 for financial services and markets' (viewed on 9 December 2025). The specific Rules are the *Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021*.

[8] ASFA, Submission to Home Affairs on the Cybersecurity Legislative Reforms Consultation Paper (29 February 2024), 5

[9] Explanatory Memorandum, Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 11[37].rep

[G]ive the entity a direction that directs the entity to do, or refrain from doing, a specified act or thing within the period specified in the direction.

ASFA further notes that the amendments passed in November 2024 replaced the narrower term 'cyber incident' with the broader term 'incident'. This substantially extends the application of these already extensive powers.[10]

In relation to these powers, ASFA recommends the following:

1. Ministerial authorisation of the Secretary giving the directions outlined above should expire after a set timeframe, to ensure that such directions are targeted, limited and subject to appropriate and regular oversight.

2. Ministerial authorisations and directions by the Secretary should be subject to the parliamentary scrutiny and disallowance provisions in the *Legislation Act 2003* (Cth)(the Legislation Act).

3. Consideration should be given as to if these powers should be narrowed, constrained by a more detailed list of legislated necessary preconditions prior to their use.

Recommendation 3 – The definition of 'protected information'

The meaning of 'protected information' is contained within section 5A of the Act.

Consistent with our previous submission in relation to the Cyber Security Legislative Package, ASFA recommends the following:

1. That there should be detailed Rules and Guidance outlining the exact circumstances in which employees of the Australian Public Service can disclose otherwise 'protected information' as the terms above are broad and open to myriad interpretations.[11]

2. These should be subject to further public consultation with industry. The Limitations on disclosures of protected information should account for the limited use protections which this package proposes to introduce in both the *Cyber Security Act 2024* (Cth)(the Cyber Security Act) and the *Intelligence Services Bill 2024* (Cth)(the Intelligence Services Bill), and ASFA's recommendations in this regard.[12]

3. ASFA further recommends that section 5A should be amended to insert the word **'directly'**, as emphasised below. All necessary consequential amendments should be made to implement this change, so that:[13]

> *[A] document or information is only protected information if the disclosure of that document or information* ~~***could***~~ ***is likely to directly*** *cause harm, or pose risk to the Australian public, the security of the asset, commercial interests, the socioeconomic stability, national security or defence of Australia*

[10] Explanatory Memorandum, Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (Cth) 11[39].
[11] ASFA Submission to the Parliamentary Joint Committee on Intelligence and Security – Cyber Security Legislative Package 2024 (25 October 2024) at 13.
[12] ASFA Submission to the Parliamentary Joint Committee on Intelligence and Security – Cyber Security Legislative Package 2024 (25 October 2024).
[13] ASFA Submission to the Parliamentary Joint Committee on Intelligence and Security – Cyber Security Legislative Package 2024 (25 October 2024) at 13.

4. Regulated entities should also be able to share threat intelligence and learnings in a protected way and without fear of prosecution. This would help better protect all regulated entities and their customers.

Recommendation 4 - Direction to vary critical infrastructure risk management program

The Act outlines that 'relevant officials' within the Government may issue directions to vary critical infrastructure risk management programs in section 30AI.[14]

ASFA recommends that this section of the Act should be amended in the following ways:

1. The class of 'relevant officials' capable of issuing a direction under this part should be simplified to just 'the Secretary or their authorised delegate.'[15] The current longer list confers this significant power on too many potential individuals.

2. Further guidance needs to be provided on examples of the kinds of situations which would constitute a 'serious deficiency',[16] because the legislative language could cover a multitude of scenarios. This should be narrowed.

3. The Regulator should be defined in the legislation, so it is clear who will be the responsible entity in respect of this clause.[17]

[14] ASFA Submission to the Parliamentary Joint Committee on Intelligence and Security – Cyber Security Legislative Package 2024 (25 October 2024) at 14.
[15] Section 30AI(2).
[16] Explanatory Memorandum, Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (Cth) 35[213].
[17] Section 30AI(2b).