Australian Banking Association

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

Department of Home Affairs

22 December 2025

Australian Banking Association

Table of Contents

Overview 2

Recommendation 1: Harmonise the SOCI Act with existing frameworks for the financial services sector 2

Recommendation 2: Rationalise duplicative reporting obligations 3

Recommendation 3: Focus on clarity, operability and proportionality in the ongoing application of the SOCI Act framework 4

Recommendation 4: Enhance the SOCI Act's practical application by emphasising recovery and resilience 4

Policy Lead: [redacted] | [redacted]

About the ABA

The Australian Banking Association advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

Australian Banking Association

Overview

The ABA welcomes the opportunity to contribute to the Independent Review of the Security of Critical Infrastructure Act 2018 (SOCI Act). The ABA broadly supports the SOCI framework and acknowledges its role in strengthening resilience across critical infrastructure sectors.

This submission highlights opportunities to improve the effectiveness and workability of the regime of prudentially regulated entities, without undermining the SOCI Act's core objectives and recognising the overlap of regulatory frameworks that already govern the financial services sector. In particular, it focuses on harmonisation with existing prudential frameworks, rationalisation of duplicative incident reporting obligations, improved clarity and operability in the ongoing application of the SOCI framework, and opportunities to strengthen its practical application with a greater emphasis on resilience, recovery and supply chain risk.

The ABA would welcome the opportunity for Dr Jill Slay AM to meet with members to discuss these issues and share practical insights from the operation of the SOCI Act framework in practice.

Q1. Is the SOCI Act achieving its intended objectives

The SOCI Act has played a significant role in elevating the focus on cyber security, operational risk and supply chain resilience across critical infrastructure sectors, including financial services and markets.

However, for prudentially regulated banks, many of these outcomes are already delivered through parallel regulatory frameworks. To maximise both efficiency and effectiveness, the ABA considers that future development of the regime should prioritise harmonisation with existing regulatory frameworks, removal of duplicative reporting obligations across SOCI and other regimes, and legislative and regulatory simplification so that entities can focus resources on substantive uplift rather than navigating overlapping rules. The following key recommendations are directed at that goal.

Q2. Is the SOCI Act:
- functioning as intended
- having any unintended consequences

While the SOCI Act is broadly functioning as intended and has delivered significant uplift for less-mature sectors, ABA members have identified a number of unintended consequences in its operation for prudentially regulated financial institutions, outlined below.

Recommendation 1: Harmonise the SOCI Act with existing frameworks for the financial services sector

For ABA members, the operation of the SOCI Act sits alongside a dense and mature prudential framework. ABA member banks are subject to Australian Prudential Regulatory Authority's (APRA) prudential standards, including CPS 230 (Operational Risk Management) and CPS 234 (Information Security), which already impose detailed requirements on operational risk, critical operations, outsourcing and information security.

In practice, the SOCI Act is often regulating the same risk domains as APRA, but using different concepts, thresholds and processes. This can result in parallel governance, documentation and assurance streams for substantially similar obligations, increasing administrative burden without a commensurate uplift in resilience or regulatory benefit.

Members consider that the SOCI Act would function more effectively if, for APRA-regulated entities, the SOCI Act were explicitly harmonised with the prudential framework. This could include standardised requirements developed jointly with APRA and other key regulators, clear "deemed compliance" pathways

where prudential standards already provide an equivalent or higher level of assurance, and targeted exemptions to avoid duplicative obligations. Such an approach would reduce unnecessary complexity and allow resources to be redirected from mapping overlapping frameworks towards substantive improvements in cyber security and operational recovery.

Recommendation 2: Rationalise duplicative reporting obligations

The ABA strongly supports the development of a single cyber incident reporting portal and the harmonisation of reporting obligations across government agencies, as a critical step to reduce duplication, improve information sharing and free up resources for frontline cyber defence and incident response. However, members emphasise that a portal alone will not resolve the underlying problem unless it is accompanied by alignment of the substantive reporting requirements themselves.

Australian banks have incident and data breach reporting obligations to numerous Australian Government and related entities. A non-exhaustive list includes:

1. Office of the Australian Information Commissioner (OAIC)
2. Australian Prudential Regulation Authority
3. Australian Securities and Investments Commission (ASIC)
4. Australian Signals Directorate's Australian Cyber Security Centre (with connected reporting requirements to the Department of Home Affairs)
5. Australian Securities Exchange
6. Reserve Bank of Australia
7. State-based regulators, including privacy and information commissioners

Regrettably, these different regulators impose reporting obligations that overlap in scope, trigger events, thresholds, recipients, formats, deadlines, escalation pathways and data.

The outcome of the current landscape is that banks must respond to the same (or only slightly different) questions and requests from multiple regulators for a single incident. The extent to which information is shared within government and by regulators is uncertain. Ultimately, this impacts the capacity of backend systems and staffing to remediate incidents and coordinate responses to the resulting investigations. In the event of a significant incident, the requirement to manage multiple and duplicative reporting obligations, presents the risk of distracting resources from management of the actual incident while providing a fragmented picture of the incident to varying Government agencies and regulators which undermines their capability to assist.

This duplication is amplified when considering reporting obligations may exist across multiple jurisdictions for entities with operations extending outside of Australia. Large, multinational financial services organisations will likely have multi-jurisdictional obligations in the case of a cyber security breach. These obligations have different reporting timelines, different information requirements and forms they must take.

The ABA holds the strong view that alignment of the underlying requirements across regulators to achieve a consistent set of reporting obligations and thresholds would bring benefits across all parties – improving information flows between the private and public sectors and allowing more resources to be dedicated to frontline cybersecurity management.

The ABA notes that this challenge is not unique to Australia and strongly endorses the final report of the Financial Stability Board, *FIRE: Format for Incident Reporting Exchange*,[1] that supports the use of a standard reporting format for cyber incidents.

[1] https://www.fsb.org/2025/04/format-for-incident-reporting-exchange-fire-final-report/

Australian Banking Association

Recommendation 3: Focus on clarity, operability and proportionality in the ongoing application of the SOCI Act framework

Greater consistency and clarity in definitions, thresholds and data classifications across regulatory instruments would materially assist entities to meet their obligations more efficiently. Members also see opportunities to improve the practical operation of the SOCI Act through clearer articulation of expectations and greater use of cross-sectoral exercising to test how the framework operates in practice.

A consequence of the current framework is inconsistency in key definitions and data classifications across SOCI, prudential standards and privacy law. Terms such as “significant impact”, “material incident”, “business critical data”, “critical” and “sensitive” are used with different thresholds, scopes or legal consequences. This makes it difficult for entities to design a single, coherent control and reporting framework, instead requiring complex interpretations that contribute to defensive reporting behaviour.

Members consider that aligning definitions and materiality thresholds across SOCI, APRA standards, ASIC and OAIC requirements would materially improve workability and support genuinely risk-based decision-making.

Members also note that exemptions and carve-outs within the SOCI Act framework are not always clearly articulated or easy to identify, particularly where they arise through a combination of primary legislation, rules and guidance. This increases reliance on legal interpretation rather than operational guidance and adds unnecessary compliance friction.

Similarly, while the government assistance and step-in powers are accepted in principle as necessary for extreme circumstances, they are complex and difficult to interpret in practice. Uncertainty remains about when these powers may be triggered, how key thresholds are assessed, and how they interact with the role of sectoral regulators such as APRA. Members are not seeking to limit the availability of these powers, but greater clarity around their operation would support preparedness and confidence.

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

Recommendation 4: Enhance the SOCI Act’s practical application by emphasising recovery and resilience

The ABA considers that the SOCI Act’s principles-based design is generally capable of accommodating new and emerging threats without the need for significant expansion of scope. The framework provides sufficient flexibility to adapt to evolving technologies and threat vectors. As cyber incidents become more sophisticated, members note the growing importance of focus not only on notification and compliance processes, but on resilience and recovery outcomes, including the ability of asset operators to restore critical services.