24 December 2025

Dr Jill Slay AM

SOCI Act Independent Reviewer

Department of Home Affairs

via email to: SOCI.Independent.Review@homeaffairs.gov.au

Dear Dr Slay

Independent Review of the Security of Critical Infrastructure Act 2018

The Australian Small Business and Family Enterprise Ombudsman (ASBFEO) welcomes the opportunity to comment on the Department of Home Affairs' Independent Review of *the Security of Critical Infrastructure Act 2018* (SOCI Act)[1].

ASBFEO supports the objectives of the SOCI Act in safeguarding national resilience. However, the current framework may impose disproportionate compliance burdens on small and family businesses, particularly through:

- legislative complexity and layered obligations
- contractual flow-down of compliance requirements from large entities to small and family businesses suppliers and service providers.

Protecting critical infrastructure is essential, but the current framework risks marginalising small and family businesses that are integral to its function. Adopting proportional, resource-sensitive reforms will create a resilient ecosystem where national security and economic prosperity are mutually reinforced.

ASBFEO advocates for a right-sized regulation that balances national security with economic sustainability:

- exempt small and family businesses below a clear threshold - businesses under $5 million annual turnover should be exempt from mandatory positive security obligations
- proportional compliance framework, where obligations are scaled based on size and inherent risk profile.
- provide guidance and support by developing tailored compliance templates and resources for small and family businesses.
- minimise contractual flow-down - establish guidelines to prevent disproportionate cascading obligations from larger entities to small suppliers.

[1] Department of Home Affairs, *Consultation on the Independent Review of the Security of Critical Infrastructure Act 2018, accessed on 2 December 2025, retrieved from https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/consultation-on-an-independent-review-of-the-soci-act-2018*

Key issues impacting small and family businesses (SFBs)

Disproportionate Compliance Burden

> Small and family businesses face significant governance costs, often up to $40,000 upfront and substantial diversion of key personnel from business operations to administrative and reporting compliance. Non-risk-based Positive Security Obligations (PSO) impose the same compliance burden regardless of business size or risk profile.

The expansion of the SOCI Act has inadvertently captured many small and family businesses delivering essential services but lacking the resources of larger entities. While the PSOs, such as mandatory cyber incident reporting and the Critical Infrastructure Risk Management Program (CIRMP), are manageable regulatory requirements for resource-rich firms, their cascading impact creates a disproportionate and more burdensome compliance challenge for small and family businesses.

Cascading Obligations

> Large entities often impose SOCI compliance obligation onto smaller suppliers including small and family businesses who are not responsible entitles under the SOCI Act, creating economic disincentives and undermining supply-chain diversity, particularly harming regional and remote businesses viability.

Cascading white tape occurs when large, regulated entities pass down their statutory compliance requirements (e.g., specific contractual security clauses, detailed audit demands, mandatory platform use) to their smaller, non-regulated small and family business suppliers, often without proportionate compensation or appropriate assistance and support.

Unintended Consequences

> Increased overheads reduce competitiveness of small and family businesses and risk the exit of critical regional service providers and suppliers; undermining resilience objectives of the SOCI Act.

A small and family business supplier (e.g., speciality IT consultancy, a regional maintenance contractor, or a data storage provider) to a major Critical infrastructure (CI) asset owner is required to:

- implement enterprise-grade security controls and governance that significantly exceed their actual operational risk and scale
- invest in compliance certification and reporting systems
- divert owner operators from their core business activities to manage complex reporting and audit requests.

This compliance burden acts as an invisible barrier to entry, imposes hidden costs on small businesses, reduces competition, stifles innovation and raises costs throughout the supply and value chains.

Case study: Regional Tech Services Pty Ltd[2]

A family-owned regional IT managed service provider with eight staff and $2.5 million turnover supports local government, a regional hospital, and utilities. Despite not being a Responsible Entity under the SOCI Act, it must now comply with the hospital's full CIRMP and incident reporting requirements. This imposes an estimated $40,000 in upfront governance costs and diverts the owner-operator for approximately 1.5 days per week to non-billable compliance tasks.

Higher overheads drive up fees, eroding competitiveness against national firms and threatening viability, potentially leaving the hospital reliant on distant providers. These cascading compliance demands create disproportionate economic pressure on a low-risk, critical regional small business.

Recommendations

The below recommended reforms will strengthen security by supporting small and family businesses.

Recommendation 1: Right-sized regulation framework

- Exempting Small and family businesses below a clear annual turnover threshold (e.g., $5 million) from mandatory PSOs.
- Creating a Simplified Critical Infrastructure Security Program (SCISP) for necessary compliance that is fit for purpose.

Recommendation 2: Immediate measures and government support

- Provide free government-developed digital compliance tools to reduce consultant reliance and support the Productivity Commission's 'tell us once' initiative from the Economic Reform Forum.
- Introducing mandated contractual clauses to limit the flow-down of white tape.

Right-sized regulation framework

To maintain national security while supporting small and family businesses, the SOCI Act must incorporate a specific, scalable framework for smaller entities, focusing on the principle of proportionality.

The Australian Government should establish a clear small and family businesses threshold for mandatory PSOs. This would create a 'safe harbour' for the majority of small and family businesses, ensuring the SOCI Act targets only entities with the material operational or data-related capacity to cause a 'relevant impact' at a national level.

Mandatory PSOs (like CIRMP and mandatory cyber incident reporting) should not apply to businesses below a certain annual turnover threshold (e.g., $5 million for non-asset-owning entities, and/or fewer employee than 20) unless they are formally designated as a System of

[2] The company name has been altered to protect the identity of the original entity.

National Significance (SoNS).[3] The Australian Government should introduce a single small and family business definition and introduce a simplified compliance tier.

For small and family businesses that must comply (due to SoNS or a low-turnover, high-risk asset ownership), replace the complex CIRMP with a Simplified Critical Infrastructure Security Program (SCISP).[4] SCISP should focus on 10–15 core cyber hygiene controls, use plain language, and rely on annual self-declaration rather than board-approved reports, significantly reducing compliance burden and lowering operating costs.

Immediate measures and government support

The Australian Government should provide free government-developed digital compliance tools to reduce reliance on consultants. This will support the Productivity Commission's 'tell us once' initiative from the *Five Pillars of productivity inquiries*.[5]

The Cyber and Infrastructure Security Centre should provide free, simplified digital templates for small and family businesses enabling standardised compliance, reducing reliance on costly consultants, and directly addressing the $40,000 compliance cost identified in the case study. The following resources are examples of what could be developed:

- develop a mandatory cyber incident reporting template could be developed as an online resource with a clear structured incident reporting form including drop-down menus and simple definitions.
- develop a SOCI risk management program template. These templates could rely on pre-filled data with customisation options that would support minimum baseline requirements. The template should focus on 'fill-in-the-blank' ease of use, if possible, with a function that could indicate possible errors and require correction.

The Australian Government should introduce a government-backed supply chain indemnity clause, enabling small and family businesses to resist unreasonable customer demands and promote fair and proportionate risk sharing.

This may include model contractual clauses that critical infrastructure entities must use for small and family business suppliers. This will limit the supplier's liability and scope of mandated compliance to the requirements of the SCISP, preventing the uncompensated flow-down of cascading white tape.[6]

---

[3] Allens, *New cyber incident response obligation for Australian Organisations.* 4 December 2024. Accessed on 12 December 2025, retrieved from https://www.allens.com.au/insights-news/insights/2024/10/new-cyber-incident-response-obligations-for-australian-organisations/

[4] KPMG, *SOCI Act: Protecting the Security of Critical Infrastructure. Accessed on 12 December 2025, retrieved from https://kpmg.com/au/en/insights/risk-regulation/critical-infrastructure-reforms.html*

[5] Productivity Commission (PC), *Five pillars of productivity inquiries*. Accessed on 10 December 2025, retrieved from https://www.pc.gov.au/inquiries-and-research/five-productivity-inquiries/
Australian Small Business and Family Enterprise Ombudsman (ASBFEO), *Productivity Commission 5 Pillars Interim Reports.* 16 September 2025. Accessed on 10 December 2025, Retrieved from https://www.asbfeo.gov.au/sites/default/files/2025-09/Productivity%20Commission%205%20Pillars%20Interim%20Reports.pdf

[6] Australian National Audit Office (ANAO), *Maximising Australian Industry Participation through Defence Contracting*. 20 May 2025. Accessed on 12 December 2025, retrieved from

The Australian Government should consider establishing a SOCI Act small and family businesses liaison to provide a low-cost, non-litigious pathway to address excessive cascading compliance burdens. Further the government could consider expanding the role of the ASBFEO to receive and mediate disputes related to disproportionate SOCI Act compliance demands on small and family businesses from larger entities.

The protection of critical infrastructure is paramount. However, the current framework risks marginalising and eliminating the small and family businesses that are integral to its function, particularly in regional Australia. Adopting these proportional, resource-sensitive recommendations will create a resilient ecosystem where national security and economic prosperity are mutually reinforced.

If you require any further information, please do not hesitate to contact the Policy and Advocacy team via email at [redacted]

Yours sincerely

[redacted]

[redacted]

[redacted]

https://www.anao.gov.au/work/performance-audit/maximising-australian-industry-participation-through-defence-contracting

Black Rome LLP, *Flow-Down Clauses: Best Practices.* 16 August 2022. Accessed on 15 December 2025, retrieved from https://www.blankrome.com/publications/flow-down-clauses-best-practices