[redacted]
www.consultaustralia.com.au
ABN 25 064 052 615

22 December 2025

Dr Jill Slay AM
Independent Reviewer
Independent Review of the SOCI Act
Submitted via online submission link

Dear [Name],

**Submission – Review of the Security of Critical Infrastructure Act 2018**

Consult Australia is the industry association representing consulting businesses in design, advisory and engineering, an industry comprised of over 58,600 businesses across Australia. This includes some of Australia's top 500 companies and many small businesses (97%). Our members provide solutions for individual consumers through to major companies in the private sector and across all tiers of government. Our industry directly employs over 285,000 people in architectural, engineering, and technical services and many more in advisory and business support. It is also a job creator for the Australian economy; the services we provide unlock many more jobs across the construction industry and the broader community.

Our members have raised significant issues with the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act), especially the unintended consequences of the Act and its implementation. Concerns include the following:

- Critical asset clients are imposing stringent, and sometimes unworkable obligations on consultant businesses, despite those businesses not being directly subject to the SOCI Act.
- The drafting of the SOCI Act is very broad without an explicit exemption for offshore supply chains.
- The data sovereignty of businesses is impacted as critical asset clients fail to take into consideration the global nature of businesses.
- The cyber security of businesses is at risk as critical asset clients require copies of corporate recovery plans.
- Critical asset clients are imposing intrusive audit rights on consultant businesses.

Members have advised that the way that critical infrastructure asset owners/managers manage SOCI obligations is to essentially 'back-to-back' their obligations with their consultant suppliers. That is, whatever the asset owner has said it will do as part of its SOCI obligations (such as have measures in a cyber risk management plan), the owner requires the consultant to do as well. The asset owner then requires the consultant to indemnify the owner for any failure to meet those obligations (whether within the consultant's control or not). This in not appropriate because:

- the legislative intent is to make those with interests in the assets responsible to manage the risk, not businesses and individuals further down the supply chain with less oversight of the risk.

- the obligations are usually quite onerous and much more extensive than what an average consultancy business would have in place.

The way the SOCI Act has been implemented could dissuade consulting businesses from providing services to critical asset clients and hinder collaboration across the Australia and New Zealand region. We recommend that the SOCI Act be amended and critical asset clients are encouraged to apply a risk-based approach to classifying critical assets, rather than a one-size-fits-all method.

Consult Australia members have noticed an increase in contracts containing onerous SOCI obligations. While consultants aren't directly subject to the SOCI Act, many government agencies and utilities that are subject to the SOCI Act are imposing obligations requiring the consultant to go to significant lengths to ensure compliance with the SOCI Act. This is usually regarding recovery plans and the storage of data and IT system set up. Often attached to the SOCI cyber security requirements are intrusive audit rights. For example, some client contracts state that the client can audit upon reasonable notice and the consultant bears the cost of the audit.

**Recovery plans**

Clients often include obligations on a business to provide a copy of its cyber security incident response and disaster recovery/business continuity plan, as well as warrant that the consultant would implement very specific cyber measures in the case of a cyber-attack. However, providing this plan to a client is highly prejudicial to the consultant's own cyber security, because if the client is subject to a breach, then the bad actors attacking the client also hold a roadmap as to how to attack the consultancy business too. Essentially the business is putting at risk their own cybersecurity as the business no longer has control over copies of pans. It is unclear how the client ensures the plan is held securely, or how long the client holds onto the plan.

The result is that the nature of the risk management measure required by the client appears to be antithetical to the law's purpose.

When this is pointed out to clients, consultants are given assurances that the client will never actually ask the consultant to follow the very specific cyber measures. Clients seem to believe that the SOCI Act requires this – rather than having a more nuanced and risk-based approach. Clients could discharge their obligations by requiring service providers and suppliers to agree to have 'reasonable' measures and procedures in place, having regard to the business size and expertise.

For example, it is recommended that instead of imposing such obligations on consultancy businesses, critical asset clients request consultants to meet a certain maturity level from the Essential Eight Maturity Model as developed by the Australian Signals Directorate. The needed maturity level of a business should be determined by considering the services provided and the project. This model provides a useful baseline and is updated regularly, having three target maturity levels.

Consult Australia would be pleased to discuss this in further, to identify how different businesses (for example global/local and multidisciplinary/specialists) could meet the different maturity levels. For example, it might be most appropriate for asset owners to require a Maturity Level One but choose certain individual requirements of a higher maturity level for the project duration relevant to project services. This could be more efficient and

cost-effective for consultant businesses, instead of implementing all Maturity Level Two requirements over its entire business.

**Storage of data and IT system set up**

The SOCI Act does not exclude offshore supply chains, and the concept of foreign control in a critical asset owner's supply chain is gaining attention and requires further exploration to ensure that critical asset owners are not unreasonably limited in finding the right suppliers of professional services. The critical aspect is for asset owners to identify risks and manage them accordingly. However, instead of applying a risk-based approach, Consult Australia members have seen critical asset clients impose stringent and/or unworkable obligations in their contracts with service providers.

As a result, data sovereignty is a significant concern for consultant businesses as critical asset clients require that all data is maintained in Australia. These contract clauses are an issue for many consultant businesses given the global nature of their business. Consultants have had to set up separate IT systems to ensure data is not stored or transferred offshore. Noting that clients often have a 'take it or leave it' approach to contracts, so there is little, if any room, to negotiate. Members have advised that they would be able to build far greater resiliency into systems without the ever-increasing restrictions on where data could be stored. Consult Australia recommends that carve-outs to data sovereignty clauses be introduced for consultant businesses providing services to critical asset clients, an example of such a carve-out clause is:

> *The Supplier/Consultant must take all reasonable steps to protect any personal information obtained in the course of supplying the Services as specified in the Privacy Act 1988 (Cth) and must provide all reasonable assistance to assist [Client] to comply with all Australian privacy laws.*
>
> *In respect of any of the Data, the Supplier/Consultant must not*
>
> *(i) host Data,*
> (ii) *transfer Data (other than to [Client]),*
> (iii) *permit the transfer to or access by a person outside of Australia of Data (save for the Supplier's/Consultant's personnel working out of offices in its international network) , or*
> (iv) *permit access to the Data by any third party without [Client's consent].*

**Cyber insurance**

Critical asset clients often require the consultant business to confirm it has cyber insurance. However, businesses have been advised that providing evidence of cyber insurance is enough to make a business an attractive target for cyber criminals, because the bad actors assume there will be a bucket of money available to pay ransoms etc.

**Our recommendations**

In conclusion we make the following recommendations:

- Critical infrastructure asset owners should take responsibility for critical infrastructure, rather than passing responsibility to suppliers, through onerous contract clauses.
- The SOCI Act and/or guidance material should emphasise the need for critical infrastructure asset owners to take a risk-based approach and dissuade the simple passthrough of risk.
- Critical infrastructure asset owners should reassess the audit requirements imposed on suppliers.
- Critical infrastructure asset owners should seek the supplier's maturity level against the Essential Eight Maturity Model rather than require businesses in their supply chain to agree to specific cyber security measures and provide commercially sensitive information about the business' risk management processes.
- Critical infrastructure asset owners should introduce as standard, carve-outs to data sovereignty clauses for consultant businesses, an example of such a carve-out clause is:

  *The Supplier/Consultant must take all reasonable steps to protect any personal information obtained in the course of supplying the Services as specified in the Privacy Act 1988 (Cth) and must provide all reasonable assistance to assist [Client] to comply with all Australian privacy laws.*

  *In respect of any of the Data, the Supplier/Consultant must not*

  *(v) host Data,*
  (vi) *transfer Data (other than to [Client]),*
  (vii) *permit the transfer to or access by a person outside of Australia of Data (save for the Supplier's/Consultant's personnel working out of offices in its international network) , or*
  (viii) *permit access to the Data by any third party without [Client's consent]*.

- Critical infrastructure asset owners should reexamine the cyber insurance requirements and proof asked for by consultant businesses.

I invite you to contact me directly at [redacted] for more information or to arrange a meeting to discuss.

Yours sincerely,

[redacted]