Proposal to Include Critical Technology Service Providers under the SOCI Act

Summary

The Security of Critical Infrastructure Act 2018 (SOCI Act) has significantly strengthened Australia's resilience against threats to critical infrastructure. However, the Act currently focuses on asset owners and operators within defined sectors, without explicitly addressing systemic risks posed by critical technology service providers. Global regulatory trends, such as the EU's Digital Operational Resilience Act (DORA), now recognize hyperscale cloud providers and other ICT service providers as critical to financial and operational stability. These providers underpin essential services across multiple SOCI sectors, creating concentrated dependencies that, if disrupted, could have cascading national impacts.

Recommendations

I recommend amending the SOCI Act to introduce a designation framework for "Critical Technology Service Providers" (CTSPs), subjecting them to proportionate security obligations and oversight. This would align Australia with international best practice, mitigate systemic risk, and enhance supply chain resilience.

Amend the SOCI Act to:

1. Define or recognise Critical Technology Service Providers (CTSPs): Entities delivering ICT services essential to the operation of critical infrastructure sectors.
2. Establish Designation Criteria: Based on systemic impact, concentration risk, substitutability, and reliance across sectors (similar to DORA Article 31).
3. Introduce Positive Security Obligations for CTSPs: Including risk management programs, incident reporting, and supply chain assurance.
4. Enable Government Oversight: Through a lead regulator that is empowered to assess resilience and enforce remediation.

Further reading:

1. https://www.esma.europa.eu/press-news/esma-news/european-supervisory-authorities-designate-critical-ict-third-party-providers
2. https://cloud.google.com/blog/products/identity-security/supporting-customers-as-a-critical-provider-under-eu-dora