SUBMISSION

Independent Review of the Security of Critical Infrastructure Act 2018

Summary

In my roles over the last several years, within specialist Security Installers/Integrators and ICT Integrators, supporting numerous Critical Infrastructure (CI) Asset Owners across various sectors has provided valuable insights into how the SoCI Act is functioning and is being implemented.

I consider that overall, the SoCI Act has achieved its goal of increasing awareness within the Executive level of CI Assets, however this understanding has not fully passed through to the day-to-day operations teams which continues to lead to obligations not being communicated or enforced adequately in tenders and contracts with Supply Chain partners.

There also needs to be an alignment across Government and Critical Infrastructure of frameworks, especially for the Supply Chain, to reduce duplication of costs and processes. Once these basics are fixed, we can then look at our future environment.

The SoCI Act needs to consolidate on what it has already achieved and build a stable foundation for the implementation of further measures to address the evolving threat environment Australia will face in the coming years and decades.

Is the SoCI Act achieving its intended objectives

Noting the Act is focused on the actual Owners and Operators of Critical Infrastructure in Australia, I consider the Act as a whole, is achieving its intended objectives in lifting awareness of security threats across all sectors and has driven a much greater understanding of the interconnectivities across all sectors in general.

I cannot comment on how Owners and Operators perceive the Acts performance, however as a supply chain partner for many Asset Owners across various sectors, and from participating in government led engagement activities, it is clear that the overall awareness of the threat environment, the need for planning for recovery from significant incidents, and the overall need to uplift security across Critical Infrastructure is starting to sink in with Asset Owners.

There is still work to be done. The focus within the Act on Asset Owners identifying the risks pertinent to their key Assets and those that have access to those Assets is long overdue.

Is the SoCI Act functioning as intended

In regards to uplifting awareness amongst Asset Owners of the need to uplift security, plan for incidents and look at how they might recover, then in general Yes.

In regards to Supply Chain management I consider this is still lagging.

Some CI Asset Owners and Operators are beginning to engage with their Supply Chain partners; however, others are not. Most CI Assets Owners that I have dealt with are still struggling with the requirements around identifying their Critical Workers and advising their contracted workforce accordingly.

Is the SoCI Act having any unintended consequences

In short, yes. I will break down some of the key issues which have impacted operations that I have been involved in for consideration below.

Background Checks and Critical Worker Management

Under the SoCI Act CI Asset Owners and Operators must detail their proposed Background Check requirements for 'critical workers' in their CIRMP, and these Checks can either be through AusCheck or 'in-line' with the requirements under the AusCheck Act 2007. The AusCheck Act at Part 1, Section 5 defines background checks under the Act as follows:

> A ***background check***, in relation to an individual, is an assessment of information relating to one or more of the following:
>
> (a) the individual's criminal history;
>
> (aa) if required or permitted under a regulation made under subsection 8(3):
>
> (i) whether the individual has been charged with a serious offence; or
>
> (ii) whether a charge for a serious offence has been resolved in relation to the individual;
>
> (b) matters relevant to a security assessment (as defined in subsection 35(1) of the *Australian Security Intelligence Organisation Act 1979*) of the individual;
>
> (ba) if the background check is conducted for the purposes of paragraph 8(1)(a)—matters relevant to a criminal intelligence assessment (as defined in section 36A of the *Australian Crime Commission Act 2002*) of the individual;
>
> (c) the individual's citizenship status, residency status or the individual's entitlement to work in Australia, including but not limited to, whether the person is an Australian citizen, a permanent resident or an unlawful non-citizen;
>
> (d) the identity of the individual.

I note that section 5(b) refers to an assessment under subsection 35(1) of the ASIO Act 1979, which appears to indicate that an ASIO Assessment can only be requested by, or supplied to, a Commonwealth Agency or to an authorized State Agency.

This appears to lock CI Asset Owners and Operators into using the AusCheck process to comply with the Background Check requirements under the SoCI Act.

I also note that the AusCheck process does not fully align with the AS4811:2022 Worker Screening requirements which are mandated as part of the Pre-Vetting Screening requirements for AGSVA (Australian Government Security Vetting Agency) Security Clearances.

I further note that there are significant numbers of contractors who support CI Assets who are also involved in supporting Defence and Defence Industry and are required to maintain DISP (Defence Industry Security Program) Membership. DISP Members are mandated to undertake AS4811:2022 Worker Screening (Pre-Vetting Screening) on all staff, however these Checks currently are not recognized by AusCheck for the preliminary Check process and there is no ability within the AusCheck process for a DISP Member to provide evidence of their staffs AS4811 Screening to AusCheck as part of the Critical Worker Permit process.

Remedy

I believe there needs to be an alignment of Background Check requirements across all Government and Critical Infrastructure environments. Having a single standard which establishes minimum requirements for entry level into the Government and Critical Infrastructure sectors, then provides a structured approach to increased requirements is needed.

Noting that Defence has mandated AS4811:2022 for all DISP Members, and this aligns with requirements under the PSPF (Protective Security Policy Framework), I would urge the following be implemented across CI.

1. The Act details that Background Checks must align with AS4811:2022 requirements for all staff and contractors engaged by CI Asset Owners.
2. Identified Critical Workers, listed in the Assets CIRMP, need to also hold a valid Critical Worker Permit through AusCheck.
3. Contractors who provide Critical Workers to CI Assets, and are DISP Members, are provided with access to the AusCheck Portal to lodge Critical Worker Permit applications and manage their identified Critical Workers.
    a. DISP Members upload their valid AS4811 Screening Certificate and National Police Check to the Portal and AusCheck request the ASIO Check as required under the Act.
    b. DISP Members can also manage applying for ASIC (Aviation Security Identification Card) & MISC (Maritime Security Identification Card) Cards for relevant staff through this process.
4. DISP Members manage their Security Clearance requirements for access to CI Assets which require Critical Workers to also hold a Security Clearance.

Supply Chain Management

Currently under the Act there is a requirement for CI Asset Owners and Operators to address risks in their supply chain as part of their CIRMP obligations, however it is up to the Asset Owner or Operator as to how they manage these risks, and this is open to interpretation.

There is no actual framework for Supply Chain partners to work within or comply with. Each CI Asset Owner is responsible for determining what security measures or standards are applicable to their operations and communicate this to their contracted providers. This process leads to ambiguity, duplication of processes, delays and significant increases in costs for the contractors when the CI Asset Owner finally begins implementing measures.

This places a significant burden upon contracting businesses which are in the supply chain and provide 'critical workers' to various CI clients across different sectors for core services such as electrical, water, IT, security, HVAC, and other critical maintenance, as there is currently no single framework to work across sectors and clients.

Take for instance a security contractor who is contracted to install and maintain Access Control and CCTV systems for CI Clients. The security contractor has contracts with various CI Operators across several sectors.

Client A's CIRMP details:

- A Police Check and proof of Right to Work in Australia, an ISMS aligned to ISO27001 (without certification).

Client B's CIRMP details:

- An AusCheck Critical Worker Permit, Police Check & proof of Right to Work in Australia, with no information security management requirements.

Client C's CIRMP details:

- AS4811 Background Screening, Compliance with the ASD Essential 8 or GDPR, Supply Chain Risk Assessments.

Client D's CIRMP details:

- DISP (Defence Industry Security Program) Membership, AusCheck Critical Worker Permit, ISO27001 Certification.

For the contractor who is providing 'critical workers' to just 4 clients across different sectors, or even in just 1 sector, the contractor has multiple compliance requirements for the same activity, often with duplicated costs and significant processing times involved for the 'critical workers' themselves. The mismatch of requirements and duplication of processes leads to:

a. Duplication of processes and checks.

b. Increased costs associated with vetting 'critical workers', including time spent preparing and submitting documentation for background checks which employers have to cover without being able to charge for it.
c. Increased delays in getting 'critical workers' approved to access sites.
d. Gaps in information management processes between clients.

It also highlights that contracted services attempting to support clients across various sectors have to in some way achieve certification/compliance to multiple cyber standards to enable them to be considered for works with different clients.

Remedy

To remedy the above issues the Act should establish a compliance framework for the supply chain partners supporting CI Assets similar to the DISP (Defence Industry Security Program) framework which supports Defence and Defence Industry.

If we're serious about strengthening the supply chain supporting CI Assets, including the Defence Industry captured under the SOCI Act, why not just extend the DISP Program to include Critical Infrastructure and provide support to Defence Security to expand the DISP Team to support this. It may involve creating a *NEW* Membership category of Associate Member, which would sit below Entry Level Membership of the program where applicants would need to meet the following requirements:

i. All Governance requirements of DISP Membership implemented.
ii. Background Screening to the AS4811:2022 Standard implemented.
iii. ISMS aligned to ISO27001 or system compliant to Maturity Level 1 of the ASD Essential 8.

Once a Supply Chain Partner of a CI Asset attains DISP Associate Member status, they can then apply for access to the AusCheck Portal to lodge and manage Critical Worker, ASIC & MISC Permits for their Team.

I know, it's radical thinking to suggest Home Affairs and Defence collaborate but surely given the nature of the threat facing Australia and our Critical Infrastructure it's time for a truly collaborative approach to this issue.

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

Definitely. There will always be emerging threats which legislation will lag behind.

Just in the last 2 years we have seen significant changes in threat vectors which have the potential to impact Critical Infrastructure from the use of drones (aerial, maritime and land based) to undertake attacks, surveillance and espionage, to the advancements in AI to the point of cybercriminals and Nation State Actors utilising AI to build malware and phishing campaigns, and now the potential for AI to actually

develop, deploy and implement full-fledged cyber campaigns independent of human interactions.

With the potential deployment of Defence related technology, i.e. C-UAS (Counter-Unmanned Aerial Systems) technology, to protect CI Assets, the need for CI security to align with Defence security requirements is now crystalising. The alignment between CI and Defence can no longer be ignored and we need a single compliance framework for everyone to work within.

Australia's CI Act aligns nicely with our Critical 5 Partners CI legislation and schemes but needs further refinement to fully align with our Partners programs. I note that both the US & UK legislation includes Emergency Services and Nuclear Industry as separate distinct sectors. I also note that the United States has recently completed its review of the AUKUS Program and has confirmed that the Program must continue. To ensure that Australia is fully aligned with our AUKUS Partners, it is paramount for Australia's designated CI Sectors to expand to include all sectors captured under both the US & UK legislation.

The inclusion of Emergency Services as a distinct sector under the Act will enable an uplift in the overall security of infrastructure which supports Australia's ability to respond to major incidents and natural disasters. The Emergency Services sector must include the State & Commonwealth Agencies such as Police, Ambulance and Fire Services, but also needs to include our Volunteer Agencies such as the State Emergency Services (SES), Bush Fire Brigades and Volunteer Rescue Associations (VRA) as these three Services are critical in supporting Australian communities in times of need. Due to the support these Services provide to the permanent Emergency Services and their existing connections to those Services systems, securing their infrastructure is a paramount requirement.

In relation to Nuclear, noting that the AUKUS Program is going to proceed at full speed, it is paramount that Australia embraces a nuclear future now. The only way a nuclear industry can gain public support is by establishing a very strong security compliance framework to support it.

Australia already has world leading nuclear specialists in the field. With the advent of Small Module Reactors (SMR's) and the ability for these to now be deployable and moved to support industry, then the opportunities to expand Australia's CI infrastructure from key population areas to regional locations to generate the power needed by energy hungry CI Assets opens up vast areas of the country for resilience of our CI Assets to support employment growth and reduce land demands within major cities.

There needs to be a much greater focus on Supply Chain risks, not just within the Critical Infrastructure environment, but across our economy. Financial pressures in our economy are driving more and more businesses which support CI Assets to the wall. Asset Owners and Government will always try to get the biggest bang for the least financial outlay, with contracts still being awarded to contractors who may not meet all

compliance requirements but can provide services at a cost which is much more palatable to procurement teams who focus on cost savings to meet KPI's.

Refinement and enforcement of existing Frameworks to enforce compliance obligations as part of the procurement processes must be looked at to help lift overall security in the Supply Chain. Contractors need to know that they will not be unfairly treated in the procurement process if they actually cost required security compliance into tender responses.

We need to look at our essential workforce requirements especially for specialist 'Critical Worker' roles, not just Cybersecurity, but also Electricians, Cablers, Security Technicians, Welders, HVAC Technicians, etc. We need to be training up new Apprentices and providing incentives to keep them in these roles. We need more women and girls in these roles; we need to seriously look at our supposed 'unemployable workforce' in the disability sector as a priority and provide much more support to businesses to take on candidates who need greater support in the workforce.

God forbid there is a geopolitical incident in our region in the short term which would require a mobilisation to support long term military operations. If such an event occurred, how does the Supply Chain supporting CI Assets still function with a reduction in workforce of 30% or more?

We need to secure onshore manufacturing of 'critical components' from semi-conductors to cabling, from steel to engine components and pipelines. We need fuel storage and processing. We need to secure our food production areas and not let these industries be pushed out of productive lands by housing or other infrastructure.

We can't just rely on legislation. We need a posture change in our overall approach to Critical Infrastructure and National Security. We need, dare I say it, a philosophical change from a Chamberlainesque posture to a Churchillian vision for our future.

The SoCI Act is only one element of this wider discussion.

[redacted]

9 December 2025