Australian Telecommunications Alliance

Setting The Standard.
Driving Progress.

19 December 2025

Dr Jill Slay AM
Independent Reviewer
Security of Critical Infrastructure Act 2018

Via email: SOCI.Independent.Review@homeaffairs.gov.au

Dear Dr Slay,

RE: STATUTORY REVIEW OF THE *SECURITY OF CRITICAL INFRASTRUCTURE ACT 2018*

Thank you for the opportunity to provide a submission for the Independent Review of the *Security of Critical Infrastructure Act 2018* (SoCI Act).

Given the time of the year and the due date, we confine our feedback to some high-level comments. Members may make individual submissions.

General comments

We would like to see improved clarity and simplicity in the SoCI regime. We remain cognisant of the risk that there may be misalignment between government expectations and industry implementation.

Members report a continued reticence from Government to indicate what 'good' or 'sufficient' practice might look like under the regime. While critical infrastructure owners (and their supply chains) require sufficient flexibility to design risk management approaches that best suit their needs, such guidance could assist critical infrastructure owners and operators to minimise the risk of expending significant capital associated with system upgrades and overhauls for potentially only marginal or incremental uplift to security or resilience. We also acknowledge the advisories from the Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) to inform cyber risk assessments that are part of SoCI regime, and the role that this plays in the evolving understanding of the regime.

While we applaud the guidance provided by the Critical Infrastructure Security Centre (CISC) and the Department of Home Affairs (Department) to date, we consider guidance of the detail and utility used by regulators, such as the Australian Securities and Investment Commission (ASIC) (see e.g., *ASIC Regulatory Guides*), may be instructive, both in their use of worked examples, and intention to provide interpretative effect to industry. For example, the CISC could issue more constructive guidance based on their sample audit reviews to give industry clear examples of what compliance or non-compliance could look like. It should be noted that such guidance ought not to curtail a regulated entities freedom to develop alternative risk management approaches which it deems compliant with all applicable regulations. In essence, members seek guidance that they may use as they see fit without such guidance amounting to an additional layer of quasi regulation.

Suppliers (e.g., vendors) to critical infrastructure owners or operators are also adversely impacted by the limited guidance. Requirements of the SoCI regime may be passed downstream to suppliers either directly under contract (through broad, ambiguous clauses requiring compliance to the regime in whole or part), or indirectly through mandatory adoption of policies and frameworks (for example, forced adoption of a security framework not necessarily mandated in the regime).

The practical effect of the limited guidance and clarity may be an inconsistent approach from critical infrastructure operators or owners in how they view the application of the SoCI regime on the operations of their suppliers downstream.

Australian Telecommunications Alliance
A Level 25 / 100 Mount St, North Sydney NSW 2060
P 02 9959 9111
E info@austelco.org.au
W austelco.org.au
ABN 56 078 026 507

ATA

It is cumbersome, costly and particularly difficult for suppliers to manage inconsistent requirements when they supply to more than one critical infrastructure owner and such requirements require operational changes and/or capital investment. Clarity and constructive guidance could foster a level of consistency and enable suppliers to better support the intent of the regime.

Improved cooperation/coordination

Our members are often subject to a multitude of regimes that either directly arise from cyber security regulation or relate to the security of networks and information more broadly. They are subject to *the Telecommunications Act 1979*, *Telecommunications (Interception and Access) Act 1979*, SoCI Act, and the *Privacy Act 1988*. We (ATA) assume that some are also subject to additional obligations that arise for systems of national significance (SoNS). Members may also be certified under the *Hosting Certification Framework* (HCF).

Most of these regimes come with significant reporting and record-keeping obligations. Entities also undergo regular audits.

Members report that they are subject to multiple overlapping audits from the Department each year. These ought to be streamlined: where information is gathered by different teams with the Department (if this is indeed necessary), such information ought to be held in a central repository available to other teams within the Department . This could substantially reduce the regulatory burden (and cost) associated with the audits, both for the audited entity and the Department.

Quantum

While the CISC provides guidance on AI in its Factsheet for Critical Infrastructure, Artificial Intelligence in Critical Infrastructure, it may be worth giving consideration to addressing other emerging technologies, such as quantum, though separate guidance.

Operational technology (OT) vs information technology (IT)

At its core, the SoCI Act establishes a regime concerned with the operational technology (OT) underpinning critical infrastructure, and the people with access to it.

Not all compliance frameworks equally apply to OT, making it potentially more difficult to establish equivalence (see TSRMP Rules r 11(5) and CIRMP Rules r 8(5)) with respect to OT. Further, the boundary between IT and OT is widely regarded as blurring.

We would like to see specific guidance on the treatment of OT (as well as IT with OT like qualities) with respect to regulated entities establishing equivalence of security frameworks. This could include providing greater flexibility to entities to apply a mixture of frameworks and controls appropriate for their circumstances and environments. In our view, this remains a significant gap left unaddressed by the SoCI regime in its present state.

Definitional concerns

The definition of 'critical telecommunications asset' in section 5 of the Act remains excessively broad due to the inclusion of the defined term 'asset', which extends to a system, network, facility, computer, computer program, computer data, premises and *any other thing* [emphasis added]. While guidance materials have proven helpful, the existing definition does not provide sufficient certainty to responsible entities about excluded assets, and this certainty is necessary for responsible entities to understand their own obligations under the Act as well as the obligations of other entities in their supply chains. We suggest the definition of critical telecommunications assets

be amended to remove this uncertainty and more intentionally capture the infrastructure, systems, and services that are critical to the availability, integrity, or confidentiality of telecommunications within Australia.

Similarly, the definition of 'data storage systems' has a very wide scope which muddies what is in fact critical to operations. The definition captures systems that 'process' business critical data. There is no definition given for 'process' so we assume this includes transporting data from point A to point B, regardless of whether there is any transformative effect on the data. Applying this definition of 'process' means most systems in a telecommunications provider technology stack are in scope, and entities cannot focus on their crown jewel systems. We consider this can have the unintended effect of entities losing focus on what systems are truly critical to operations.

As the regime develops past its infancy into a more mature and better understood framework, it would be good to get clarity (ideally through guidance) as to common understandings between Government and industry.

For instance, we remain concerned that there may still be uncertainty about what level of granularity should be adopted in identifying critical components, and this affects the level at which controls may be adopted. As the CISC and the Department receive information from each critical infrastructure sector, we think it would be beneficial for it to share, through industry guidance, its preferred (or at least the most common) levels of granularity which are applied.

Further guidance would support industry's understanding of threshold questions such as those relating to the 'materiality' of risks and the threshold for a 'relevant impact' on an asset that would be reportable as a mandatory 'other' cyber incident. Taken generally, we appreciate that Government is concerned with the sort of risk that affects large numbers of people, large areas of geography or otherwise may significantly and adversely impact the economy or national security. However, this broad understanding exists alongside (and in many cases incongruently with) industry-specific regulatory frameworks that set thresholds for various sector-specific regulatory interventions (e.g., the recent telecommunication regulations applicable to network outages and Triple Zero calls) on the basis of some version of a 'significance' or 'materiality' test. We take the view that, where possible, guidance should be given about whether those industry specific thresholds should be taken as de facto indicia of 'materiality' or whether it is intended to apply some other threshold or degree.

It would also be helpful to see guidance on the interaction of the requirements around 'protected information' with the information sharing requirements contained on other regulatory instruments, e.g., the *Telecommunications (Customer Communications for Outages) Industry Standard 2024* and the *Emergency Call Services Determination 2019*.

We also note that the definition for a 'cyber security incident' in the Act does not align with the *Guidelines for Cyber Security Incidents* published by the ASD's ACSC. It would be helpful for industry if there were alignment on this definition.

In relation to the hazard areas, there is overlap between the definition of physical security hazards and natural hazards. Further guidance as to how these two hazard areas can be distinguished would be helpful.

Members also raised questions in relation to the definition of 'critical workers'. This definition captures a broad range of workers who have incidental physical or privileged access to locations with critical components. This could include workers such as cleaners, reception staff, and contractors delivering goods, because these workers could intentionally or unintentionally cause damage to critical components. However, it seems from the *CIRMP Guidance* on critical workers (page 11), that the Government's intention is for critical workers to include roles such as Chief Information Security Officer and workers with unrestricted administrator rights to systems rather than all workers with incidental physical or privileged access to locations with critical components. The SOCI Act's wording and the guidance do not appear aligned. It would be helpful for the Government to amend the Act or provide further clarification on this point.

We look forward to continuing our constructive engagement with the Department of Home Affairs and all other relevant stakeholders to further uplift Australia's cyber security stance.

If you have any questions or wish to discuss, please do not hesitate to contact me at c.gillespiejones@austelco.org.au.

Kind regards,

Christiane Gillespie-Jones
Deputy CEO

The Australian Telecommunications Alliance (ATA) is the peak body of the Australian telecommunications industry. We are the trusted voice at the intersection of industry, government, regulators, and consumers. Through collaboration and leadership, we shape initiatives that grow the Australian telecommunications industry, enhance connectivity for all Australians, and foster the highest standards of business behaviour. For more details, visit www.austelco.org.au.