

Australian Information Industry Association

Submission on

Streamlining and Modernising the Security of Critical Infrastructure Act 2018

About the AIIA

The Australian Information Industry Association (AIIA) is the nation's peak body for those in the digital ecosystem, leading strategic policy and advocacy to shape a thriving digital sector. Through strong engagement with government, industry, and the broader community, the AIIA ensures the voice of its members informs decision-making on technology, innovation, and digital capability.

Membership provides direct access to influential networks, premium events, and opportunities to collaborate on initiatives with the sector's best and brightest to drive industry growth, improve productivity, and secure Australia's place as a global technology leader. AIIA members access real collaboration, real connections, and real outcomes.

Introduction

The AIIA welcomes the opportunity to comment on the Department of Home Affairs' consultation on Streamlining and Modernising the Security of Critical Infrastructure Act 2018.

The AIIA supports the objectives of the reform package. The SOCI Act has lifted board-level attention to infrastructure risk and established a common language for discussing security and resilience across sectors. Reducing complexity, clarifying uncertain asset boundaries and improving assurance settings are worthwhile goals.

This submission responds to three measures of particular relevance to AIIA members:

- Measure 8 (data storage or processing capture pathways)
- Measure 17 (operations and maintenance and managed service providers)
- Measure 19 (supply chain cyber security assurance).

Measure 8: Data storage or processing capture pathways

The AIIA supports the objective of creating a clearer and more predictable basis for identifying critical data storage or processing assets. However, the proposed facility-based and service-based pathways risk treating commercial scale as a substitute for criticality.

Scale could operate as a screening factor, not as an independent test for SOCI regulation. A large data centre or widely used service may cause significant disruption if unavailable, but this does not necessarily mean that its disruption, compromise or prolonged unavailability would have nationally significant consequences for critical infrastructure, essential government functions, economic stability or national security.

The current section 12F model reflects an important principle: the criticality of a data storage or processing service is generally derived from the critical infrastructure asset and function it supports and the impact of compromise or loss. The consultation paper identifies legitimate concerns about whether providers can determine their regulatory status and whether customer notifications occur consistently. However, it does not demonstrate that the underlying factors of customer regulatory status, downstream use and the criticality of the relevant data or systems are inappropriate. Rather, it demonstrates that these matters may not be visible to providers and are not always communicated effectively.

The AIIA therefore recommends that the Department:

1. introduce a certification-based pathway for relevant Hosting Certification Framework (HCF) certified facilities or services;
2. retain and improve the section 12F(3) notification pathway for providers not already captured through certification; and
3. defer broad facility and service-scale pathways unless evidence demonstrates that material coverage gaps remain after those reforms.

If the Department proceeds with facility-based or service-based capture, scale thresholds should only identify providers or facilities for further assessment. They should not establish criticality without an additional consequences-based nexus.

Certification-based capture

The AIIA supports certification-based capture in principle. HCF certification provides a stronger connection to government security and assurance requirements than general measures of commercial scale. It reflects an assessment that a specified facility, service or environment is suitable for hosting sensitive government information.

Capture should therefore be limited to the particular facility, service or environment covered by the certification. Certification of one facility or service should not

automatically bring a provider's unrelated facilities, services or broader corporate group within scope. Where the relevant facility or service is already captured through HCF certification, a critical infrastructure customer should not also be required to notify the provider under section 12F(3).

Retention and improvement of section 12F(3)

For providers not captured through a HCF-based pathway, the AIIA recommends retaining tenant-derived criticality through an improved section 12F(3) notification process.

The critical infrastructure customer should remain responsible for identifying whether a third-party service supports its business-critical data or systems. The customer is ordinarily best placed to understand how the service is used, why the data or system is important and the consequences that disruption would have for the relevant critical infrastructure asset. The provider is generally better placed to determine which of its facilities, infrastructure and services support the notified arrangement. The respective responsibilities should therefore remain:

- the customer identifies and communicates the criticality of the workload or service dependency; and
- the provider identifies the relevant supporting asset or service and complies with applicable SOCI obligations once captured.

Section 12F(3) already specifies the circumstances that trigger notification and requires the responsible entity to notify the provider as soon as practicable. However, the process could be made more consistent and auditable through practical guidance or a standard notification mechanism, including minimum information requirements and processes for updating or withdrawing notifications. The notification should not require disclosure of the business-critical data itself or unnecessary operational or security-sensitive information.

Facility-based capture

The AIIA does not support automatic capture based solely on rated IT load. The proposed starting point of 1 MW appears particularly broad. The consultation paper acknowledges that this threshold is low relative to industry norms and may capture most commercial data-centre facilities.

A large facility may host substantial volumes of ordinary commercial workloads without being nationally significant. Facility size may indicate concentration, but it does not establish:

- the importance of the workloads hosted;
- the consequences of their disruption;

- the availability of geographic or technical redundancy;
- whether customers could transfer workloads to another facility; or
- the time required to restore or migrate affected services.

The AIIA recommends deferring the facility-based pathway until the effect of HCF-based capture and an improved section 12F(3) process can be assessed. If the Department proceeds with facility-based capture, rated IT load should operate only as an initial screening threshold. As an indicative range, a threshold in the order of 5–15 MW or above would better reflect industry norms than the proposed 1 MW starting point, while continuing to operate only as a screening factor and not as a determinative test. A facility should also be required to satisfy a systemic-significance test demonstrating that its disruption, compromise or prolonged unavailability could materially affect critical infrastructure, essential government functions, economic stability or national security. That test should focus on the function the facility serves and the consequences of its compromise or loss, rather than on scale alone, but should still account for concentration risk, that is, whether the facility hosts multiple critical infrastructure dependencies whose combined loss could be nationally significant even where no single dependency would independently satisfy the test.

Furthermore, rated IT load should be measured by reference to commissioned capacity that is operationally available for customer workloads. Uncommissioned design capacity and future stages of a development should not be included until brought into operation. Separate buildings, halls or sites should only be aggregated where there is material operational interdependence or shared essential infrastructure such that disruption of one component could materially affect the operation or resilience of the others. Common ownership, common management, a shared network operations centre or common security tooling should not be sufficient without evidence of a material common failure mode.

Service-based capture

The AIIA does not support capturing service providers principally by reference to revenue, customer numbers, data volume, employee headcount or similar measures of commercial scale. These metrics may identify popular or commercially successful providers, but they do not necessarily identify services whose disruption would have nationally significant consequences. Customer count is particularly unsuitable because it may capture high-volume, low-consequence services whose disruption would be widespread but would not materially affect critical infrastructure operations.

The AIIA recommends retaining the existing criticality nexus through section 12F(3), rather than introducing a separate scale-based service pathway. If the Department proceeds with service-based capture, the pathway should require both of the following limbs to be satisfied cumulatively.

1. Primary-purpose test

The relevant service must itself be principally a data storage, processing or infrastructure service, such as infrastructure as a service, storage as a service, managed hosting, backup and disaster recovery, or another comparable infrastructure-layer service.

Application-layer software should not be captured merely because storing or processing data is technically necessary to provide the application. Ordinary software licensing, professional services, advisory services and incidental data handling should remain outside scope, consistent with the stated intention of the consultation paper.

2. Criticality-nexus test

The service must support business-critical data or systems for a critical infrastructure asset, and disruption or compromise of the service must be capable of materially affecting that asset. The existing statutory concept of business-critical data should be retained as the starting point and clarified where necessary, rather than replaced with a new and potentially inconsistent concept.¹

Routine corporate and back-office systems should ordinarily remain outside scope unless their disruption would materially impair the operation or continuity of the critical infrastructure asset. Whether a service is captured should depend on the function it performs and the consequences of disruption, rather than on broad product categories or provider size.

The two limbs should be expressly cumulative. Neither the fact that a provider supplies storage or processing services nor the fact that it holds personal, operational or commercially sensitive information should independently be sufficient for capture.

The pathway should also exclude a provider that does not exercise independent operational control over the environment whose compromise could materially affect the security of the relevant asset.

If a scale metric is retained as an additional screening mechanism, Australian-derived revenue from clearly defined in-scope services would be preferable to total customer numbers, global revenue, total data volume or employee headcount. Any such threshold should remain subordinate to the primary-purpose and criticality-nexus tests.

Transition arrangements

We recommend that any entity newly captured under Measure 8 should receive a minimum twelve-month transition period.

¹ *Security of Critical Infrastructure Act 2018* (Cth) ss 5, 12F.

Measure 17: Operations and maintenance and managed service providers

The proposed relevant operator concept represents a significant increase in regulatory burden on industry and a departure from the guiding principle that it is the responsible entity that is to be regulated under the SOCI framework.

Where this reform is nevertheless progressed, it should remain strictly limited to entities that have both practical operational authority and a material operational dependency in relation to a specific critical infrastructure asset or function. Consistent with this position, general-purpose cloud, software-as-a-service, platform-as-a-service, software and platform services should be expressly named as outside scope where supplying technology through which the customer exercises direct operational control over the critical function of the specific asset.

Customer-configured automation and agentic AI

The Department should provide specific guidance for customer-configured agentic AI and automated workflows. Supplying configurable technology, including automation, orchestration or agent-based functionality, should not of itself constitute practical operational authority. A platform provider should not be captured merely because its technology enables a customer to automate a critical process. Capture should depend on the provider's actual authority, involvement and practical control over the deployed workflow.

Any direct duties should be proportionate and limited to matters within the relevant operator's role, knowledge and practical control, while the responsible entity remains primarily responsible for the asset and its CIRMP obligations. In particular, the duty not to materially compromise the asset should be qualified in the operative provision by reference to what is within the provider's actual knowledge/visibility, given that providers of multi-tenant services may have no knowledge of how a customer has configured or deployed the service.

Below the threshold of practical operational authority, responsibility for matters such as change control, audit rights and evidence sharing is properly allocated through contractual governance between the responsible entity and its service providers. The statutory relevant operator concept should complement, not duplicate, this existing allocation of responsibility.

Measure 19: Supply chain cyber security assurance

The AIIA supports in principle Measure 19 and the objective of providing clearer and more consistent expectations for the cyber security assurance of major suppliers.

Critical infrastructure entities already undertake supplier due diligence, with current practices varying considerably. Suppliers may be required to complete multiple bespoke assessments covering substantially similar risks, while other customers rely on recognised certifications, independent assurance reports or shared assessment arrangements. This duplication increases costs for both responsible entities and suppliers without necessarily improving security outcomes. The consultation paper similarly recognises that repeated bespoke assessments can impose a particular burden on small and medium enterprises.

The reform should therefore promote convergence around (and leverage where appropriate) recognised assurance frameworks, proportionate assessment of major suppliers and clear limits on the treatment of sub-tier dependencies.

Recognition of existing certifications and assurance

The AIIA supports recognition of existing cyber security certifications and accreditations as evidence relevant to supplier cyber due diligence and as satisfaction of any new supply chain assurance obligations, including those already referenced in the CIRMP cyber hazard settings.

Mature critical infrastructure entities already conduct this due diligence. However, some entities issue bespoke custom assessments, others accept SOC 2 or ISO 27001 certification, and others rely on third-party shared assessment services. Suppliers therefore answer materially similar questions in different formats for different customers, which imposes cost without improving assurance outcomes. This burden falls most heavily on smaller suppliers.

The reform should drive convergence rather than divergence. The AIIA recommends that CIRMP guidance:

- identify the certifications and accreditations that responsible entities may rely on, and the circumstances in which reliance is sufficient;
- establish consistency in what responsible entities ask of suppliers, so that assurance requests converge on a common set of matters; and
- recognise established international schemes, so that global suppliers are not required to maintain Australia-specific assurance artefacts that duplicate assurance already provided.

Recognition should be scheme-agnostic and criteria-based, as proposed, with entities able to leverage existing, suitable assurance mechanisms to satisfy any new supply chain assurance obligations. The AIIA supports the criteria identified in the consultation paper (independence, scope, currency, assurance rigour, renewal requirements and treatment of material changes) and recommends that a flexible recognition mechanism allow schemes to be added as they mature.

Reliance on a certification should be limited to the specific scope it actually covers. A certification such as SOC 2 may be scoped narrowly, for example to a single product, environment or business unit, or broadly across a provider's operations. Where the certified scope does not cover the specific facility, service or environment relied on to meet a supply chain assurance obligation, the certification should not be treated as sufficient evidence for that purpose.

Sub-tier dependencies

The consultation paper provides that responsible entities would consider sub-tier risks where those risks materially affect the cyber risk presented by a direct major supplier, and confirms that entities would not be required to identify, assess or contract directly with every supplier in the chain. The AIIA supports that intent, but "materially affect" is not a boundary that can be applied consistently. Without clearer expression, individual interpretation will lead to materially different expectations across entities, and supply chain assessment will extend without a defined endpoint.

The AIIA recommends the following boundary:

1. A responsible entity should be expected to satisfy itself that its major suppliers maintain their own supplier risk assessment process. It should not be expected to obtain, review or assess the specific results of its suppliers' assessments of their suppliers.
2. In addition, a responsible entity should identify sub-tier suppliers that present high risk and could directly affect the critical infrastructure asset. That identification should be targeted at the small number of dependencies capable of direct impact, rather than applied across the supply chain generally, and satisfied through leveraging existing supply chain assurance requirements under relevant frameworks, including CIRMP and/or HCF for example.

This approach maintains visibility of the dependencies that matter while providing a defined and administrable limit.

Downstream impacts on small and medium suppliers

The measure risks increasing assurance requests directed at suppliers, including smaller suppliers that support critical infrastructure indirectly or in specialised roles. Convergence of assurance practice is the most effective mitigation. Where responsible entities converge on recognised certifications and a consistent set of assurance questions, a smaller supplier can invest once in a recognised certification rather than responding to numerous bespoke assessments. Conversely, if expectations remain unstandardised, smaller suppliers will bear disproportionate cost and some may withdraw from critical infrastructure supply chains.

The AIIA recommends that guidance and any recognition instrument be published in advance of the obligation taking effect, so that suppliers can pursue recognised certification if necessary before assurance requests begin.