31 July 2026

BSA COMMENTS ON STREAMLINING AND MODERNISING THE SECURITY OF CRITICAL INFRASTRUCTURE ACT 2018

Submitted Electronically to the Department of Home Affairs (DHA)

The Business Software Alliance (**BSA**)[1] welcomes the opportunity to respond to DHA's Consultation Paper on Streamlining and Modernising the Security of Critical Infrastructure Act 2018 (**Consultation Paper** and **SOCI Act** respectively).[2]

BSA is the leading advocate for the global software industry. BSA members create technology solutions that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, network infrastructure services, cybersecurity solutions, and collaboration systems. Our members have made significant investments in Australia, and we are proud that many Australian companies and organisations continue to rely on our members' products and services to do business and support Australia's economy.

BSA has provided comments on Australia's critical infrastructure protection framework at each major stage of its development[3] and we are encouraged by the Consultation Paper's clear focus on improving regulatory coherence in this space. This approach responds directly to a central finding of the Independent Review of the SOCI Act 2018 (**Independent Review)**,[4] namely that the SOCI Act is overly complex, duplicative, and creates substantial administrative burden.[5] This finding echoes concerns that BSA has raised consistently throughout its engagements on the

[1] BSA's members include: Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

[2] Consultation Paper: Streamlining and Modernising the Security of Critical Infrastructure Act 2018, July 2026, https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/consultation-on-proposed-amendments-to-streamline-and-modernise-the-soci-act-2018/consultation-paper.pdf.

[3] See: BSA Response to Proposed Security of Critical Infrastructure Act Amendments (Ministerial Direction Powers), May 2026, https://www.bsa.org/policy-filings/australia-bsa-response-to-proposed-security-of-critical-infrastructure-act-amendments-ministerial-direction-powers; BSA Submission to the PJCIS Review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, February 2022, https://www.bsa.org/policy-filings/australia-bsa-submission-to-the-pjcis-review-of-the-security-legislation-amendment-critical-infrastructure-protection-bill-2022; BSA Comments on Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, January 2022, https://www.bsa.org/policy-filings/australia-bsa-comments-on-security-legislation-amendment-critical-infrastructure-protection-bill-2022.

[4] Independent Review of the SOCI Act 2018, February 2026, https://oia.pmc.gov.au/sites/default/files/posts/2026/04/Independent%20Review%20of%20the%20SOCI%20Act%20-%20Final%20Report%20%282026%29.pdf.

[5] Independent Review (2026), p. 11. The Independent Review's very first recommendation is to "[r]emove all possible Commonwealth regulatory duplication from the SOCI Act to produce harmonisation and reduce administrative burden".

SOCI Act, and we appreciate the opportunity to work with DHA to ensure that this consultation achieves its desired policy objective.

Summary of BSA's Recommendations

Given the breadth of the Consultation Paper, we have focused our comments on the measures with implications for the enterprise software sector. Our recommendations are as follows:

Measure 1 (Exemptions Framework)

- Adopt an outcomes-based approach when assessing whether another regime is substantially equivalent, and publish draft assessment criteria for public consultation.
- Prioritise assessment of the Privacy Act 1988 (**Privacy Act**) and the Prudential Standard CPS 234 on Information Security (**CPS 234**), which applies to entities regulated by the Australian Prudential Regulation Authority (**APRA**), against the cyber and information security hazard requirements of the Critical Infrastructure Risk Management Program (**CIRMP**) Rules.
- Confirm whether frameworks arising from other markets can also be assessed for equivalence under the same criteria.

Measure 5 (Cyber Security Incident Definition)

- Confirm that unauthorised access, modification or impairment is not excluded merely because it is caused by or through an automated system, software agent, AI-enabled tool or comparable technology.
- Retain a single, technology-neutral incident definition rather than introducing a separate AI incident reporting track.
- Define "materially uncontrolled" to require both a material loss of effective operational control and a direct link to cyber-related harm, and expressly exclude ordinary software defects, configuration issues, routine outages, model errors and other non-security AI issues.

Measure 8 (Data Storage or Processing Capture Pathways)

- Calculate Australian-facing thresholds by reference to Australian customers' use of a service, rather than the location of infrastructure within Australia.
- Adopt a multi-factor test that gives the provider's role independent weight, and confine the test applied to an individual provider to matters that provider can objectively self-assess.
- Expressly exclude Software-as-a-Service (**SaaS**) from the service-based pathway.
- Confine certification-based capture to the certified facility or service rather than the provider more broadly and defer settling this pathway in the Rules until the Hosting Certification Framework (**HCF**) review has concluded.

Measure 15 (CIRMP Governance and Assurance)

- Retain the admissibility restrictions. If they are removed, confine evidentiary use to reports knowingly submitted as materially false or misleading with a clear intention to deceive.
- Recognise independent audits conducted against a framework adopted under section 8 of the CIRMP Rules as satisfying the assurance requirement for that domain.

- Ensure that assurance directed at providers of multi-tenant or shared services does not compromise other customers' information, and does not require direct system access or production testing where independent evidence is available.

Measure 17 (Operations, Maintenance and Managed Service Providers)

- Maintain the cumulative requirement of both practical operational authority and material operational dependency, and publish a non-exhaustive list of excluded services supported by case studies and examples.
- Confirm that providers of general-purpose SaaS, Platform-as-a-Service (**PaaS**) and AI models do not become relevant operators merely because customers use their platforms to configure workflows, automations or AI-enabled processes.
- Limit duties to matters within the operator's role, knowledge and practical control, and confirm that they do not require monitoring of customer usage or disclosures that would compromise security, confidentiality or legal obligations.
- Confirm that a relevant operator's notice is not an admission that an incident occurred or that the operator is responsible for it, and that responsible entities remain responsible for reporting under the SOCI Act.
- Consult the responsible entity before directing a relevant operator, confine any such direction to the Australia-facing asset or service, and provide a grace period before duties commence.

Measure 19 (Supply Chain Cyber Security Assurance)

- Recognise established certifications and reports, including ISO/IEC 27001, System and Organization Controls 2 (**SOC 2**) reports and HCF certification, as evidence of supplier cyber due diligence.
- Assess schemes on independence, scope, currency and rigour rather than mapping their controls against every CIRMP requirement, and maintain a mechanism to keep the recognised list current.
- Confirm that Measure 19 does not create a new directly regulated supplier class.

Measure 1 – Exemptions Framework

Measure 1 establishes a "single, consolidated exemptions framework that could apply across a range of specified SOCI obligations" to replace the fragmented "obligation-specific" exemptions in the current SOCI Act, making it easier for entities to understand how and where they may be able to obtain exemptions.[6] In addition, the proposed exemptions framework will exempt entities from specified obligations where another law or recognised enforceable framework delivers substantially equivalent or stronger outcomes.

BSA supports Measure 1 as it addresses a core concern of regulated entities: that it is administratively difficult for entities subject to multiple regulatory regimes to obtain recognition for compliance work they have already done, resulting in duplicative efforts without any corresponding security benefit. In response to Measure 1, we make the following observations and recommendations:

[6] Consultation Paper (2026), p. 14.

- **On the criteria used to assess whether another regime or framework is substantially equivalent**, we agree that the focus should be on desired outcomes. As a starting point, the relevant criteria could include whether the framework in question: 1) pertains to the same risk category; 2) requires comparable levels of risk management; and 3) requires comparable verification through reporting, attestation or certification. DHA should also publish draft assessment criteria for further consultations.
- **On existing obligations and frameworks to be assessed for equivalence,** we recommend prioritising equivalent obligations under the Privacy Act and CPS 234, which were previously identified by DHA.[7] Regulated entities under the Privacy Act are required to take reasonable steps to protect the personal information they hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure.[8] Similarly, under CPS 234, entities regulated by APRA "must maintain an information security capability commensurate with the size and extent of threats to its information assets" and, where "information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets".[9] These obligations may deliver equivalent outcomes to the cyber and information security hazard requirements of the CIRMP Rules,[10] and an entity that already satisfies them derives no additional security benefit from documenting the same controls a second time in a different form.

Relatedly, while we note that the focus of Measure 1 is consistency and harmonisation within the Australian regulatory landscape, we encourage DHA to consider whether frameworks arising from other markets can also be assessed for equivalence. Many BSA members operate globally and are subject to security obligations covering the same systems and the same risks in several jurisdictions. Where a foreign framework delivers equivalent or stronger outcomes against the criteria above, recognising it would reduce duplication without weakening the security outcome.

Recommendations: DHA should adopt an outcomes-based approach when assessing equivalence under the consolidated exemptions framework, publish draft assessment criteria for public consultation, and prioritise assessments of the Privacy Act and CPS 234. DHA should also confirm whether frameworks arising from other markets can be assessed for equivalence under the same criteria.

[7] Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy, July 2025, https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/charting-new-horizons-horizon-2-policy-discussion-paper.pdf, p. 17.

[8] Australian Privacy Principles, Chapter 11: APP 11 Security of personal information, https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information.

[9] CPS 234, Section 15.

[10] BSA accepts that the scope of coverage may not always align. For example, obligations under the Privacy Act pertain to personal information, whereas the CIRMP requirements extend to the availability, integrity and security of the asset and other information. Nevertheless, the point stands that where equivalence is established for a given obligation, an entity that already satisfies it should not need to document the controls multiple times.

Measure 5 – Cyber Security Incident Definition: Automated Systems, Software Agents and AI

Measure 5 amends the definition of "cyber security incident" in section 12M of the SOCI Act to make clear that unauthorised access, modification or impairment "is not excluded merely because it is caused by or through an automated system, software agent, AI-enabled tool or comparable technology".[11]

BSA supports this amendment in principle, as it confirms that unauthorised access, modification or impairment remains within the definition regardless of whether it is caused by AI. AI-enabled tools are increasingly capable of independently discovering and exploiting vulnerabilities in ways that outpace conventional, human-directed attack patterns. As AI becomes further embedded in the tools used by malicious actors, it is important that the relevant regulations keep pace with these developments. BSA also supports DHA's decision to not create a "separate AI incident reporting regime".[12] Cyber security incidents involving AI should be assessed against the same cyber security character that governs every other incident under the SOCI Act. Creating a separate reporting track would further complicate the incident reporting landscape, which runs counter to the consultation's policy objective.

However, we note that this amendment also captures incidents where an authorised automated or AI-enabled system is "compromised, manipulated or materially uncontrolled in a way that causes cyber-related harm".[13] The term "materially uncontrolled" requires further clarification, as it could be interpreted in an overly broad manner. AI tools can occasionally produce unexpected outputs in the course of operation without any security compromise having taken place. In such a situation, entities might be required to report events that have nothing to do with cyber security. As such, BSA recommends that the term "materially uncontrolled" be defined to require a material loss of effective operational control over the system, together with a direct link to cyber-related harm. This is also consistent with the stated objective of "not convert[ing] ordinary software defects, configuration issues, routine outages, model errors, technology failures or non-security AI issues into cyber security incidents merely because automation or AI is involved".[14]

Recommendation: DHA should confirm that unauthorised access, modification or impairment is not excluded merely because it is caused by or through an automated system, software agent, AI-enabled tool or comparable technology. DHA should also retain a single, technology-neutral cyber security incident definition rather than introducing a separate AI incident reporting track, and define "materially uncontrolled" to require both a material loss of effective operational control and a direct link to cyber-related harm. The definition should also expressly exclude ordinary software defects, configuration issues, routine outages, model errors and other non-security AI issues, so that only genuine cyber security incidents fall within the definition.

[11] Consultation Paper (2026), p. 24.

[12] Consultation Paper (2026), p. 25.

[13] Consultation Paper (2026), p. 24.

[14] Consultation Paper (2026), p. 25.

Measure 8 – Data Storage or Processing Capture Pathways

Measure 8 is especially significant for BSA members, as it proposes to replace the current customer-driven test in section 12F of the SOCI Act with four operator-facing capture pathways that will determine if an entity's asset is a "critical data storage or processing asset":[15]

1) **Facility-based capture**, where capture depends on the physical and operational characteristics of a data-centre facility, measured principally by rated IT load.
2) **Service-based capture**, where capture depends on the type and scale of service provided. The Consultation Paper states that this is directed to "[l]arger cloud, hosted infrastructure, managed hosting, backup and disaster recovery, and comparable service-layer providers", which "provide data storage or processing services on a commercial basis and meet a prescribed Australian-facing scale threshold".
3) **Certification-based capture**, where capture is based on objective certification held by the provider for a relevant facility or service, rather than on customer identity or service knowledge. The principal model under consideration is certification under the HCF or an equivalent prescribed scheme.
4) **Reserve Ministerial designation**, which operates as a "limited reserve mechanism" for exceptional cases of government dependency that fall outside the ordinary thresholds.

Our comments pertain to the service-based and certification-based capture pathways. The Consultation Paper states that the policy intent "is not to create a separate new sector or make all data centres, cloud services or data services critical infrastructure",[16] and each of the recommendations below is directed at giving effect to that intent.

Service-Based Capture Pathway

The service-based pathway will capture service-layer providers "whose scale and role make them systemically significant," and is "not intended to capture services where data handling is merely incidental".[17] BSA agrees with this approach, as an overly broad scope that regulates any entity that provides a service digitally, regardless of their criticality or importance, risks diverting limited regulatory resources from where they are needed the most.

In this regard, the Consultation Paper proposes to set thresholds "potentially by reference to Australian revenue from in-scope services, customer numbers, data volume, employee headcount or a combination of these".[18] BSA recommends that, to accomplish its stated goals, Australian-facing metrics should reflect Australian customers' actual use of a service rather than the physical location of infrastructure within Australia, as that infrastructure is frequently and

[15] Consultation Paper (2026), pp. 36-37. Once captured, the asset becomes subject to the SOCI Act's general obligations, including registration on the Register of Critical Infrastructure Assets, a CIRMP under Part 2A, and cyber incident notification under Part 2B.

[16] Consultation Paper (2026), p. 36.

[17] Consultation Paper (2026), p. 37.

[18] Consultation Paper (2026), p. 37. Furthermore, if quantitative metrics such as data volume are utilised, the framework must distinguish between substantive customer-owned business data (e.g. hosted files or databases) and operational or authentication metadata (e.g., usernames, email, routing logs) generated by the software itself just to function. A high volume of operational metadata is necessary for delivering specialised functional capabilities, but capturing this telemetry artificially inflates the perceived scale of a provider compared to true data storage hosts.

effectively used by non-Australian persons to achieve better security and resilience and so does not necessarily align with the goals of the SOCI Act.

BSA is also concerned that these metrics only account for the provider's scale, but not the provider's role, in the ecosystem. A cloud infrastructure provider whose systems underpin the operations of critical infrastructure customers presents a significantly different systemic risk profile from a SaaS provider that offers customer relationship management or human resources management software, even if they both fulfil the proposed metrics.

Beyond the scale-versus-role concern, BSA cautions against capture criteria that turn on facts or information outside the provider's knowledge. A cloud or SaaS provider generally does not have visibility over what data customers place on its platform or how they use it. This reflects a basic design principle that obligations should rest with the party that has the relevant knowledge and control, not the party that merely supplies the underlying capability. Capture criteria under the service-based pathway should accordingly be confined to matters a provider can objectively self-assess, such as the scale of its own service, and should not incorporate factors such as the sensitivity of customer data or how a customer uses the service. Together with the role-based concern above, this points to a capture test built on factors the provider can actually assess.

BSA therefore urges DHA to adopt a holistic, multi-factor test for service-based capture that gives the provider's "role" independent weight, rather than allowing scale to operate as the de facto determinant. Factors such as whether a class of services is typically relied on by critical infrastructure entities, and whether dependent customers could readily switch to an alternative provider, should inform how DHA defines and calibrates in-scope services in the Rules. They should not form part of the test an individual provider applies to itself, which for the reasons above must remain self-assessable. Those service definitions and thresholds should be reviewed periodically as market conditions evolve.

We also recommend that DHA expressly exclude SaaS from this capture pathway as its disruption does not carry the same risk of cascading, systemic impact that disruptions to the infrastructure layer may have. An outage to a functional software service typically causes a localised access or operational failure, not the mass loss or corruption of the customer's actual critical data assets. Not excluding SaaS would also create further regulatory duplication, as the customer relying on the SaaS product is typically already regulated under the SOCI Act and remains accountable for the governance of its own data. Capturing the SaaS provider as well would apply two regimes to a single underlying risk.

A comparable policy position is emerging in Singapore, which has recently released its Digital Infrastructure Bill for public consultation.[19] The Bill seeks to introduce a licensing regime for providers of "Major Foundational Digital Infrastructure Services," namely data centre facility services and cloud computing services whose scale means their disruption could cause widespread impact on Singapore's digital economy. Importantly, the Bill expressly excludes SaaS

[19] Public Consultation on Digital Infrastructure Bill, July 2026, https://www.mddi.gov.sg/newsroom/public-consultation-on-digital-infrastructure-bill/.

from the definition of a regulated Cloud Computing Service, confining the regime to IaaS and PaaS offerings.[20]

Recommendation: DHA should calculate Australian-facing thresholds by reference to Australian customers' use of a service, rather than the location of infrastructure within Australia. DHA should also adopt a holistic, multi-factor test for service-based capture that gives the provider's role independent weight. Factors such as the criticality of the customer base served and the substitutability of the service should inform how DHA defines and calibrates in-scope services, and those settings should be reviewed periodically as market conditions evolve. The test applied to an individual provider should be confined to matters that provider can objectively self-assess, and should not turn on the sensitivity of customer data or how a customer uses the service, because a provider may not know or have access to this information. Finally, DHA should expressly exclude SaaS from the service-based capture pathway, as SaaS offerings do not carry the same risk of cascading, systemic impact that disruptions to the infrastructure layer may have.

Certification-Based Capture Pathway

On the scope of capture, BSA recommends that the capture should be expressly confined to the certified facility or service, rather than the provider more broadly. A provider that certifies a single service for government hosting under the HCF should not have its entire portfolio of services and offerings fall within the SOCI Act. This would expand the scope well beyond the policy intent and create a direct disincentive to obtain certification.

Relatedly, the certification-based capture pathway should not be settled in the Rules until the ongoing HCF review has concluded. The purpose of the certification-based pathway is to give providers an objective, self-assessable basis for determining whether their assets are critical infrastructure under the SOCI Act. This purpose is defeated if the certification scheme on which the pathway depends is itself under redesign, since a provider's obligations could change as a consequence of reforms to a separate framework, rather than any change to its own facilities, services or operations. Where the HCF review does result in changes to certification scope or requirements, DHA should make transitional arrangements available to affected providers (e.g., provide a suitably long grace period before obligations commence).

Recommendation: DHA should confine capture under this pathway to the certified facility or service rather than the provider more broadly. DHA should also defer settling the certification-based capture pathway in the Rules until the HCF review has concluded, and provide a suitably long grace period before obligations commence for any provider whose status changes as a result of that review.

Measure 15 – CIRMP Governance and Assurance

BSA is concerned with proposals under Measure 15 to: 1) remove current restrictions on the use of annual compliance reports in civil penalty proceedings; and 2) introduce mandatory periodic independent assurance of CIRMP design and implementation, on a base cycle of at least once every three years.[21]

[20] Public Consultation on Digital Infrastructure Bill (2026), para 7b.

[21] Consultation Paper (2026), p. 69.

Removing Admissibility Restrictions

BSA does not support the repeal of the admissibility restrictions in sections 30AG and 30AQ of the SOCI Act, which would allow annual compliance reports to be relied on in civil penalty proceedings where appropriate.

The purpose of the annual compliance report is to give the regulator an accurate picture of an entity's risk management posture, including its deficiencies. The current restriction is critical insofar as it promotes open communication between the entity and the regulator. If these reports can later be tendered as evidence against the entity in civil penalty proceedings, the incentive shifts toward defensive drafting, where entities disclose only the minimum necessary and frame deficiencies to limit legal exposure rather than to give the regulator a candid account of where their risk management genuinely stands. The result is a reporting mechanism that yields less useful information, which undermines the very purpose the annual report is meant to serve.

In this regard, BSA has consistently advocated for the incorporation of "no-fault" and "no-liability" principles into cyber security reporting obligations, on the basis that the punitive use of disclosed information discourages full and frank disclosure and ultimately weakens the regulator's visibility over the risks it is seeking to manage.

If DHA proceeds notwithstanding the above, we strongly urge DHA to confine evidentiary use of annual compliance reports to narrow and highly specific situations, such as when an entity has submitted a report that is materially false or misleading with a clear intention to deceive the regulator. Mere incompleteness should not fall within scope, as a report may be incomplete for reasons that have nothing to do with any intent to mislead, including the inherent difficulty of characterising an evolving risk environment and genuine differences in interpretation.

Recommendation: DHA should maintain the current restrictions on the use of annual compliance reports in civil penalty proceedings. If DHA does remove these restrictions, the evidentiary use of these reports should be clearly confined to cases where an entity has knowingly submitted a report that is materially false or misleading with a clear intention to deceive the regulator. Mere incompleteness should not be sufficient.

Independent CIRMP Assurance

The Consultation Paper itself acknowledges that, by introducing mandatory periodic independent assurance of CIRMP design and implementation, "the recurring cost…is expected to be the most material ongoing element of this measure".[22] We agree with this observation, and further note that these costs could compound substantially, especially where an entity is responsible for multiple captured assets or products. Costs could increase even further if the entity operates in multiple jurisdictions. BSA members commonly fit both descriptions, and the cumulative burden of periodic independent assurances is likely to result in significantly higher compliance costs.

The Consultation Paper recognises that this measure "may reduce duplication where SOCI assurance can be aligned with existing audit, prudential or assurance requirements",[23] but does

[22] Consultation Paper (2026), p. 73. The Consultation Paper observed that the main costs "comprise strengthened governance and approval processes, periodic independent assurance, preparation and review of assurance reports, remediation where deficiencies are identified, and engagement with the CISC on assurance outcomes".

[23] Consultation Paper (2026), p. 73.

not commit to a mechanism for achieving this. BSA recommends that DHA establish one, and notes that the foundation already exists. Section 8 of the SOCI (CIRMP) Rules 2023 (**CIRMP Rules**), which pertains to cyber and information security hazards, requires entities to meet the cyber and information security hazard requirements by maintaining a process that complies with recognised frameworks, including ISO/IEC 27001 and the Essential Eight Maturity Model.[24] As such, an entity that holds current certification against, or is independently audited under, one of those frameworks already undergoes recurring independent assessments by accredited assessors, on a cycle that meets the proposed three-year assurance baseline.

Finally, the assurance framework should not become a vehicle for unrestricted customer audit rights over service providers. Where a responsible entity relies on a provider operating a multi-tenant or shared service, assurance activity directed at that provider should protect the information of the provider's other customers and its sensitive shared service architecture. It should also not require direct access to the provider's systems or testing in production environments where suitable independent evidence, such as an existing third-party audit or certification, is available. This protects the integrity and security of the shared environment while still giving the responsible entity and the regulator the assurance they need.

Recommendation: DHA should make clear that independent audits conducted against a framework an entity has adopted under section 8 of the CIRMP Rules (Cyber and Information Security Hazards) would satisfy the assurance requirement for that domain. DHA should also confirm that assurance directed at providers of multi-tenant or shared services must not compromise other customers' information or sensitive service architecture, and should rely on existing independent evidence rather than direct system access or production testing where such evidence is available.

Measure 17 – Operations, Maintenance and Managed Service Providers

Measure 17 proposes a new “relevant operator” concept, which imposes direct statutory duties for third parties that hold “practical operational authority” and “material operational dependency” over a critical infrastructure asset on which the responsible entity materially depends.[25]

As a general principle, primary responsibility for the security of a critical infrastructure asset, and for interfacing with the regulator, should always remain with the responsible entity. The Consultation Paper acknowledges this by confirming that "the responsible entity would remain the primary regulated entity", that its obligations under the SOCI Act are "non-delegable", and that a relevant operator's duties "would apply only to matters within the relevant operator's role, knowledge and practical control".[26]

Against this backdrop, BSA’s comments focus on two issues: limiting the scope of “relevant operator” to entities that exercise genuine operational control, and ensuring that any direct duties imposed on them are proportionate and operationally workable.

[24] CIRMP Rules, Section 8(4).

[25] Consultation Paper (2026), p. 77.

[26] Consultation Paper (2026), pp. 79 and 81.

Scope of Relevant Operators

The Consultation Paper proposes that a person will only be considered a relevant operator if *both* "practical operational authority" and "material operational dependency" are present.[27] BSA agrees with the cumulative application of both requirements, which ensures that the scope of capture is not overly broad. Many BSA members provide products and services that may be important to a responsible entity's operations, but the responsible entity retains control over deployment and usage. A provider in that position should not become a relevant operator unless it clearly exercises substantive operational control over the relevant asset or critical function. This distinction is necessary to ensure that Measure 17 remains focused on operational control risks, rather than becoming a broad mechanism for directly regulating suppliers.

In this regard, BSA supports including a non-exhaustive list of excluded services and activities, supplemented by case studies and examples. The Consultation Paper already recognises this, stating that providers of "professional advice, monitoring-only services, minor maintenance, emergency support, commodity inputs, general-purpose infrastructure, software support, equipment supply or ordinary subcontracted services"[28] are not intended to be in scope. Likewise, "[g]eneral-purpose infrastructure services, including cloud computing" are also excluded "unless the provider exercises direct operational control over a critical function of the specific asset".[29]

To make the scope of capture more precise, BSA recommends that DHA clarify how the exclusion applies to general-purpose SaaS, PaaS, and AI models. A provider should not become a relevant operator merely because a responsible entity uses the provider's AI model or platform to configure workflows, automations or AI-enabled processes. Capture should arise only where the provider itself has independently exercisable authority to operate, configure, disable, restore, materially alter or materially influence the customer-specific workflow or function that controls the critical infrastructure asset.

Recommendation: DHA should maintain the cumulative requirement of both "practical operational authority" and "material operational dependency," and should create a non-exhaustive list of excluded services and activities, supplemented by case studies and examples. In addition to excluding cloud computing infrastructure providers, DHA should also confirm that providers of general-purpose SaaS, PaaS and AI models do not become relevant operators merely because a responsible entity uses their platform or model to configure workflows, automations or AI-enabled processes. Capture should turn on whether the provider itself has independently exercisable operational control over the specific workflow or function that controls the critical infrastructure asset.

Duties of Relevant Operators

Measure 17 would impose the following duties on relevant operators:

---

[27] Consultation Paper (2026), pp. 77-78. The Consultation Paper notes that practical operational authority may include the ability to operate, configure, maintain, disable, restore, materially alter or materially influence the operation, availability, integrity or security of the asset or critical function. Material operational dependency would arise where the responsible entity depends on the exercise of that control for the continued operation, availability, integrity or security of the asset.

[28] Consultation Paper (2026), p. 81.

[29] Consultation Paper (2026), p. 81.

1) Cooperating, so far as reasonably practicable, with the responsible entity's compliance with Part 2A of the SOCI Act, including by providing reasonable access to information, systems and personnel where needed for risk management, assurance, incident response or remediation.
2) Notifying the responsible entity, without unreasonable delay, of events, changes or circumstances within the operator's knowledge that could materially affect the operation, availability, integrity or security of the asset.
3) Not taking action that the operator knows or ought reasonably to know would materially compromise the security, integrity, availability or operation of the asset.

BSA recognises that limited duties may assist responsible entities in managing operational dependencies. However, those duties should be appropriately framed so that they are operationally workable and limited to matters within the relevant operator's knowledge and practical control.

- First, the duty to cooperate should not require the relevant operator to provide access to information, systems or personnel in a manner that would compromise the security of its own systems, disclose proprietary technical information[30] or personal information related to customers, reveal sensitive security architecture, or conflict with confidentiality, privacy, protected-information, regulatory, or foreign-law obligations.[31] This limitation is particularly important for enterprise software and cloud service providers that operate shared, multi-tenant and globally integrated services.
- Second, the notification duty should be tied to actual knowledge obtained through the relevant function or relationship. Large technology providers may operate through multiple teams, systems and jurisdictions. The fact that one part of a global organisation has information about a technical issue should not automatically mean that the relevant operator had knowledge that the issue could materially affect a specific Australian critical infrastructure asset. The duty should apply where the operator, through personnel responsible for the relevant service, account or operational function, becomes aware of an event, change or circumstance that it reasonably understands could materially affect the operation, availability, integrity or security of the specific asset or critical function. Relatedly, DHA should confirm that neither the cooperation duty nor the notification duty requires a provider to monitor, log or inspect customer usage where doing so would breach privacy obligations or contractual commitments to customers.
- Third, the duty not to materially compromise the asset should not impose strict liability for ordinary service interruptions, customer configuration decisions, customer-directed changes, or emergency actions taken in good faith to protect security or continuity.

BSA also recommends that DHA clarify the relationship between relevant operator notification and the responsible entity's own SOCI incident reporting obligations. A relevant operator should notify the responsible entity of relevant matters within its role and knowledge, but the responsible

[30] Examples include model weights and security testing materials. Disclosure of such material would create security risk without improving the responsible entity's risk management.

[31] For example, the cooperation duty should also be expressly subject to applicable data protection law, including restrictions on cross-border transfers of personal data. Discharging the duty may require a provider to move personal data out of a jurisdiction that restricts such transfers.

entity should remain responsible for determining whether the event is reportable under the SOCI Act. This reflects the fact that the responsible entity is best placed to assess asset-level consequences, dependencies and statutory reporting thresholds. DHA should also confirm that a notice given by a relevant operator is not itself an admission that a cyber security incident occurred, that a statutory reporting threshold was met, or that the relevant operator is responsible for that incident. Without that confirmation, operators face an incentive to delay or narrow notifications in order to manage legal exposure.

Separately, the Consultation Paper proposes that "[w]here a Ministerial direction relates to a critical infrastructure asset and compliance requires action within a relevant operator's direct control", the direction could be given to the relevant operator for those matters.[32] BSA understands the rationale of addressing a direction to the entity capable of taking the required action, but proposes two safeguards:

- First, there should be an express requirement for DHA to consult the responsible entity before issuing such a direction to the relevant operator. It is the responsible entity, not the relevant operator, which has the full picture of the asset and its dependencies. Directions addressed straight to the relevant operator should be reserved for cases where DHA has determined, through its consultations with the responsible entity, that the responsible entity cannot take the required action.
- Second, any direction given to a relevant operator should be confined to the Australia-facing asset or service. Unlike a disclosure obligation, a direction requires operational action, and action taken on shared infrastructure can affect customers in other jurisdictions with no connection to the Australian asset.

Finally, DHA should provide a suitably long grace period before duties commence for newly identified relevant operators, as entities that become relevant operators will need to identify affected arrangements, establish notification and escalation processes and renegotiate contracts.

Recommendation: DHA should ensure that the direct duties imposed on relevant operators are expressly limited to matters within the operator's role, knowledge and practical control. These duties should not require disclosures that would compromise security, customer confidentiality, proprietary technical information or legal obligations, including applicable data protection law. Notification duties should be triggered only by actual knowledge through the relevant function, and should not require a provider to monitor, log or inspect customer usage. The duty not to materially compromise an asset should not extend to ordinary service interruptions, customer-directed changes or good-faith emergency action. DHA should also confirm that responsible entities remain responsible for SOCI incident reporting, and that a notice from a relevant operator is not an admission that an incident occurred, that a reporting threshold was met, or that the operator is responsible for the incident. Before giving a direction to a relevant operator, DHA should consult the responsible entity and confine the direction to the Australia-facing asset or service. Finally, DHA should provide a suitably long grace period before duties commence for newly identified relevant operators.

[32] Consultation Paper (2026), p. 81.

Measure 19 – Supply Chain Cyber Security Assurance

Measure 19 requires responsible entities to assess and manage cyber security risks from major suppliers whose products, services, access or role matter to the security or operation of a critical infrastructure asset.[33] As part of Measure 19, DHA proposes to recognise established cyber security certifications and accreditations as evidence of supplier cyber due diligence, so that a responsible entity can rely on a supplier's existing certification rather than commissioning a separate, bespoke assessment.

BSA supports this approach in principle. We highlight the following for consideration:

- First, recognising existing certifications. The Consultation Paper identifies duplicative supplier assessments as a core problem, noting that responsible entities and suppliers often "repeat bespoke assessment processes that ask materially similar questions in different formats".[34] This adds cost, multiplied across every customer, without a matching security benefit. Recognising established certifications and reports, such as ISO/IEC 27001, SOC 2 reports and HCF certification, is the best way to reduce duplicative efforts.
- Second, the criteria for recognition. The Consultation Paper proposes criteria based on "independence, scope, currency, assurance rigour, renewal requirements, treatment of material changes, and suitability".[35] BSA supports this focus. The criteria should test whether a scheme is independently audited, properly scoped and current. They should not attempt to map every control in a scheme against every CIRMP requirement, which would simply recreate the duplication this measure is designed to remove.

BSA also agrees with the approach to not have Measure 19 directly regulate suppliers.[36] This avoids extending SOCI obligations to suppliers with no visibility or control over the asset itself.

Recommendation: DHA should recognise established certifications and reports, including ISO/IEC 27001, SOC 2 reports and HCF certification, as evidence of supplier cyber due diligence. The criteria for recognition should focus on a scheme's independence, scope, currency and rigour, rather than mapping its controls against every CIRMP requirement, and should maintain the recognised list through a mechanism that can be updated as schemes evolve. DHA should also confirm that Measure 19 does not create a new directly regulated supplier class, with supplier cyber assurance remaining the responsibility of the responsible entity through its CIRMP.

Conclusion

We thank DHA for the opportunity to provide our recommendations in response to the Consultation Paper. We hope our comments are useful as you continue to refine the SOCI Act and the broader security regulatory landscape. We welcome DHA's consistent commitment to engaging with industry stakeholders, including BSA and our members and we look forward to continued dialogue in support of your important mission to protect Australian citizens and assets.

[33] Consultation Paper (2026), pp. 86-87.

[34] Consultation Paper (2026), p. 87.

[35] Consultation Paper (2026), p. 89.

[36] Consultation Paper (2026), p. 88.

Yours sincerely,

Tham Shen Hong
Director, Policy – APAC