INTERNET ASSOCIATION OF AUSTRALIA LTD
ABN 71 817 988 968
ACN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

29 July 2026

Critical Infrastructure Security Policy Branch
Department of Home Affairs

By submission: Consultation on proposed amendments to streamline and modernise the Security of Critical Infrastructure Act 2018

RE: Streamlining and Modernising the *Security of Critical Infrastructure Act 2018* – Consultation Paper

The Internet Association of Australia Ltd (**IAA**) thanks the Department of Home Affairs (**Department**) for the opportunity to respond to the Consultation Paper on Streamlining and Modernising the *Security of Critical Infrastructure Act 2018* (**SOCI Act**).

IAA is a member-based association representing Australia's Internet community. Our membership is largely comprised of small to medium sized Internet service providers (**ISPs**), many of which are subject to the SOCI Act and its subordinate legislation, including but not limited to the Security of *Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025* (**TSRMP Rules**). These ISPs represent the smaller entities within the designated communications sector, and often lack resources to engage directly themselves in regulatory reform processes. This response is thus primarily in representation of these smaller entities that make up a largely underrepresented portion of the communications sector, despite being disproportionately affected by the associated regulatory burdens. IAA itself, as a licenced carrier, is also a responsible entity for critical telecommunications assets as defined under the SOCI Act.

We have thus been heavily involved in the development of regulation within the SOCI framework, particularly in relation to the TSRMP Rules as a representative voice for smaller entities within the sector. IAA and our members appreciate the importance of the SOCI framework and its pertinence in today's evolving threat environment. We further appreciate Government's continued collaborative approach to ensure it remains fit for purpose amidst great technological, social and economic changes. Moreover, we continue our interest and commitment to working with Government, industry and other stakeholders for the continued development of an effective legislative regime ensuring the security and resilience of Australia's critical infrastructure ecosystem.

We therefore provide our response to the Consultation Paper to ensure any reforms to the SOCI Act will be fit-for-purpose, proportionate and practicable, particularly as it relates to the telecommunications industry. Indeed, we understand that is the intent behind the proposed reforms – to reduce uncertainty and improve clarity. To that end, we raise concerns where the proposed changes risk:

- the SOCI framework becoming more prescriptive, at the risk of eroding the key principles of flexibility and proportionality; and

- focusing on enforcement, at the risk of eroding government-industry trust, and reinforcing the collaborative approach taken to date.

We take this opportunity to stress that the collaborative, proportionate and flexible approach has been fundamental to the effective operation of the regime as it has allowed industry to engage meaningfully with its compliance activities, and has therefore supported genuine uplifts in Australia's security and resilience posture. We are therefore concerned that some of the proposals would be counter to this approach and would risk undermining the very outcomes the SOCI framework intends to achieve.

We are also concerned about the pace and volume of regulatory reform in relation to the SOCI framework. We note that these proposals are being considered alongside reforms to the Ministerial powers and following recent updates relating to enhanced CIRMP obligations. Given the continued evolution of technologies and threat landscape, we appreciate the need to continue developing the SOCI framework to ensure it remains current and fit-for-purpose. However, this must be balanced with the regulatory burdens being placed on industry. Accordingly, where there are alternative ways to address new threats and risks rather than via prescriptive legislative requirements, they should be prioritised.

OUR RESPONSE

PART A: REDUCING COMPLEXITY, DUPLICATION AND UNCERTAINTY

Measure 1 — Exemptions Framework

IAA recommends a broader entity exemption model to introduce a mechanism to exempt entities that should not be captured by the SOCI Act at all.

As expressed in previous consultations on the SOCI framework, and particularly in relation to the TSRMP Rules, we consider that certain telecommunications entities should be exempt from the SOCI Act, and its subordinate rules entirely. The definition of 'carriers' and 'critical telecommunications assets' means any entity with a carrier licence is a responsible entity for the purposes of the SOCI Act, and the TSRMP Rules. These definitions do not adequately distinguish between:

- highly interconnected telecommunications networks that are indeed central to national security, and the operation of Australia's essential services; and
- smaller telecommunications entities with specialised networks that have limited interdependencies or limited likely impact on Australia's national security, yet hold a carrier licence for its operations.

We note that the TSRMP Rules introduces a threshold to carve out smaller carriage service providers (**CSPs**) that have less than 20,000 services in operation, in recognition that not all telecommunications entities provide such national-critical infrastructure. However, all carriers remain subject to the full extent of the SOCI Act and TSRMP Rules, even where their operational footprint may be smaller than the CSPs who are carved out under the threshold.

It is not sufficiently clear why these types of carrier networks and operators should be captured to the same extent as large, telecommunications providers delivering services to highly critical systems or institutions, or to significant numbers of end-users/customers, particularly in the

absence of clear evidence demonstrating the benefits of inclusion. For such entities, the cost and complexity of implementing the TSRMP Rules are disproportionate to the risk they pose to Australia's national security.

We therefore recommend the introduction of an exemption model, to carve out select entities. We propose this exemption model adopts the approach taken under the *Telecommunications (Interception and Access) Act 1979* (TIA Act).[1] Under such a model, the burden and onus of demonstrating why a carrier's assets are not 'critical' for the purposes of the SOCI framework would fall on the carrier. Examples of when an exemption may be granted would be where the carrier has sufficiently demonstrated their limited operational footprint, and limited interdependencies across Australia's critical infrastructure ecosystem. The Minister would then grant or reject the exemption application, on a case-by-case basis.

We consider this model would be appropriate, and in the Government's mutual interest, as we appreciate that it is difficult to identify the type of carriers that should be exempt. Indeed, we understand that this complexity was a core motivating reason why the TSRMP Rules applied to all carriers in our previous engagement with the Department on this matter.

Measure 2 — Register of Critical Infrastructure Assets

We support, in principle, the proposal to change the architecture between what type of registrable information is prescribed in the SOCI Act, versus the subordinate rules, to ensure the registration scheme is agile and remains fit for purpose. Furthermore, we support the intent for any subordinate rules that prescribe information to be subject to public consultation and parliamentary scrutiny.

Question 8: Should the approved form be expressly prevented from requiring information beyond the kinds prescribed in the Rules?

We consider any information sought via the approved form that is not prescribed in the Rules is only sought on a voluntary basis.

Question 9: What systems, suppliers or dependencies information would be most useful for critical infrastructure visibility, incident modelling and cascading-risk analysis, and what limits should apply?

We consider this may vary between the sectors, and therefore recommend the Department engages separately with each critical infrastructure sector to identify the most appropriate and useful information.

Question 12: What transition settings are needed so entities that have already registered do not need to re-register unnecessarily?

We disagree with the assessment that this change will be largely cost-neutral for industry. Prescribing more detailed categories of information for notification in the rules will likely increase the frequency with which entities are required to update the register, and the regulatory impact assessment should reflect this. Furthermore, as it particularly relates to small entities who often lack capability to engage in regulatory reform, any change in the legislative framework is likely to cause some confusion and uncertainty, and therefore introduce some costs as they seek to understand new obligations. We there recommend transition arrangements of at least six months.

[1] See Division 3 of Part 5-1A and Division 2 of Part 5-3 of Chapter 5 of the TIA Act.

Measure 3 — CIRMP Annual Reporting Simplification

Question 13: Does the proposed annual reporting model provide a workable way to make reporting more adaptable while preserving clear statutory limits?

We support the proposed changs to the annual reporting model, subject to our below feedback.

Question 14: What matters should remain fixed in the Act, and what matters should be set through the approved form or Rules?

We are concerned that the approved form, as it would not be subject to legislative scrutiny, risks becoming overly prescriptive or burdensome over time. We appreciate that the intent is for the approved form to operate within statutory limits, and that advance publication of the form will be provided. However, we do not consider these sufficient safeguards. **Instead, we recommend that any future changes to the approved form and its reporting questions be subject to public consultation.**

Furthermore, the SOCI Act or rules should specify a minimum consultation period (of at least 30 days) before any changes to the approved form can take effect ahead of a relevant reporting period.

Question 15: How far in advance should proposed reporting questions be published? Would a minimum period of three months before the reporting period provide sufficient predictability?

A three-month notice period is insufficient. This is particularly the case for smaller entities who lack the resources to quickly adapt to changes in compliance expectations, and also follow the requisite governance processes required under the CIRMP Annual Reporting obligations. **We consider six months is necessary, with four months as an absolute minimum.**

We also request that a downloadable version of the form be made available and maintained, to support entities completing internal review and governance purposes ahead of formal submission using the approved form.

Q16: Should corporate groups be able to lodge a consolidated or group-level report where this reduces duplication and still provides clear asset-level and entity-level information?

We support the introduction of group reporting and consolidated reporting pathways

Measure 4 — Part 2D Notification Clarification

Question 17: Does the proposed clarification make the legal effect of a section 30ED notice sufficiently clear?

In order to further improve clarity and reduce the risk of confusion amongst entities, we also recommend that the clarification explicitly notes that further notices or proposed changes are not required where later project, system, service, ownership or implementation change is not likely to have a material adverse effect on the entity's capacity to comply with its security obligation under section 30EB of the SOCI Act.

Question 19: What guidance or examples would help responsible entities apply the continuing notification obligation where a project or arrangement evolves after an earlier section 30ED notice?

Practical guidance is required on what constitutes a change that is likely to have "material adverse effect" on an entity's ability to comply with the security obligation.

Question 21: Is an increase in the civil penalty for non-compliance with section 30EC appropriate to reflect the importance of timely notification? If not, what alternative approach should be considered?

We do not support an increase to the civil penalty for non-compliance with section 30EC of the SOCI Act. There is no evidence to suggest that telecommunications entities are intentionally breaching compliance obligations and treating the penalties set out under Part 2D to be insignificant or merely an acceptable cost of doing business. Rather, in the event that entities are not complying, we consider this is likely to be the result of lack of awareness and confusion with respect to how the obligations apply. As such, we strongly recommend greater guidance from Government and collaboration with industry – particularly smaller entities within the sector – as a more effective way of improving the sector's compliance posture.

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

Question 22: Does the proposed definition-level clarification make clear when a cyber security incident involving automated systems, software agents, AI-enabled tools or comparable technologies should be treated as a cyber security incident under the SOCI Act?

Question 25: What guidance, examples or consequential amendments would help responsible entities apply the revised definition consistently, including for Part 2B reporting?

It is unclear why changes to the legislative definition of a cyber security incident are necessary, as opposed to guidance clarifying how an incident involving automated systems, software agents, AI-enabled tools or comparable technologies apply. Cyber security has, since at least the early days of internet protocol networks, always comprised a strongly automated component. Technology will continue to evolve and give rise to new systems and tools, and it is not clear that legislative amendment should be required at each stage of that evolution.

Instead, we recommend further guidance material on the inclusion of cyber security incidents involving automated systems, software agents and AI-enabled tools. This guidance should furthermore provide examples of what sort of incident would qualify a report to be made under Part 2B, and where AI issues would not prompt a report.

Question 23: Does the proposed approach preserve the cyber security character of the definition, including by excluding ordinary software defects, configuration issues, routine outages, model errors, general technology failures and non-security AI issues?

Notwithstanding our position stated above in response to Question 22, if the definition of 'cyber security incident' is amended, the legislation or explanatory memorandum must clearly state that the threshold for reporting obligations remains unchanged, particularly in respect of technical failures, defects, or issues involving no element of compromise, manipulation, or material loss of control which would not trigger incident reporting.

Question 24: How should the legislation deal with incidents involving authorised automated or AI-enabled systems that are compromised, manipulated or materially uncontrolled in a way that causes cyber-related harm?

The legislation should remain technology-neutral for the purposes of the incident notification obligations. Cyber security is already recognised as a key hazard under the CIRMP framework, which is the more appropriate place to deal with any sector or risk-specific requirements.

Measure 7 — Submarine Telecommunications Cables and Associated Infrastructure

We support this measure in principle. However, we recommend targeted consultation, particularly with the affected segment(s) of the telecommunications sector, given the specialised nature of these assets.

PART C: GOVERNANCE, ASSURANCE AND ACCOUNTABILITY

Measure 15 — CIRMP Governance and Assurance

Question 72: Should the current admissibility restrictions on annual compliance reports be removed entirely, or should any limitations on use be retained? If safeguards are needed, what should they be?

We strongly oppose the proposal to remove the current admissibility restrictions set out in sections 30AG and 30AQ of the SOCI Act. While we understand the policy intent behind this proposal, we note that removing the admissibility restriction is counter to the original rationale for including it, which we understand was to encourage transparency and meaningful reporting amongst responsible entities. We are concerned that with the removal of the admissibility restrictions, industry will take a defensive posture due to the fear of enforcement, resulting in a greater risk of the CIRMP attestation process being treated as more of a tick-box exercise. This would not be in the interest of Government, nor industry, as this would greatly diminish the value of the data being provided to Government and therefore its ability to assess Australia's overall security and resilience posture. This would then pose the risk that Government is unable to intervene accordingly, whether through targeted engagement with entities facing capability gaps, broader guidance or other enforcement action. Overall, we consider that the removal of the restrictions would erode the quality and reliability of CIRMP reporting, and would undermine the collaborative and trust-based relationship, ultimately also negatively affecting Australia's readiness and resilience against incidents affecting our critical infrastructure.

Furthermore, we note the Consultation Paper has not provided any evidence to suggest that the current restrictions have impeded necessary civil proceedings or other enforcement action. It would be helpful to understand whether such instances have in fact occurred, and if so, the alternative steps taken by Government in response, and the overall outcome. We believe this information is crucial to complete a meaningful cost-benefit analysis of removing the restrictions.

Question 73: Is a clearer governance and review framework, including governing-body or senior-manager approval, a minimum review cycle and event-based triggers for earlier review, the right way to improve CIRMP currency and accountability?

In principle, we agree with the proposed amendments to clarify governance and review frameworks. **However, we recommend that this clarification is provided through guidance material, rather than via prescriptive legislative reform.** Flexibility and proportionality are key principles underpinning the SOCI Act and the CIRMP, and IAA and our members greatly appreciate the approach Government has taken to date in recognising that each responsible entity is best placed to make decisions about its own risk management. Rather than introducing prescriptive rules around governance and review processes which may result in the CIRMP becoming tick-box exercises, we consider that these expectations would be better addressed through guidance, which would then support entities develop in their security maturity in a manner that is consistent with the key principles.

Furthermore, as it pertains to the governing-body or senior-manager approval, we note that this is already addressed through the CIRMP attestation form, which requires the responsible entity to attest that its submission has been approved by the entity's governing body.

Question 74: Are the proposed CIRMP currency criteria appropriate, including whether the CIRMP reflects the entity's current operating environment and asset configuration, current threats and hazards, current regulatory requirements, current governance arrangements, and lessons learned from incidents, exercises or reviews?

Similar to our response to Question 73, we recommend that any measures taken to set out currency criteria be addressed through guidance, rather than in the legislative framework itself.

Question 75: Should periodic independent assurance be mandatory for responsible entities subject to CIRMP obligations? If so, is a three-year base cycle appropriate?

Question 77: In what circumstances should more frequent review or stronger independence requirements apply?

IAA is strongly opposed to this measure. Prescribing mandatory independent audits would introduce a significant cost impost to industry. Even a three-year assurance cycle represents a substantial burden, particularly for smaller entities. This is particularly concerning given our comments above regarding the capturing of small telecommunications entities that we consider fall outside the intended scope of the SOCI Act.

As such, we recommend that, if this measure is pursued at all, it should apply only to SONS entities or those subject to enhanced CIRMP rules.

Q76: What assurance models should be acceptable for different risk profiles, including external assurance, internal audit or other operationally independent assurance functions?

We note that for smaller entities, even internal independent assurance processes will be difficult to pursue given the limited team size. Many small carriers across Australia subject to the SOCI framework have under five staff members, and of those staff, those capable of undertaking an CIRMP assurance audit are likely involved in the design and operation of the CIRMP.

Q78: Should assurance reports be provided to both the responsible entity's governing body and the CISC? What timeframes should apply for reports and remediation plans where material deficiencies are identified?

Assurance reports should only be provided to the responsible entity's governing body, and not to the CISC as part of the CIRMP reporting. We consider that a CIRMP assurance report is likely to hold commercially confidential information. We further consider providing access to the CIRMP assurance report would be counter to the approach taken thus far, as mentioned above – that the responsible entity is best placed to manage its own risks.

As follows, as part of annual reporting, entities should only be asked to confirm whether an assurance report has been completed (or, if not, when completion is expected) and the overall assessment of the responsible entity's compliance with the CIRMP.

Timeframes for remediation of any non-compliance should be flexible and depend on the nature of the deficiency identified, and the risk posed by the non-compliance as some issues will require materially more time to address than others, while some issues may not require urgent addressing.

Measure 16 — Graduated Civil Penalty Settings

We note that again, there is no evidence to suggest that the current civil penalty amounts are viewed by industry as trivial, or merely an acceptable cost of business, and are therefore not complying, opting instead to risk enforcement actions. While we understand the policy intent, we do not believe the proposal to increase the maximum civil penalty for the preventative and assurance duties is necessary to deter non-compliance. We reiterate that in general, education and continued collaboration with industry, particularly with small entities who find it difficult to engage with Government due to their limited resources would be more beneficial to improve meaningful compliance.

Measure 17 — Operations and Maintenance and Managed Service Providers

Question 82: Does the proposed "relevant operator" concept identify the right class of entities? Should the test require both practical operational authority and material operational dependency?

We support this measure in principle, and welcome the Department's approach to only capture operators with substantial operational authority. We support that the 'relevant operator' test should require both practical operational authority and material operational dependency.

Measure 18 — Corporate Group Cooperation

We welcome this measure as a helpful way for entities operating under a corporate group structure to better manage CIRMP compliance obligations.

Measure 19 — Supply Chain Cyber Security Assurance

Question 92: Is a cyber-specific supplier assurance expectation a clear and workable addition to the CIRMP framework? What practical outcomes should responsible entities be expected to demonstrate?

We understand the policy intent of introducing cyber-specific supplier assurance obligations under the CIRMP. However, we consider the proposal as currently framed, is too prescriptive and again fails to reflect the principles of proportionality and flexibility. We appreciate that the framework intends to focus only on major suppliers and services whose products and services are material to the asset's risk profile. However, we reiterate that the SOCI framework in relation to the telecommunications sector captures all carriers, regardless of size or criticality to Australia's national security.

Consequently, we are concerned this measure would introduce great imposts for industry, particularly disproportionately affecting smaller providers. In practice, small entities often have low visibility over their suppliers' risk controls, and moreover have limited commercial leverage to mandate or monitor such controls. In cases of large, global vendors, it is also likely that entities will be unable to maintain a direct point of contact with suppliers to discuss security assurance where no dedicated account or business manager exists. Furthermore, this will likely increase the friction between vendors and the Australian market.

This measure will therefore materially drive-up costs for entities as there will be increased pressure to acquire goods and services from certified or accredited suppliers, as well as require significant additional handling and management of vendors.

To that end, we propose that this may also be better addressed through guidance material rather than introducing further complex obligations under the SOCI Act. We further consider that the cyber security of supplier goods and services is already captured under the supply chain hazard of the CIRMP. Thus, to the extent Government considers cyber security within supply chains to be a gap, rather than introducing new but overlapping obligations, the cyber security concerns in relation to suppliers can be clarified in the guidance material. This would then also be better aligned with the proportionality and practicability principles underpinning the SOCI framework.

Question 95: How should responsible entities address supplier cyber risk through contractual or equivalent measures, including at contract entry, renewal or material variation?

Notwithstanding our position stated above in response to Question 92, we appreciate that if this proposal is introduced, this measure is intended to operate prospectively and apply at defined milestones such as contract entry or renewal. We stress that this is crucial as entities, and in particular smaller entities, do not have the capacity to re-negotiate contractual terms. The telecommunication sector also experiences a high level of vendor lock-in due to the nature of technology, contractual obligations, and procurement being based on multi-year refresh cycles. As such, the implementation timeframe must be calibrated accordingly.

Measure 20 — Specified Risk Information

Question 99: Is a procedural obligation to consider specified published risk information and record a response the right calibration?

We understand that a similar proposal has been recently consulted on under the Department's consultation on amendments to the Ministerial Directions Powers (Measure 3 – Restrictions on the use of high-risk vendors, products or services). We are thus concerned that this measure would overlap with the proposed amendment to the directions power, compounding the regulatory burdens facing industry. **We consider that this approach is more appropriate than the proposal to introduce a vendor-risk directions power under Part 3 of the SOCI Act, subject to the below considerations.** However, this measure should only operate to notify responsible entities of current and emerging risks that should be managed in a proportionate and practicable manner. This obligation should not be introduced to prescriptively control how entities conduct business.

Question 102: What safeguards are needed to ensure specified material informs risk management without becoming a de facto prescriptive control list?

Question 104: How should the framework operate where specified material overlaps with another legal, regulatory, contractual or operational requirement?

We note that the risk information material will sit outside statutory scrutiny, and as such, the legislative framework will need to provide for robust safeguards to ensure the measure remains proportionate in practice and fit for purpose.

Content and scope

There should be clear statutory limits in relation to the content and scope of the specified material, so that it aligns with the existing CIRMP framework. This includes confining the risk information to the hazards already established under the CIRMP framework, rather than introducing new risk categories.

The specified material should also not direct any controls or actions to be taken, though best practice guidance and suggestions to support responsible entities manage the identified risks should be provided.

Entity's response

The legislation should also specify that entity responses need only be proportionate to the risk identified in the specified material and the entity's own risk context. The relevance and applicability of the risk information should be assessed by the responsible entity itself, and where the responsible entity reasonably considers that the risk information does not apply, it should not be required to take any further action other than to consider the risk information and determine its limited applicability on its asset(s).

The responsible entity should likewise determine the necessary actions to be taken, timeframe for actions to be implemented, and method of implementation for itself, in a manner that reflects its own risk profile, rather than being directed to adopt controls prescribed by the material.

Overlap with other obligations

The legislation should explicitly provide that an entity does not fail to comply with the proposed obligation where it is constrained from taking action under the specified material due to other legal, regulatory, contractual or operational requirements. Consideration of the specified material, a good faith attempt to manage the risk in a manner that does not conflict with the entity's other obligations and clear documentation of this interaction and the actions taken, should satisfy an entity's compliance with the obligation.

Question 103: What accessibility, timing, notification or guidance settings are needed so affected entities can reasonably comply once material is specified?

In addition to the above safeguards recommended in response to Question 102, we note the below settings required to ensure entities are given a reasonable opportunity to consider the specified material.

Government must establish multiple, clear communication channels to ensure responsible entities actually receive the relevant risk information. At minimum, this includes publication on the CISC website, via the Trusted Information Sharing Network (TISN), and importantly, via the relevant regulator and government Department/agency for that sector (for example, in the case of telecommunications, both the ACMA and the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts). We note there is currently no subscription or mailing list maintained by the CISC to notify entities of new resources as they are published. We request that a notification feature is developed so that entities can subscribe to be notified when risk information is published.

Additionally, we welcome the intent to provide supporting information in a plain-language and accessible format to support compliance efforts.

We consider that entities should be given at least 30 days from the date the specified material is provided to consider the material. Importantly, this timeframe should not be to take actions or respond to the specified material, and only relates to providing entities with a reasonable period to actually receive the specified material, and consider it, noting the likelihood of entities being unaware of any new material.

As mentioned above, responsible entities should be allowed to determine the appropriate timeframe to implement actions in response to specified material. We note that depending on the nature of the identified risk, actions required, governance processes and the size and resources of the entity makes it difficult to establish what should be considered a reasonable time for implementation.

Measure 21 — Critical Workers and Critical Components Definitions

Question 105: Does an objective, access-based and authority-based definition better identify the people whose role, access or authority gives rise to personnel-security risk for critical infrastructure assets?

We support the measure in principle, and appreciate the policy intent. However, we do not agree that different obligations, controls or checking requirements should apply depending on the class of the critical worker. Rather, the legislative framework should recognise that different obligations, controls or checking requirements should be pursued in accordance with the risk posed by each critical worker depending on the degree of sensitivity of the access or information, the level of operational authority, and the potential impact should that access or authority be compromised or exploited.

Question 106: What kinds of security-sensitive access, operational authority, information holdings, systems, facilities or locations should be specified in the Act or Rules?

The legislative framework must be careful in prescribing what level of access or operational authority should constitute a worker being considered 'critical' for the purposes of the SOCI Act and CIRMP.

For example, in many cases, mere knowledge of, or access to information about, network configuration or design should not, on its own, make someone a 'critical worker'. Marketing staff, for instance, may hold design and configuration information for communications or promotional purposes, but have no operational authority over the relevant systems and therefore pose no meaningful risk if that information were compromised.

Hence again, we reiterate the importance of calibrating the classification to the degree of risk.

Question 107: Does the proposed approach to critical components provide a workable balance between an Act-level concept and Rules-based specification for different sectors, asset classes and circumstances?

Similar to our concerns raised in response to Question 106, we are concerned that this approach of specifying components of an asset to be treated as critical is unduly prescriptive. We reiterate the importance of keeping the framework proportionate and practicable, rather than prescribing a blanket list of components.

To the extent Government considers that there is currently a gap between what components should be considered critical, this should be addressed through guidance which should establish what sort of components are likely to be critical, and under what contexts. We believe this preserves proportionality and reflects the existing principle that entities are best placed to determine what is genuinely critical within their own environment.

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the Consultation Paper on Streamlining and Modernising the *Security of Critical Infrastructure Act 2018*. We reiterate our commitment to working with Government and other stakeholders to continue improving Australia's national security and resilience posture. To that end, we look forward to engaging further on the proposed legislative reform to ensure the SOCI framework remains fit-for-purpose, consistent with the proportionate and practicable approach underpinning the framework to encourage meaningful compliance that will better serve Australia's national security.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia Ltd (**IAA**) is a not-for-profit member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (**WAIA**), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations, and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IAA regularly engages with government and regulatory bodies on policy matters affecting the Internet industry. In particular, our advocacy efforts represent the small to medium sized internet service providers in Australia who are often disproportionately disadvantaged by law reform affecting the telecommunications sector. Our public policy work is guided by the following principles:

We stand for an internet for the common good

We stand for an open internet platform

We stand for measured, effective and practical regulation

IAA is also a licenced telecommunications carrier and provides the IX-Australia service to Corporate and Affiliate members on a not-for-profit basis. It is the longest running carrier neutral Internet Exchange in Australia. Spanning seven states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.