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

25 October 2024

To the Committee Secretary
Parliamentary Joint Committee on Intelligence and Security

PO Box 6021
Parliament House
Canberra ACT 2600

By submission: https://www.aph.gov.au/Parliamentary_Business/Committees/OnlineSubmission

RE: Cyber Security Legislative Package 2024

Thank you for the opportunity to express feedback on the Cyber Security Legislative Package. The Internet Association of Australia Ltd (**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**).

Our response to the inquiry of the Parliamentary Joint Committee on Intelligence and Security (**Committee**) is thus primarily in representation of these members, as well as for the general public good of the Internet, and broader telecommunications industry. IAA is also a licensed telecommunications carrier, in its operation of Internet exchanges across Australia, and would therefore also be subject to many of the obligations introduced by the proposed cyber security and critical infrastructure legislation.

From the outset, we express our support of the government's initiative in introducing legislation to establish a regulatory framework that is fit for the modern digital era. We have thus been actively engaged in the consultation surrounding the cyber security legislation, responding to various rounds of consultation. We also appreciate the opportunity to continue to contribute to the effort to uplift Australia's cyber security systems. However, we are also concerned that some of the feedback provided in previous consultations has not been addressed.

We believe that in order to ensure compliance and therefore, be effective in achieving greater security and resilience as per the legislative objectives, such legislation must be measured and practicable. Moreover, we are concerned that some of the proposed reforms, and in particular, the definitions, are too broad and vague, making certain obligations unnecessarily onerous and go beyond the legislative intent. We offer our response below in sincere hopes it will contribute to the development of legislation that are effective and fit for purpose that will improve the cyber security posture and resilience of Australia's critical infrastructure ecosystem.

OUR RESPONSE

SECURITY OF CRITICAL INFRASTRUCTURE AND OTHER LEGISLATION AMENDMENT (ENHANCED RESPONSE AND PREVENTION) BILL 2024

Definition of 'incident'

We understand that the government seeks to broaden the scope of the types of 'incidents' for the purposes of Part 3A of the Security of Critical Infrastructure Act (**SOCI Act**) in line with its all-hazard approach. However, we are concerned that the term 'incidents' has not been defined under the proposed *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024* (**SOCI Reforms Bill**) and is therefore unclear in what situations certain powers could be invoked by the Secretary or Minister in response to such 'incidents' arising. Indeed this term potentially enables an extremely broad set of cases that, should they be included, would lead to significant imposts on Agency time and effort to process irrelevant notifications, as well as that of industry in making the notifications themselves.

Similarly, 'serious incident' is not defined and causes further confusion as to the distinction between an 'incident' as opposed to a 'serious incident', and the legislative obligations and implications of a 'serious incident' occurring.

Definition of 'critical telecommunications asset'

We also believe that changes to the definition of 'critical telecommunications asset' as per section 6 of Schedule 5 to the SOCI Reforms Bill are too broad and would unnecessarily and likely inappropriately capture various telecommunications systems, given the similarly broad definition of 'carriage service'.

This in turn would result in greater regulatory burden on entities, which has a disproportionate effect on smaller telecommunications providers who lack the resources to unpack complex legislation with vague and broad definitions. It also goes beyond the legislative intent of the reforms, especially when it comes to compliance with specific obligations. For example, with regard to the asset register obligations that is likely to be consolidated to apply to telecommunications providers under the SOCI Act framework in due course, this would result in too much information neding to be notified to the ASD, and would go beyond what is necessary for the ASD to understand the landscape of Australia's critical infrastructure ecosystem. This would also increase the potential of the creation of a honeypot of information about critical infrastructure assets that could likely become a target for malicious actors.

We especially note that there has been ongoing consultation with the telecommunications sector, including with the Australian Telecommunications Sector Reference Group, particularly with regard to 'switching on' the risk management program rules, as well as consolidating the other positive security obligations under the SOCI Act as they apply to telecommunications providers. Such sector-specific engagement has been in recognition of the unique and complex landscape of the telecommunication sector that requires thresholds and carve-outs for smaller carriage service providers. Thus, the broad definition of 'critical telecommunications asset' is not aligned with this approach to consolidating security obligations for the telecommunications sector and making it easier for smaller telecommunications providers who do not need to be unnecessarily burdened by the SOCI framework.

As consultation on the subordinate critical infrastructure legislation for telecommunications continues, we look forward to continue consulting with the government, industry and other stakeholders to ensure such legislation is fit for purpose.

CYBER SECURITY BILL 2024

Definitions of 'internet connectable product' and 'network connectable product'

We understand that the security standards that apply to specified classes of relevant connectable products will be subject to subordinate legislation that has yet to be drafted. However, given the broad definitions for 'internet-connectable product' and 'network-connectable product' as per the proposed *Cyber Security Bill 2024* (**Cyber Security Bill**), we are concerned that the classes specified in the subordinate legislation will unnecessarily capture telecommunications equipment and products that are already subject to existing regulations. We note the existence of rules that apply to the telecommunications sector under Standards developed by the ACMA[1] and Communications Alliance.[2] We strongly urge the government to refer to the extensive regulation that applies to telecommunications products, and sufficiently limit the classes of relevant connectable products that would be subject to new subordinate legislation intended to create security frameworks for IOT devices.

Security standards for smart devices

We understand that the specific standards for smart devices will be set out in subordinate legislation as set out in section 14 of the Cyber Security Bill which we expect will be subject to consultation in due course. We take this opportunity to note that any such standards should specify that relevant connectable products should manufactured with sufficient basic security and mechanisms for updates so they are fit for purpose.

Coordination of major cyber security incidents

For clarity, under subsection 35(3) of the Cyber Security Bill, there should be another Note 2 that clearly states that although there is no obligation to provide information to a request for the National Cyber Security Coordinator (**NCSC**), this does not affect any other obligations an entity may have to report a cyber security incident under other legislation, such as the SOCI Act. We understand and appreciate that this is already provided for by way of section 44 of the Cyber Security Bill. However, we note that smaller entities, such as many of the ISPs that IAA represent, often do not have dedicated regulatory or legal teams, and do not have the capacity to dissect multiple pieces of legislation, and the various bodies that exist under Australia's expanding cyber security and critical infrastructure framework. Thus to avoid any confusion, we would appreciate including another note that clarifies an entity's obligations in the case of a cyber security incident. The note could instead point out the provision set out in section 44.

We are also concerned that the provisions under Division 3 of Part 4 of the Cyber Security Bill do not give enough assurance to encourage entities to share information to the NCSC. We acknowledge and appreciate that sections 42 and 43 attempt to reassure entities that information voluntarily given to the NCSC will not be used as admissible evidence in, nor will the NCSC be compellable as a

[1] Please refer to list of technical standards as regulated by the ACMA: https://www.acma.gov.au/technical-standards#telecommunications-standards

[2] Please refer to list of technical standards as developed by the Communications Alliance body: https://www.commsalliance.com.au/Documents/all/Standards

witness in criminal or civil proceedings. However, we do not believe this is sufficient, given the breadth of situations where information voluntarily submitted to the NCSC may be shared with other agencies and bodies under sections 38 to 39. We appreciate that information sharing is necessary and important to ensure the government has a sound understanding of the threat landscape. However, given the current drafting, we are not convinced that entities will feel adequately reassured so as to share information freely with the NCSC, thereby defying the legislative intent of the functions of the NCSC.

Cyber Incident Review Board

In general, we are concerned about the lack of oversight over, and accountability of, the Cyber Incident Review Board (**CIRB**). Its powers seem to be quite broad and there do not appear to be sufficient protections to entities and the information provided by entities.

Protection of Sensitive Information

We believe that section 49 powers to require entities to produce documents should be subject to provisions that establish certain considerations that the CIRB must take into account before invoking this power. Considerations should include at the very least, the criticality of the document for the CIRB's review, whether the CIRB can conduct its investigations without the document, and the sensitivity of the information contained in the document(s). Furthermore, these powers should only be invoked following consultation with the entity.

CONCLUSION

Once again, IAA greatly appreciates the opportunity to continue contributing to the reform of Australia's cyber security and critical infrastructure legislative frameworks. We understand the increasing threat level in today's digital age will only continue as we become more reliant on digital and evolving technologies, and therefore the need to ensure we have appropriate legislative protections in place. To that end, we are committed to working with government and other stakeholders to establish practicable and fit-for-purpose regulatory frameworks that will improve Australia's security and resilience.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia (IAA) is a 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.

IX-Australia is a service provided by the Internet Association of Australia to Corporate and Affiliate members. 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.

IAA is also a licenced telecommunications carrier, and operates on a not-for-profit basis.

Yours faithfully,

Narelle Clark
Chief Executive Officer
Internet Association of Australia