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

13 February 2025

Department of Home Affairs

PO Box 25
Belconnen ACT 2616

By submission: https://www.cisc.gov.au/resources/online-forms/consultation-on-subordinate-legislation-form

RE: Cyber Security Legislative Package - Subordinate Legislation

The Internet Association of Australia Ltd (**IAA**) thanks the Department of Home Affairs (**Department**) for the opportunity to respond to its consultation on the subordinate legislation to the *Cyber Security Act 2024* and *Security of Critical Infrastructure Act 2018* (**SOCI Act**). We greatly appreciate the Department's continued engagement with industry to ensure a legislative framework that will improve Australia's cyber security and protection of its critical infrastructure. IAA has been consistently involved throughout the various iterative consultation processes in relation to the cyber security legislative package, and we are keen to continue engaging with the Department, industry and other stakeholders to ensure the passage of remaining subordinate instruments that are practicable, measured and effective.

As a member-based association representing Australia's Internet community in the telecommunications sector, as well as a licensed carrier, this response will primarily focus the legislative instruments that affects the telecommunications sector. We especially note that our membership is largely comprised of small to medium sized carriage service providers (**CSPs**), a disproportionately underrepresented cohort in formal consultation processes. We therefore use this opportunity to highlight concerns arising from the subordinate legislation that would particularly affect smaller telecommunication providers.

OUR RESPONSE

RELEVANT CARRIAGE SERVICE PROVIDER ASSET

In general, we support the threshold established under the *Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2024* (**TSRMP Rules**) via the demarcation of a 'relevant carriage service provider asset' (**relevant CSP asset**). However, we are concerned that the TSRMP Rules do not explicitly ensure that CSPs who do not meet the threshold of owning or operating relevant CSP assets are sufficiently exempted from other ancillary obligations relating to its critical telecommunication assets.

We note that although a CSP may not own or operate relevant CSP assets, its assets would still constitute a critical infrastructure asset for the purposes of the overarching SOCI Act by way of section 9(a) and the broad definition of 'critical telecommunications asset' under section 5 of the

SOCI Act. Paragraph 9(2)(a) of the SOCI Act provides that the rules may prescribe that a specified critical telecommunications asset is *not* a critical infrastructure asset. However, the TSRMP Rules, the existing *Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022* and *Security of Critical Infrastructure (Application) Amendment (Critical Telecommunications Assets) Rules 2024* (**SOCI Application Telecommunications Rules**) do not prescribe a CSP's assets that are not a relevant CSP asset as not being a critical infrastructure asset. Rather, the TSRMP Rules and the SOCI Application Telecommunications Rules have been drafted in such a way so that only relevant CSP assets are subject to the positive security obligations under the overarching SOCI Act:

- Register of critical infrastructure assets (Part 2);
- Critical infrastructure risk management programs (Part 2A); and
- Notification of cyber security incidents (Part 2B).

This means that other obligations relating to critical infrastructure assets more generally still apply, or have the potential to apply, to CSPs and their telecommunications assets. We understand that the intention of this particular drafting was to ensure that CSPs and their telecommunications assets would still be captured for the purposes of the below provisions:

- Enhanced security regulation for critical telecommunications assets (Part 2D – not yet compiled);
- Directions by the Minister (Part 3);
- Responding to serious incidents (Part 3A); and
- Gathering and using information (Part 4).

However, we are concerned that the nature of this drafting approach means there are additional obligations that apply to CSPs that do not own or operate relevant CSP assets, in excess of intentions of the Government, as specified below.

Data Storage System Rules may inappropriately catch CSPs

Following the recent enactment of the *Security of the Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024*, section 9(7) of the SOCI Act now prescribes the data storage system of a responsible entity used in connection with the entity's critical infrastructure as also being part of that critical infrastructure asset (subject to the conditions set out in paragraphs (a) to (d)). We understand that this data storage system, is distinguished from a data storage or processing asset which itself is a critical infrastructure asset class. We further understand that the intent of this new provision is to ensure responsible entities also comply with the positive security obligations in respect of their data storage systems.

However, as per the above analysis of the definitions, it is our view that the language used in the legislation does not sufficiently make clear that carriage service providers are not subject to the positive security obligations (Parts 2, 2A and 2B) in respect of their *data storage systems*. We appreciate that this is not the legislative intent. However, we would appreciate if this was explicitly expressed in the TSRMP Rules and SOCI Application Telecommunications Rules with a note that a CSP that does not own or operate relevant CSP assets are also not required to comply with obligations under Parts 2, 2A and 2B in respect of their *data storage systems*. We would also appreciate this to be clearly set out in any guidance material developed by the Department in relation to the new rules affecting the telecommunications sector.

Obligation to notify data storage or processing provider is unnecessary

According to the Explanatory Document provided by the Department in relation to the Security of Critical Infrastructure Rules, the Government intends to capture CSPs that do not own or operate relevant CSP assets under section 12F(3) of the SOCI Act, relating to the obligation to notify data service providers (**DSPs**) that the DSP is storing or processing data that relates to critical infrastructure of the CSP. We do not understand why this is necessary, and respectfully disagree that CSPs should so be captured by this obligation.

This obligation has the potential to effectively switch on obligations for that DSP, as the DSP is then also considered to be a responsible entity for a critical infrastructure asset, and must then also be compliant with positive security obligations in relation to its assets. We believe this to be a similar scenario to the one described above regarding a CSP's obligations in relation to its data storage system wherein the DSP would face positive security obligations in relation to its assets as a result of the CSP's data, despite the fact that the CSP itself would not be subject to those same obligations in respect of its telecommunications assets.

This may not affect DSPs that would otherwise be subject to those positive security obligations by virtue of providing data storage or processing services for other government clients (section 12F(1) of the SOCI Act) or other responsible entities of critical infrastructure assets (section 12F(2).[1] However, for those DSPs that would not otherwise be subject to those obligations, by becoming notified by a CSP that does not own or operate *relevant CSP assets*, but are still considered to own or operate *critical telecommunications assets*, that DSP would now also be captured by the SOCI Act. We believe this to be an overreach and do not understand why those DSPs should be so captured.

We therefore request that the TSRMP Rules or the SOCI Application Telecommunications Rules (as applicable) are amended so as to exempt CSPs that do not own or operate relevant any CSP asset/s from its notification obligations under section 12F(3).

MANAGED SERVICE PROVIDERS NEED A BUSINESS UNIT DEMARCATION OPTION

We are also concerned about the breadth of the data storage and processing providers captured by the SOCI Act more generally. We note that many CSPs are also managed service providers (**MSPs**) and provide a broad range of services, and would likely be or potentially be considered 'data storage or processing providers' for the purposes of the SOCI Act. This is due to the extremely broad definition of data storage or processing service under section 5 which does not clearly or separately define 'data processing'.

Many CSPs are MSPs provide specialised services for government clients, or for other entities that would be a responsible entity of a critical infrastructure asset. This would mean that despite not owning or operating relevant CSP assets, they would still be subject to the positive security obligations in respect of their data storage or processing assets. However, this would cause great and arguably undue, regulatory burden on smaller MSPs, especially in relation to the risk management program obligations. In particular, for the purposes of the requirement to comply with a cyber security framework in accordance with section 8(3) of the *Security of Critical Infrastructure*

[1] For clarity, where those other clients are entities that are **not** CSPs that do not meet the threshold of relevant critical infrastructure assets.

(Critical infrastructure risk management program) Rules (LIN 23/006) 2023 (**CIRMP Rules**), it is not practicable for an entity to demarcate its business units for the purposes of achieving compliance with the security framework, and segregate areas and assets that only relate to its data storage and processing services. A CSP that is also an MSP cannot simply carve out sections of its operations and systems to ensure only those that are strictly data storage and processing assets are compliant, and will likely end up having to comply with the CIRMP Rules for the whole of its systems and assets. We understand that many small MSPs operate as niche service providers for government entities, and by subjecting them to these CIRMP Rules, would introduce a huge regulatory impost that could cripple businesses, and therefore not in the best interest of the wider Australian economy in terms of ensuring a thriving, innovative industry with healthy competition.

Furthermore, given that MSPs that do indeed supply to government are already subject to various security obligations, including cyber security obligations, due to the contractual arrangements in place, we consider the application of the CIRMP Rules as unnecessary. We understand that government entities already have procurement security risk consideration requirements, and therefore any contractual arrangements with an MSP would set out the necessary security principles.

However, we understand these are not matters that can be resolved by the subordinate legislation currently being consulted on. However, we do consider this a significant issue that should be addressed, and we would greatly appreciate if the Department could draft subordinate legislation in respect of the data storage and processing sector, and engage in further consultation with the data storage and processing sector, particularly in relation to those smaller providers.

WE RECOMMEND THE TIA ACT EXEMPTION MODEL BE INCORPORATED

Finally, we reiterate the need for an exemption model to ensure select carriers are excluded from the regulatory burdens that would be imposed. We understand that the Government has not introduced a threshold for carriers in the same way that the 'relevant CSP asset' threshold has been set out for CSPs. We further understand that this is due to the role that carriers play in the overall telecommunications network as the underlying infrastructure provider for communications. While we generally agree with and support this approach, we do importantly note that not all carriers play such a critical role in the overall telecommunications network.

By way of example, we reiterate that IAA itself is a licensed carrier as we own and operate a very limited number of dark fibre cables as part of our overall network architecture for operating Internet Exchanges (**IXes**). An IX serves as a nexus where multiple networks (including ISPs, enterprise providers, and content providers) connect to exchange internet protocol traffic directly. This has the benefit of ensuring faster speed, improved resilience and reduced costs, and therefore also benefits end-users of the Internet.

While we view this service and this work critical in the sense that it significantly reduces latency, and reflects a much more efficient network set up, we do not consider that this is the sort of network that Government intends to capture as 'critical' for the purposes of the SOCI Act. Indeed, though IAA operates various IXs across Australia, only one IX incorporates cables owned by IAA, and we are in principle, able to operate IXes without such line links. Additionally, should our network experience an incident, the impact this would have on the end-user is vastly different to the sort of impact that would result due to a network failure of an underlying infrastructure provider such as one of the

large telecommunications providers. The end-user would still be able to connect to the Internet and at most, *may* experience some delay in speed.

Thus, we have consistently raised that there should be a carrier exemption to ensure that select telecommunications entities are properly scoped out of the SOCI framework. Due to the breadth of the telecommunications sector, there are various reasons why an entity may hold a carrier licence, and why they may operate a network unit or facility, which is defined in the *Telecommunications Act 1997* to include as little as a *single* line link connecting distinct places that are over 500 metres apart. Not all of these carriers would constitute the sort of network infrastructure providers that are considered critical by the Government for the purposes of the SOCI framework. However, we understand that this makes it equally difficult for Government to define and set out a threshold to appropriately demarcate what sort of carriers are or are not considered critical for the purposes of the SOCI Act.

Thus, we have recommended the exemption model set out in Division 3 of Part 5-1A and Division 2 of Part 5-3 of the *Telecommunications (Interception and Access) Act 1979* (**TIA Act**). Given the difficulty in scoping out an appropriate threshold for exempt carriers, an exemption framework modelled after those contained in the TIA Act would place the onus on the carrier to submit an application for exemption including a sufficient explanation why it is not 'critical' for the purposes of the SOCI Act. This then provides the Minister of Home Affairs (or other designated personnel, as seen fit) with the power to consider such an application, and in the event that it is determined that the carrier operates a network of a kind that should so be deemed critical, the application can be rejected. Furthermore, we consider that this exemption model will also allow Government a deeper and more holistic insight into the breadth of the telecommunications industry as it provides an opportunity for the various types of carriers to explain the nature of its business and networks.

Given the nature of this exemption model, we consider that it may also be possible to extend the exemption so as to also apply to MSPs that are considered DSPs under subordinate legislation relating to DSPs. This may be an efficient way to resolve the issue identified above about the undue burdens placed on DSPs.

Furthermore, we understand that the Department has not received much feedback in relation to the exemption model, including from other carriers. It is our view that many of the small carriers that would so be unnecessarily burdened by the positive security obligations under the SOCI framework are often underrepresented in consultation processes. Due to their lack of resources, many of these small carriers are not able to engage in consultation, and may possibly be unaware of the regulatory reform.

ACMA COORDINATION AND LIAISON NEEDED TO BETTER PROMOTE COMPLIANCE

We therefore also use this opportunity to urge the Department to engage closely with the Australian Communications and Media Authority (**ACMA**) to raise awareness amongst small carriers, and CSPs. We particularly note that the Carrier Application Form[2] managed by the ACMA sets out compliance information under Section 6 of the Application Form, which sets out amongst other things, a carrier's obligations to comply with Part 14 of the *Telecommunications Act*. However, the Application Form does not include the security obligations such as the asset registration and mandatory notification requirements despite these obligations having been in place for the sector since 2022

[2] https://www.acma.gov.au/publications/2019-11/form/form-t033-application-carrier-licence

under the SOCI Act equivalent legislative instruments[3] for the telecommunications sector. We therefore strongly encourage improved coordination and collaboration between government agencies and regulators to ensure consistency and clarity in their materials so that they reflect updated and accurate information to assist industry with its compliance efforts.

To that end, we also look forward to continue working with the Department in relation to the guidance material we understand it will develop in relation to the SOCI framework for the telecommunications sector.

CONCLUSION

Once again, IAA sincerely appreciates the opportunity to contribute to the subordinate legislation to the *Cyber Security Act 2024* and *Security of Critical Infrastructure Act 2018*. As we get closer to finalising the legislative material, we look forward to continue engaging with the Department, industry, regulators and other stakeholders to ensure a fit for purpose legislative framework, as well as accurate and appropriate supplementary material that will improve the security and resilience of not only the telecommunications sector, but the overall network of critical infrastructure in Australia.

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

[3] *Telecommunications (Carrier License Conditions – Security Information) Declaration 2022.*