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

29 March 2022

To: Department of Infrastructure,
Transport, Regional Development
and Communications

Thank you for the opportunity to express the Internet Association of Australia (IAA) perspective on the *Telecommunications (Carrier Licence Conditions – Security Information) Declaration 2022* and *Telecommunications (Carriage Service Provider – Security Information) Determination 2022*. Many of IAA's members are small to medium sized internet service providers (ISPs) who are also NBN retail service providers (RSPs). IAA also holds a carrier licence and would be subject to the new obligations. Our response is written on behalf of the interest of IAA, our members – particularly the smaller entities we represent, and for the general public good of the internet.

IAA and our members recognise the significant part that the telecommunications sector plays in the ecosystem of Australia's critical infrastructure. We understand the grave concerns due to the increasing risks to Australia's critical infrastructure and the growing threats to our industry. To this end, we are committed to cooperating with the government to ensure the safety of our systems, and therefore Australia's critical infrastructure. We acknowledge the work of the Department of Infrastructure, Transport, Regional Development and Communications (DITRDC) in developing rules to align the telecommunications sector with the obligations that will apply to other sectors as overseen by the Department of Home Affairs (DoHA).

It is on this basis therefore that we seek to raise our concerns with the extreme breadth of scope of these new rules, and the lack of clarity provided in some instances. We believe these factors will result in significant costs for the sector, which have a disproportionate burden for the smaller businesses we represent, and believe the proposed obligations and resulting costs to be counter to the objective of protecting Australia's critical infrastructure systems.

NEW CARRIER LICENCE CONDITION AND SERVICE PROVIDER RULE

REGISTER OF CRITICAL TELECOMMUNICATION ASSETS

We note the breadth of scope of the information that would be required under ss 12 and 13 of the respective instruments. The definition for "asset" being a "tangible asset owned or operated by a carrier or CSP and used to supply a carriage service" would encompass a very large range of property, especially given that the instruments will capture all carriers and essentially all CSPs under its scope of "eligible carriage service provider". We believe that not all "assets" are critical

to Australia's security, and should not be captured in the obligation to notify the Secretary of Home Affairs. IAA recommends that the provisions be amended so that only genuinely critical assets be required. In following, we recommend that an appropriate threshold for criticality be established in consultation with industry and included in the instruments.

In addition, the type of data that would be required under the definition of "operational information" is extremely extensive and therefore means that entities will need to keep record of and keep updating the Secretary about a great volume of data. Similarly, we note that the definition of "interest and control information" is also very comprehensive. Hence, we believe the reduced scope of "assets" to be extremely significant to ease the burden for business so as to avoid collating and securing data that is unnecessary or irrelevant to Australia's critical infrastructure. We also request that the government work with industry to develop a clear and standardised form for entities to complete in regard to "operational" and "interest and control" information to avoid any confusion, and assist with compliance.

Furthermore, we note that the current commencement date of six months following the commencement of the instrument under s 12(2)(b)(i) is not sufficient. In order for entities to develop a record containing the comprehensive extent of data required, and any software to be able to track any changes, industry ought to given sufficient time to build, test and implement the necessary systems. Given that these records will contain asset information which pertains to critical infrastructure, it is of particular importance that any systems that will host such data are secure and reliable.

MANDATORY REPORTING

Given the lack of clarity or finality on some of the terms contained in the instruments, it is difficult for us to comprehensively comment on the appropriateness or reasonableness of the provisions.

For example, under ss 10 and 11 of the instruments, "cyber security incidents" are distinguished from "critical cyber security incidents" which relates to an incident which has had, or is having, a "significant impact" on the availability of a carrier or CSP's assets. However, "significant impact" is defined to relate to "essential goods or services". We note that "essential goods or services" is not defined in the instruments, and we note that the definition of this term is a live discussion which requires further clarification, as this could substantially expand or reduce what type of security incidents are considered critical or not. In addition, the definitions for "cyber security incident" and "relevant impact" under s 11 will include a very broad range of cases of interference to systems that would then have to be reported. We believe the scope should be further clarified and limited to more strictly to matters of cyber security.

We also note that the "approved form" as required under the instruments has not been specified. We believe that it is important this remains technology neutral and request that businesses are given flexibility in the forms that are considered acceptable for providing notice.

There is an inconsistency in the notice that is required between the written report that is required following the initial oral reporting of a security incident. While s 10(4)(d) allows carriers/CSPs 84 hours following the initial oral report for critical cyber security incident, s 11(4)(d) provides for a substantially shorter period of only 48 hours. We recommend the amendment of s 11(4)(d) to make the time periods consistent, and implement the 84 hour period for both provisions. Given

that s 11 concerns non-critical security threats, we believe that this shorter time period is not necessary and would only create confusion for businesses as to their obligations.

ESTIMATED COSTS OF COMPLIANCE

Due to the restricted time period for this consultation and limited resources, we have been unable to fully quantify the costs of compliance for IAA and our members in numeric terms. However, we believe the costs of compliance will require an assessment of the following factors:

- Cost of staff time to assess, evaluate and then implement the new obligations
- Cost of recording all relevant information for initial reporting
- Cost to purchase/build/integrate new software to store and track data

We believe that the cost of complying with the obligations as it currently stands will be substantial for industry. Moreover, we raise our concerns for its particular adverse implications for the smaller entities IAA represents. Given the issue of competition and the high barriers to entry for new businesses which already exist for the telco sector, we are concerned that these obligations will further hold back innovation and competition in the industry.

CONCLUSION

Once again, I would like to thank the Department for providing us with the opportunity to contribute to the *Telecommunications (Carrier Licence Conditions – Security Information) Declaration 2022* and *Telecommunications (Carriage Service Provider – Security Information) Determination 2022*. IAA is committed to the development of rules for the telco sector which will assist the safety of Australia's critical infrastructure. We look forward to continuing to work with the government, industry, and other stakeholders to create measured, effective and practical rules to fulfil this purpose.

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 six 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