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

DATE: 1 March 2022

To: Parliamentary Joint Committee on Intelligence and Security

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

INTRODUCTION

Thank you for the opportunity to express the Internet Association of Australia (IAA) perspective on the review of the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* ('the Bill'). IAA participated in the consultation process held by the Department of Home Affairs on the Bill, and we greatly appreciate the chance to provide further response in its continued review of before it comes into effect. From the outset, IAA acknowledges the need for greater security measures to protect Australia's critical infrastructure. We recognise the growing security threat, particularly seen during the COVID-19 pandemic and we appreciate the efforts to conduct comprehensive reforms of security across various legislative instruments in recent years. However, we are concerned with the attempted implementation of the Bill which we view as premature as greater consultation is required with industry to clarify various aspects of the Bill.

Many of IAA's members are small to medium sized internet service providers (ISPs). Our response will largely be from the perspective of our smaller members as well as for the broader public good of the internet.

COMMITTEE QUESTIONS:

DID YOU PROVIDE FEEDBACK ON THE EXPOSURE DRAFT AND DO YOU FEEL LIKE THE CONSULTATION WAS INCLUSIVE AND WIDE RANGING?

IAA has been actively involved in the development process of the overarching reforms being undertaken to bolster Australia's security recently, particularly as it pertains to cyber security. We therefore submitted a response to Home Affairs on the Exposure Draft of the Bill which closed 1 February 2022.

We note that the consultation period was being held in conjunction with other reform proposals related to cyber security from Home Affairs including the Draft Security of Critical Infrastructure (Application) Rules, and the comprehensive reform of Australia's Electronic Surveillance Framework. Furthermore, these consultations commenced in December 2021, and closed early to

mid-February, running over the holiday season and at a time when many Australians were directly experiencing illness from the pandemic. Given the gravity of the issues being addressed in these reforms, we believe that greater time was required to give interested parties sufficient time to thoroughly respond to each reform, including the Exposure Draft.

In addition, the Bill has since been referred to the Committee only 10 days after submissions closed, and we further note that it has now already been introduced to the Lower House despite the inquiry still currently under way by the Committee, thus before the Committee's final report. Therefore, we raise our concerns that the implementation of the Bill may be being rushed and sufficient review and proper consideration of the feedback provided on the Bill is not being afforded. Given the scope and subject matter of the Bill, we strongly advise that this could have numerous serious adverse consequences for businesses as well as the wider Australian society and could furthermore result in greater security risks in contrast with the object of the Bill.

HAS YOUR FEEDBACK BEEN INCORPORATED IN THE BILL OR ADDRESSED IN EXPLANATORY MATERIAL?

The Bill reflects consideration of some matters raised in our feedback to the Exposure Draft. For example, we support the item 34 which clarifies the definition of 'critical data storage or processing asset' to ensure critical telecommunications assets will not be captured within its scope, as well as amendment to the definition of 'critical telecommunications assets' under item 11 as per industry request. However, we believe this is still insufficient to address the concerns raised by IAA and other industry organisations about the matters concerning the reasonableness of imposing burdens on entities, as well as the overreaching powers which will be granted to Home Affairs, as will be discussed further below.

WHAT ARE YOUR FIVE KEY THEMES OF FEEDBACK ON THE BILL?

Our position can be summarised under the following thematic concerns:

(i) Clarity

We believe that there needs to be much greater clarity as to the scope of the Bill with proper consideration of which entities will become subject to greater obligations. This should be accompanied with an explanation as to how and why these entities were assessed and determined. We are particularly concerned about its application on the telecommunications sector. Whilst the Bill notes that the rules may prescribe that a specified critical telecommunications asset is not a critical infrastructure asset, we note that s 9(3) of the *Security of Critical Infrastructure Act 2018*, which establishes the prescription of an asset as a critical infrastructure asset, is very broad. Furthermore, there is nothing in the Bill to suggest there are limitations established to determine when critical telecommunications assets should be considered a critical infrastructure asset.

In addition, we believe that in the case where an entity is determined to require greater security obligations, there needs to be greater clarity as to how to implement these new obligations, and the criteria for such that apply. As it currently stands, we believe it will be difficult for entities to

prepare their systems so that they will be able to comply with any new obligations when the Bill comes into effect and if they are called upon to do so.

This is particularly the case for our members who are smaller businesses in the telecommunication sector. Not only is it unclear in the Bill whether limits are in place to exclude smaller businesses from becoming subject to the enhanced obligations, the lack of clarity will make it extremely difficult for our members to comprehend and comply with any potential obligations.

(ii) Process

As mentioned above, IAA is deeply concerned with the short timeframe in which the Bill has gone through consultation and review to reintroduction to Parliament. We strongly believe that greater time needs to be spent working with industry and other stakeholders in the development of the Bill.

Furthermore, we note that potential timing issues exist as result of the Draft Application Rules which were also open for consultation at the same time as the Bill. As such, we believe the due diligence for the consultation, review and amendment process of the Bill and Rules should be prioritised to ensure no inconsistency and sufficient time and resources provided to assist businesses in preparing for the new obligations.

(iii) Reasonableness

In its current state, we believe that the Bill grants the Minister with likely overreaching powers, such as the ability to privately declare a critical infrastructure asset a SONS. This is an area we particularly believe requires amendment on the grounds it is unreasonable. The 28-day consultation period provided under s 52C is too short and unreasonable given the highly technical nature of the obligations. We believe that the consultation period should be increased, and extend our support to the position taken by Communications Alliance in their submission to Home Affairs' consultation regarding the Exposure Draft of the Bill that the period should be extended to at least 45 days.

Again, we reiterate the particularly onerous burdens that will be likely faced by smaller businesses which we represent. As such, we believe it is crucial that principles of reasonableness and proportionality are paramount considerations to ensure entities are not being unnecessarily burdened by potential greater security obligations.

(iv) Oversight

We strongly believe that an independent oversight mechanism should be set in place to ensure accountability. The enhanced security obligations would see entities subject to overreaching government powers and thus we believe it is crucial to the function of Australia's democracy that there is proper oversight of the use of such powers.

(v) Consistency and Overlap

IAA along with other industry organisations are concerned about the potential overlap with the currently existing security framework that exists for the telecommunications sector under the Telecommunications Sector Security Reforms. We note that this was addressed for the Draft Application Rules but as it pertains to the Bill, there is nothing to prevent the Minister from applying the enhanced obligations to telecommunications carriers and/or carriage service providers. We believe that the Bill should address this potential for duplicated obligations.

DO YOU THINK THE POTENTIAL REGULATORY IMPACT HAS BEEN CAPTURED ACCURATELY?

As it stands, we believe that industry has not been given sufficient time or materials to adequately review Home Affairs' assessment of the potential regulatory impact of the Bill. We emphasise our request made in our original response to Home Affairs that a proper cost-benefit assessment should be conducted for the proposed reforms.

For example, one of our key concerns pertains to s 30DJ of the Bill which may require entities to install system information software determined by the government. We believe this to be an extreme overreach in government powers and also gives rise to several serious issues. Contrary to its intention, we believe that such a measure will become a security liability. We believe that a thorough cost-benefit and security assessment on measures like these are necessary and that industry should be given the opportunity to properly scrutinise any such assessments to ensure the Bill is measured, robust, and actually able to serve the functions it seeks to achieve.

ON BALANCE, DO YOU SUPORT THE BILL IN ITS PRESENTED FORM, RECOGNISING THE RISKS FACING CRITICAL INFRASTRUCTURE ASSETS IN AUSTRALIA?

IAA reiterates our support for the Bill in principle, recognising the efforts to bolster Australia's security. However, on balance, we believe that the Bill in its presented form has not undergone sufficient scrutiny and that further consultation between Government, industry and other relevant stakeholders is necessary to ensure a reasonable, efficient, and measured approach to managing Australia's critical security.

Once again, IAA appreciates the opportunity to contribute to the inquiry on the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*. We sincerely hope to continue engaging with government as well as other stakeholders in continued consultation regarding the Bill before its passage through Parliament.

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 and lowest cost 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