1 February 2022

To: Department of Home Affairs

By Email: CI.Reforms@homeaffairs.gov.au

Introduction

Thank you for the opportunity to express the Internet Association of Australia (IAA) perspective on the *Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*. IAA acknowledges the importance of ensuring Australia's critical infrastructure is secure and protected, particularly in the global context which has increasingly seen systems more vulnerable to external events and attacks.

Many of IAA's members are small to medium sized internet service providers (ISPs) and also include domain name systems and data storage or processing businesses. This submission is written from the perspective of our members, and for the general well-being of the internet.

Sector and Critical Infrastructure Asset Thresholds and Definitions

IAA recognises the greater clarity provided under the Bill through the sector specific definitions and appreciates the effort in consulting with industry to further clarify the amendments which would come into place under the Bill.

IAA requests that the new rules the Minister would be allowed to create in relation to critical domain name systems will only be made following continued consultation with industry stakeholders. It is of paramount importance that such rules will not be overly burdensome on entities and will only be created to the extent it is intended to strengthen the security of Australia's critical infrastructure.

Similarly, IAA notes of the increased number of businesses which would be captured under the new definition for the data storage or processing service sector. We emphasise the need for continued consultation with industry to ensure only the entities necessary and relevant to be captured are being required to comply with the new obligations.

Positive Security Obligations

Risk Management Program

IAA welcomes the principles-based approach of the Risk Management Program (RMP). We emphasise that entities are best placed to understand the risks posed to their operations and the ways in which to develop and manage the appropriate risk mitigation practices. However, whilst we support entities being trusted to follow the procedures appropriate to their business, it is also true that entities will be bearing the full costs of the additional resources required to undertake the comprehensive processes under the RMP. Thus, we believe greater guidance and support is required to assist entities in the development and implementation of the RMP.

Furthermore, IAA raises concerns over any penalties which would apply for failure to comply with the RMP requirements. We oppose the pecuniary penalty that could see businesses liable for amounts potentially greater than $40,000. We support the intentions stated in the explanatory document that the compliance approach is intended to be education and awareness raising. IAA recommends that comprehensive support materials and guidance be provided to supplement the principles-based requirements of the RMP and that any failure in compliance take a more conciliatory and collaborative approach.

IAA also recommends that safeguards be implemented to avoid excessive and unwarranted background checking of staff to ensure the privacy of individuals is maintained. Any overly strict regimen of background requirements may also further exacerbate the skills shortages already experienced within the ICT industry with no real net benefit.

Enhanced Cyber Security Obligations

Declaration of Systems of National Significance

IAA recognises that the increasingly interconnected and digital landscape of the systems which underpin Australia's critical infrastructure gives rise to increased vulnerability and risk. However, given the great implications and responsibilities which an entity would be subject to following a 'System of National Significance' declaration, IAA requests the Minister be required to take into account greater and more stringent considerations in order to declare an asset. For example, the Minister should be required to provide a cost-benefit analysis to the entity which would be subject to a declaration.

Obligations

Given that following a declaration, deemed entities will still not necessarily be subject to all the enhanced cyber security obligations until following notice from the Minister, IAA recommends that further support material and guidance be provided to entities following a declaration to assist in their preparation to fulfil any further obligations. In addition, such support should be extended further to entities who are called upon to comply with one or more of the enhanced obligations. It is our view that these obligations will prove to be resource intensive for deemed entities.

In particular, IAA is concerned that an obligation to provide access to system information is likely to prove onerous for entities, and potentially give the government excessive control over the entity. We believe that while information sharing should be encouraged to foster collaboration, such direct intervention is an overreach of the government's powers over businesses.

Furthermore, as in the case of the RMP, IAA opposes the penalty currently in place of up to 200 penalty units for failure to comply with any of the enhanced obligations as being excessive.

Conclusion

Once again, IAA appreciates the opportunity to contribute to the consultation on the Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022. We look forward to representing our members and the broader public interest in continued engagement with the Department of Home Affairs, as well as other stakeholders, to ensure the development of a measured, effective and practical security approach to managing Australia's Critical Security.

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