INTERNET ASSOCIATION OF AUSTRALIA LTD
ABN 71 817 988 968
ACN 168 405 098
[redacted]

04 September 2025

Department of Home Affairs

By submission: https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/consultation-horizon-2-of-2023-2030-australian-cyber-security-strategy

RE: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy – Policy Discussion Paper

The Internet Association of Australia Ltd (**IAA**) thanks the Department of Home Affairs for the opportunity to respond to the consultation on its Discussion Paper on Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy.

From the outset, we commend the Australian Government for its continued focus on cyber security as the digital economy continues to grow and become increasingly integrated with our daily lives. We appreciate the Department's engagement efforts as the Government considers next steps to better secure Australia's digital future.

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**). IAA and our members are part of the telecommunications sector, which is now a critical infrastructure sector following reforms to the *Security of Critical Infrastructure Act 2018*. We are therefore very invested in the continued improvement of Australia's cyber security posture and have thus been active in engagement with the Department on policies relating to the critical infrastructure ecosystem and Australia's cyber security overall. Our response will primarily be in representation of our members that constitute the smaller providers within the telecommunications industry. As a not-for-profit association that advocates for an open Internet that operates for the common good, our response is also shaped by our interest in the public benefit of the Internet and all its end-users.

IAA's members present a unique perspective as small to medium sized businesses (**SMBs**) operating critical infrastructure, and thereby subject to higher regulatory standards while constrained by the limits faced by SMBs in terms of resources. We therefore promote a cyber security strategy that will proactively work with industry to uplift cyber security and resilience and prioritise effectiveness and proportionality. To that end, we raise some of our concerns in response to the Department's proposals for Horizon 2 below.

OUR RESPONSE

EVALUATION OF HORIZON 1

We recognise the immense work undertaken under Horizon 1 of the Cyber Security Strategy and commend the work of the Government, as well as all stakeholders in implementing significant reforms aimed at setting the foundations for strong cyber resilience, and addressing gaps within

Australia's cyber security posture. Furthermore, we empathise that due to the incredible pace of technological development and equally, the exploitation of such technologies by malicious actors, it is necessary to quickly look forward and consider next steps to ensure the continued maturation of Australia's cyber security and resilience.

However, it is not clear that there is enough information and data on the outcomes and results of the measures introduced under Horizon 1 to determine prudent next steps under Horizon 2. We note that many key legislative instruments including the *Cyber Security Act 2024*¸ *Security of Critical Infrastructure (Telecommunications Security Risk Management Program) Rules 2025* (**TSRMP Rules**) and *Cyber Security (Ransomware Payment Reporting) Rules 2025* were only introduced less than 12 months ago, with many of the requirements prescribed under the instruments not actually having commenced yet. We are therefore concerned that the timing of this consultation for Horizon 2 is too soon. Not only has there been insufficient time or evidence to assess the effectiveness of Horizon 1, there is also a real risk of consultation fatigue, thereby greatly diminishing the quality of engagement.

We appreciate that there will be an independent review of the SOCI Act in late 2025 and look forward to consulting on the findings of this review. However, we consider this review is too soon given that many of the subordinate legislation under the SOCI framework has only been recently introduced. We therefore recommend a staged approach to the review.

We also note that there is currently a significant consultation being held on economic reform being undertaken by the Treasury, with key input from the Productivity Commission. One of the core concerns as part of this reform is regulatory burden and alternatives to the current regulatory approach taken by the Government. It is unclear to what extent, if at all, the Department has considered these broader reforms to harmonise regulatory approaches and ensure efficiency.

CYBER SECURITY, CRITICAL INFRASTRUCTURE AND SMALL BUSINESSES

8. How can industry at all levels and government work together to drive the uptake of cyber security actions by SMBs and the NFP sector to enhance our national cyber resilience? What type of support would be useful and who should provide it?

33. How effective do you consider the SOCI Act is at protecting Australia's critical infrastructure from cyber attack? Are the current obligations proportionate, well-understood, and enforceable?

35. Is the regulatory burden on industry proportionate to the risk and outcomes being sought?

As expressed above, IAA's members hold a unique position of the industry as SMBs in the telecommunications sector. They thus face the double-burden of being under-resourced while facing more stringent regulation due to the importance of communications in Australia's overall critical infrastructure landscape.

We greatly appreciate that the Government has been cognisant of the burdens being placed on SMBs and the especially intensive work undertaken with the telecommunications industry via the Australian Telecommunications Security Reference Group in the development of bespoke risk management rules, alongside other obligations for the telecommunications sector. However, we consider that despite best efforts, the resulting rules are still too burdensome for SMBs in the sector, and do not reflect the proportionality that was sought during consultations.

For example, the TSRMP Rules capture all carriers without any exemption provisions to appropriately demarcate entities that do not in fact operate any infrastructure 'critical' to

Australia's economy or national security. Members have expressed feeling 'overlooked' and 'left behind' due to the legislative requirements, and the limited concerted effort on the part of Government and regulators to ensure that smaller operators within the sector to fully understand their obligations.

While we appreciate the existence of the TISN, including the refreshed weekly cross-sectoral webinars, as well as sector specific groups, we note that the barrier for entry can be quite high for smaller entities. Lack of resources means limited time to engage in these meetings and some smaller entities may be intimidated by the confidentiality requirements that is a pre-requisite for joining the TISN.

Furthermore, the strict confidentiality rules, as set out for TISN participation, do not reflect proportionality. In most cases, all documents shared in the TISN are prohibited from sharing with Member entities, meaning representative bodies such as ourselves are not able to fulfil our function to serve as a bridge between Government and regulators to disseminate information to SMBs that cannot engage in these forums directly. We consider that in majority of cases, the information shared amongst the TISN need not be rated as being of such a confidential nature. Thus, we recommend there should be a much more proportionate approach in determining what information and materials should be kept confidential, and what can be shared to improve the cyber security across industry.

17. Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues?

While we don't consider that the regulatory requirements in and of themselves to have a negative impact on cyber security, we do consider the approach taken in implementing reforms, as well as limited engagement opportunities severely limits effectiveness, and therefore the cyber maturity of organisations. The issues raised above risk SMBs feeling disillusioned by well-intentioned regulation, and therefore perceiving them only as tick-box exercises rather than meaningfully engaging to ensure robust cyber security and resilience.

However, the great volume of regulatory reform underway affecting the telecommunications sector overall and not just in the cyber security space negatively affects cyber maturity. Organisations do not have sufficient time to implement all the various reforms in a thorough manner, which can also severely limit the effectiveness of such regulation.

We reiterate the work being underway under the Economic Reform Roundtable and the considerations for the Government's regulatory approach with recommendations for streamlined regulatory reform that will minimise burdens for industry. We strongly recommend that any future reform undertaken under Horizon 2 be cognizant of other regulatory reforms going on to ensure industry has sufficient time to properly implement any changes.

We also strongly recommend that the proposed independent audit requirement to assess an entity's risk management be subject to further consultation and oppose its introduction under Horizon 2. At least for the telecommunications sector where the risk management program isn't due to commence until 4 October, it is far too soon to be contemplating a further set of requirements. We are concerned that introducing new requirements will erode trust between industry and Government and result in adverse outcomes.

11. Do you consider cyber insurance products to be affordable and accessible, particularly for SMBs? If not, what factors are holding back uptake of cyber insurance?

We consider this is still a space in development and providers are not yet providing cyber insurance products at accessible, affordable rates. This is considerably so in relation to telecommunications networks where the nature of the industry is considered to be of greater risk, thereby again severely

disadvantaging telecommunications operators that are also SMBs. Products are hard to assess, do not reflect some of the specialised services nor the expertise of those offering the services and it is difficult to find favourable value for money coverage.

36. What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices? What role should government play in enabling uplift, including through tools, guidance or incentives?

Lack of awareness is a fundamental issue for SMBs in the telecommunications sector. There needs to be concerted effort from Government, working with the ACMA as the regulator for the communications industry to produce clear, consistent and important, updated information about the cyber security obligations that apply to the telecommunications industry.

We greatly appreciate that previous requests for the Department to work with the ACMA to update its carrier licensing guide and carrier application form has been actioned with the ACMA updating these materials in August 2025. We recommend continued collaboration with the regulator as any further regulatory reform is introduced.

In particular, we would greatly appreciate if the Department works with the ACMA to publish updates to the telecommunications sector of any updates affecting industry in relation to critical infrastructure legislation or relevant cyber security legislation. As the ACMA administers the carrier register with contact information of the majority of industry, we consider this an efficient way to disseminate relevant information to boost awareness.

We further note the Government is now also considering introducing a registration scheme for carriage service providers to be administered by the ACMA, which will operate in a similar manner to the carrier licencing regime, we believe there is real opportunity for the various Government bodies and entities to work together to operate these arrangements in a way that is actually helpful for industry. Again, disseminating news and guidance material via the ACMA would be a practical step that can be taken to ensure SMBs are not left behind and left unaware about important regulatory changes.

We also recommend updates to the Critical Infrastructure Security Centre's website[1] to make it easier for entities to keep updated of reform as well as any new guidance material that can aid compliance efforts. In particular, we consider it would be useful to introduce a subscription capability so that entities can 'subscribe' to updates to the Resources being published by the CISC, thereby making such resources more accessible.

INTERNATIONAL CYBER NORMS AND STANDARDS

49. In which forums and on which issues would you like Australia to focus efforts to shape rules, norms and standards in line with its interests most effectively in Horizon 2?

We greatly appreciate and commend the Government's commitment to an open, secure and interoperable Internet. We consider the Internet Governance Forum, as well as the national and regional forums (auIGF and APrIGF) of great relevance that aligns with the interests of cyber security in Australia, as well as regionally and globally. We also note the 20-year review on the World Summit on the Information Society (WSIS+20) is currently underway and believe this to be critical to shaping the future of Internet governance that will be relevant to cyber security.

We understand that the Department of Communications is already significantly involved in these forums. However, it is unclear to what extent there has been collaboration with other Government

[1] https://www.cisc.gov.au/resources/pdf-documents

departments such as the Department of Home Affairs and Department of Foreign Affairs and Trade, as well as regulatory bodies to ensure consistency across sectors and all regulatory initiatives being deployed across Australia.

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the consultation on Horizon 2 of the 2023-2030 Australian Cyber Security Strategy. As cyber security continues to be a pressing concern for all Australians, we look forward to working with the Government, and other stakeholders to ensure the progression of the Cyber Security Strategy in a way that will deliver real benefits to ensure Australia's secure and resilient digital future.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia (IAA) is a not-for-profit 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.

IAA is also a licenced telecommunications carrier and provides the IX-Australia service to Corporate and Affiliate members on a not-for-profit basis. 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.

Yours faithfully,
Internet Association of Australia