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

14 April 2023

Strategy Expert Advisory Board
Department of Home Affairs

By email: auscyberstrategy@homeaffairs.gov.au

RE: 2023-2030 Australian Cyber Security Strategy Discussion Paper

INTRODUCTION

Thank you for the opportunity to express the Internet Association of Australia's (**IAA**) perspective on the 2023-2030 Australian Cyber Security Strategy Discussion Paper (**Discussion Paper**).

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**). This response is primarily written in representation of these members, as well as in support of the general well-being of the Internet and the Internet and telecommunications industry.

Given the nature of our sector, cyber security is a core issue that we are heavily invested in. We have been involved in various consultations with the Department of Home Affairs (**the Department**) and other government departments or agencies, civil society and industry for the development of other legislation and regulatory frameworks that concern, or are adjacent to, cybersecurity including those related to critical infrastructure.

IAA and our members appreciate the increasing level of risk to Australia's cyber security that threatens the stability of our economy and society. The increase in the volume and sophistication of cyber-attacks is unprecedented and poses a real issue to all Australians, including our sector. To that end, we recognise the work of the government in trying to uplift Australia's cyber security posture and resilience.

In order to achieve this, we strongly believe that the approach that must be taken is one of collaboration and development which prioritises active engagement with stakeholders to develop and implement measures that are actually effective as well as transparency to increase the level of trust between government, industry and the general public.

Our responses to the specific questions set out in the Discussion Paper are as follows.

OUR RESPONSE

CORE POLICY IDEAS AND REFORMS

Questions 1, 2a, 2b, 2d, 2e

We support the harmonisation of regulatory frameworks as proposed in the Discussion Paper. However, to clarify, we believe harmonisation as opposed to enhancement should be prioritised as harmonisation allows for greater compliance due to industry being able to understand and follow measures, which will in turn enhance the effectiveness of regulatory frameworks. This also implies increased collaboration, both internally, between government agencies and departments, but also external government and non-government stakeholders.

This is as opposed to what seems to be the current policy landscape where we have seen a great number of legislative reforms, many of which are at least in part, concerned with cyber security issues and pose new obligations for industry such as critical infrastructure, consumer data right, and privacy laws, all headed by different departments, with lack of clarity as to the way different frameworks will be operating alongside each other. This thereby creates a complex web of obligations that organisations need to comply with but struggle to understand. Rather than considering enhancement to the legislative or regulatory frameworks by expansion, clarification and simplification should be prioritised.

We strongly support regulatory guidance and active engagement with industry to be the mechanism that government prioritises to improve operational cyber security standards. We reiterate that current frameworks are difficult to follow and thus further expanding legislation and regulation is unlikely to improve this. What is needed is genuine and effective collaboration between government and industry to implement practical and effective solutions, rather than using the threat of penalties for non-compliance to create complex and ineffective business practices and procedures that are only implemented to prove compliance on paper.

Government should also work with industry, and conduct sector specific research into the costs involved with regulatory compliance, and assess the effectiveness of compliance in actual improvement to Australia's cyber security posture and resilience.

We do not support the expansion of the SOCI Act as considered in the Discussion Paper. This is likely to further obfuscate the complexity of legislative and regulatory frameworks. We appreciate that in our increasingly data-driven economy, customer data and systems should indeed be sufficiently protected. However, we do not see how inclusion into the SOCI Act would necessarily improve the safeguard the protection of data sets and systems.

Instead, the better approach would be to consider how government departments and agencies such as the CISC, ACSC, and OAIC, should work together in the case of such major data breaches to ensure a more holistic approach. Indeed, this may be a method of streamlining existing regulatory frameworks, as per question 2e. For example, one method would be to consider how the Notifiable Data Breach Scheme and Mandatory Incident Reporting may be harmonised to reduce the number of different notification obligations entities are subject to. A notification portal could be developed in such a way that different regulators and agencies are notified when a cyber incident relevant to its remit is submitted via the portal. Using this type of system, entities would only have to report once and the relevant information required by each agency or regulator is packaged and sent to the applicable recipient.

Similarly, we question the need for a new Cyber Security Act. Again, the priority of government should be to collaborate and work with industries to identify the pain points and where Australia's cyber security and resilience is lacking, where cyber security issues and threats currently exist, conduct joint research on how the threat landscape is likely to evolve, and develop solutions accordingly. If legislation is deemed necessary following such engagement, then the next steps should be to consider the development of a new instrument. However, we believe that considering the need for a new legislation – without details as to what this should include – illustrates misguided priorities that suggest legislation for the sake of legislation without real consideration as to what such an instrument would really achieve.

Question 8

We appreciate that confidentiality obligations may improve engagement between entities experiencing a cyber incident and agencies to assure organisations that they will not face penalties from regulators. However, in general, we support greater transparency overall. To clarify, we do not necessarily oppose the confidentiality obligations but believe that a more holistic approach is needed.

As such, we believe this goes again to the need for restructuring or reframing legislation so that rather than penalties and enforcement measures, priority is placed on encouraging compliance and supporting industry to implement cyber security best practices. In principle, it is not desirable that there isn't greater information sharing within and between government, regulatory bodies, and industry.

If there is to be legislative reform in this area, we strongly recommend the reconsideration of the framing of legislation to develop a way in which there can be greater transparency, without the fear of facing undue penalties.

The reality is that cyber attacks are only going to continue, and therefore, we need to learn from cyber incidents to improve our understanding of the threat landscape. Thus, both models of either restricting information sharing between agencies, or the threat of penalties discouraging organisations to report cyber incidents effectively result in reduced transparency and information sharing which ultimately impedes the development of cyber security practices and measures.

Question 13

We reiterate our support for the consideration of a single reporting portal for all cyber incidents to harmonise existing requirements. However, in consideration of our response to question 8, we also emphasise that any such reform resulting in a harmonised reporting framework be for the aim of simplifying compliance and encouraging greater information sharing, and not so that companies face greater penalties from different regulators. Indeed, in the reform process, we strongly recommend that government actively consider how this consequence of automatically notifying regulators may be mitigated.

In addition, overall, we believe that the government's response to major cyber incidents should be to prioritise organisations in containing incidents and mitigating the risk of harm to protect all Australians. This includes greater awareness raising and education amongst the Australian population with regards to data security and best practices online.

Question 2c

We acknowledge the principle behind specifically addressing cyber security risks and consequences for company directors' obligations. However, we reiterate that legislative reforms are not necessarily the best method of ensuring improvement of cyber security practices. Furthermore, we believe that with existing laws, recent legislative reforms and major cyber security incidents, there is already a growing understanding and acceptance by boards that cyber security is a real issue that must be sufficiently considered and accounted for. If there is evidence to suggest that this is lacking, particularly at the level of company boards, we strongly encourage the government to consider more collaborative approaches.

Furthermore, we assume that the level of recognition by company directors will differ according to industries and sectors. Thus, we recommend the government conduct further research into where there is the lack of understanding and work with those industries to ensure company directors across all sectors understand the importance of cyber security, to improve Australia's cyber security posture more generally, rather than applying blanket legislative obligations that only cause further friction between government and industry.

Questions 2f, 2g and 9

We recognise the complexity and difficulty of dealing with ransoms and extortion for both industry and government. We appreciate there are valid points on both sides of the argument for prohibiting payment of ransom demands, as well as not being punitive and the adverse consequences that may result in companies being even more unprotected and unsecure.

As such, rather than focusing on the prohibition of ransom payments, or in what circumstances they should be prohibited which is only considering cyber security from the lens of post-cyber incident, we strongly recommend the government to develop preventative methods so that ransomware attacks do not pose such a big issue.

Again, we posit that government should collaborate with industry, and in particular, make concerted effort to conduct sector specific engagement, in addition to wider multistakeholder inquiries. We believe this would be immensely beneficial in government identifying key and different issues affecting the different sectors, as well as learning ways to improve the security of systems as has been implemented in other industries.

With regards to the expansion of notification obligations of cyber security incidents, again, we posit whether harmonisation between the existing obligations could be implemented in such a way so as to over ransomware and extortion demands. In addition, if there are to be legislative reforms to include ransomware and extortion demands, we strongly recommend that government prioritises encouraging compliance as opposed to enforcement considerations.

GOVERNMENT BEST PRACTICE

Questions 6, 7, 15, 16, 20 and 21

We appreciate the consideration of how Commonwealth Government departments and agencies can better demonstrate and deliver cyber security best practice. We believe this is indeed an objective they should seek to achieve. However, in working to achieve this, we believe it is crucial that government looks to collaborating with industry rather than view it as an endeavour to undertake alone.

Realistically, we believe that it would be extremely difficult for government to demonstrate and develop best practice due to the knowledge and experience gap between government and certain industries or sectors. For example, as part of the Internet industry and broader telecommunications sector, we recognise our sector has a more mature understanding and often better practices when it comes to cyber security by nature of the industry.

We fully appreciate this doesn't make the telecommunications sector wholly resilient and immune to cyber incidents, as was clearly demonstrated in both the Optus and Telstra data breaches of late 2022. However, this is why it is so critical for there to be more proactive and in-depth engagement between industry and government that actually examines technical problems and solutions.

For example, smaller network operators, engineers and other technical professionals in the Internet industry meet regularly at a technical conference run by network operator groups (NOGs) to discuss different issues and strategies to help the sector, often related to the security of the Internet. This also exists in Australia with the AusNOG conference being held annually in Australia, however participation by law enforcement or government historically has been extremely limited, compared with the NZNOG conference which routinely has New Zealand law enforcement and regulator updates as part of the program.

Similarly, there are multiple initiatives already taken by industry to increase the level of trust in our networks, and thereby improve the security of the Internet including the Resource Public Key Infrastructure (RPKI) framework designed to secure internet routing, the Mutually Agreed Norms for Routing Security (MANRS) initiative and uptake of Internet Protocol version 6 (IPv6). The Asia Pacific Network Information Centre (**APNIC**) which is the regional Internet registry for the Asia-Pacific region also host training and forums to support the deployment of these mechanisms. Not only are these infrastructure initiatives that should be adopted by government itself to improve the security of government networks, but the government should also work with industry to support the wider deployment of these measures across Australia.

There are also other various forums and initiatives where issues of security are considered such as Internet governance forums, which again, also exist in Australia in the form of events such as NetThing. We therefore strongly recommend that government should maintain active presence and investment in these sorts of industry events and communities as they have a lot to offer in terms of practical network and Internet security, and therefore opportunities to enhance Australia's cyber security. This is to reiterate our position that there needs to be a serious improvement in genuine engagement and collaboration to develop and implement practical solutions to combat cyber security. This would also provide government with an opportunity to identify what sort of technical or other gaps that exist in industry, as well as identify gaps that exist in government.

Furthermore, information sharing is a two-way relationship and should be treated as such. There should be greater reporting from government to improve transparency and therefore trust between government, industry and the broader public. In particular, there should be greater information sharing as to the effectiveness of the compliance obligations that are in place or recently implemented.

For example, in light of the recent amendments to the SOCI Act which have significantly broadened the scope of sectors and assets captured under the critical infrastructure regime, we

believe it would be very beneficial if the government researched and reported on the outcomes that have been achieved through such expansion, and the improvements to Australia's security and resilience.

This would have multiple benefits. For one, it would achieve greater transparency and trust, and improving industry's understanding as to why these obligations are actually required and therefore encourage compliance. In addition, it would also give government an opportunity to consider what sort of legislative frameworks are genuinely effective, what outcomes government is seeking to achieve, and what sort of impact is actually being had as a result of its intervention. Indeed, we believe this would be useful for government in measuring its impact on uplifting national cyber resilience.

Considerations that government should have in assessing its impact include amongst others, the level of trust between government and industry as well as government and the general public, the maturity level of government departments and agencies according to the Essential Eight Maturity Model, the level of maturity of specific industry sectors, number and type of cyber incidents, and responses to cyber incidents.

REGIONAL AND INTERNATIONAL FOCUS

Questions 3, 4 and 5

With respect to Australia and the Australian government's contribution to improving cyber security resilience in the region and internationally, again, we emphasise the need for greater engagement and collaboration. We believe government should adopt approaches which promote community development, are human-centred and collaborative, as opposed to heavy-handed intervention.

There is a serious gap in both the technical knowledge and experience, and also arguably in the strength of political processes that create sound legislation when comparing Australia and other governments in the region, particularly in the Pacific. Moreover, the governments in many of these countries often don't have the technical or the human resources to assist industry. As such, there is a need to develop a strong trust relationship between government and industry.

Thus, in terms of opportunities and work required of Australia and the Australian government, prioritisation of working with not only the governments of neighbouring countries, but also the industry within these regions is crucial in order to ensure a holistic and effective improvement to cyber security and resilience in the region.

Again, these sorts of regional and international initiatives and relationships already exist in the Internet community. Due to the nature of the Internet, which is inherently open and public, maintaining this global outlook is a core principle in Internet governance and policy, reflected in the protocols developed to improve the security of the Internet.

We strongly encourage the Australian government to work with the Internet industry in Australia and regionally to build the technical capabilities within regional governments and their industries to help create step change in development of their cyber security and resilience.

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the 2023-2030 Australian Cyber Security Strategy. We recognise the importance of this work to ensuring the safety and resilience

of Australia's economy and society. We are therefore sincerely committed to working with the Australian government, industry and other stakeholders to develop and implement an effective Strategy. We sincerely urge the government to prioritise proactive, genuine and meaningful engagement with industry and other stakeholders, and focus on collaboration to achieve this.

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