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

01 March 2024

Department of Home Affairs

PO Box 25
Belconnen ACT 2616

By submission: https://www.homeaffairs.gov.au/help-and-support/departmental-forms/online-forms/cyber-security-legislative-reforms-form

RE: 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms – Consultation Paper

The Internet Association of Australia (**IAA**) thanks the Department of Home Affairs for the opportunity to respond to the consultation on the 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms – Consultation Paper (**Consultation 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**). Our response to the Consultation Paper is primarily in representation of these members, as well as for the general public good of the Internet, and broader telecommunications industry.

IAA has been actively engaged in the development of cyber security related policies, including legislation related to the security of critical infrastructure, as well as the 2023-2030 Australian Cyber Security Strategy – Discussion Paper (**Discussion Paper**). To that end, we continue to be interested and committed to the development of a sound and fit for purpose cyber security legislative regime.

Overall, we appreciate the efforts of the government in creating a comprehensive and medium to long term strategy that will ensure the safety of the Australian economy and public in the age of increased and ever increasing cyber threats. We understand the need for such concerted focus and legislative reform, and in general, acknowledge the intent behind majority of the proposed measures is for this purpose of ensuring the security, safety and resilience of Australia. However, we are concerned that in some instances, the measures may go beyond their legislative intent, and would result in outcomes potentially adverse for not only industry, but also individuals and the government. In particular, we are concerned that many of the proposals will result in greater amounts of data being made public or accessible, that may itself result in further susceptibility to unauthorised access. We therefore offer our submission to raise our concerns with respect to such proposed measures.

Furthermore, we reiterate our overall concerns that were raised in our response to the Discussion Paper about the disproportionate regulatory burden that would be experienced by smaller entities. To that end, although we support proposals to introduce thresholds to ensure certain onerous obligations are only applied to larger entities, we believe this to be a nuanced issue where it is equally important smaller entities do not get left behind, and themselves become targets for malicious activity. As such, we recommend that there is concerted effort placed into engaging the smaller entities across each sector to encourage voluntary compliance, and an overall uplift in their security posture and understanding of the regulatory processes. Similarly, we reiterate our recommendation made in our response to the Discussion Paper for government to support the widespread adoption of other mechanisms that will overall boost the security posture of entities and government bodies such as MANRS, RPKI and uptake of IPv6.

In addition, in general, we advocate for the government to continue its educative and consultative approach following any implementation of proposed measures, especially in relation to small businesses. We recommend allowing for a generous grace period for all legislative reform before penalties apply, during which period, government should actively work with industry to uplift entities' understanding of their obligations. Furthermore, in cases of non-compliance that does not appear to be cases of egregious or wilful non-compliance, to work with industry to assist with their compliance efforts rather than to take a punitive approach.

PART 1: NEW CYBER SECURITY LEGISLATION

MEASURE 2: RANSOMWARE REPORTING

9. ***What additional mandatory information should be reported if a payment is made?***

In relation to the reporting obligation, following an entity's payment of a ransom, relevant information that we believe would be useful include:

- the outcome and/or consequences following the entity's payment of the ransom;
- method and amount of payment, if different from the requested method and amount of payment previously reported prior to the entity's payment of the ransom;
- nature and timing of communications between the entity and ransomware actor regarding ransomware payment; and
- timing between payment of ransom, and following outcomes and/or consequences – for example, how long after making payment did the entity gain access to its systems/data etc.

10. ***Which entities should be subject to the mandatory ransomware reporting obligation?***
11. ***Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?***

In general, we support exempting small businesses from the reporting obligations, given the limited resources and capacity for small businesses to engage. However, we recommend that government works extensively with small businesses, particularly in high-risk industries to encourage such entities to engage with the reporting obligations on a voluntary basis, as increased information sharing and reporting is very important to uplift the security of

Australia more broadly. Furthermore, we are concerned that isolating small businesses entirely could result in an unintended adverse result where small businesses become honey pots for malicious actors to target, aware of small businesses' lack of engagement with an anti-ransomware reporting framework that may mean that such malicious actors are also less likely to be caught.

In addition, when setting a threshold for 'small business', we recommend that keeping it consistent with other definitions of small businesses for the purposes of other legislation such as the *Privacy Act 1988* (**Privacy Act**), or in relation to the *Australian Consumer Law* may be helpful for entities so that entities do not have to remember different thresholds and requirements under various legislative regimes.

12. ***What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?***

In general, we are strong supporters of only subjecting entities to regulatory burden to the extent it is reasonably necessary and there are genuine benefits from doing so. As such, the time periods with which an entity must comply with should be reasonable and practicable, in consideration of the high stress an entity will be experiencing even without needing to meet reporting obligations. However, we also understand that there may be genuine benefits of requiring entities to report as soon as possible, such as where government may be able to offer assistance, or where that information can be disseminated and used to alert other entities to help prevent other attacks in the industry, or wider Australian economy.

When balancing these principles to set the timeframe for reporting, it is paramount that the government is genuine in its consideration of how the government will actually use the information, and whether it has the capacity to meaningfully make use of any reporting immediately or promptly to require entities to report within short time periods. We know that under the critical infrastructure regime, both the mandatory cyber security incident notification and asset register obligations require prompt reporting. However, there has been a lack of evidence or output from the government to indicate that making notifications within short periods following the occurrence of a relevant event (such as a change to an entity's asset), has been promptly processed and meaningfully used, or analysed by the government to justify imposing such regulatory burden on industry. We believe that in the long term, this approach is detrimental to the industry-government relationship as compliance with obligations become more of a tick-box exercise, rather than meaningful engagement if industry does not feel their compliance with obligations is having a genuine impact.

This is particularly relevant in relation to setting a time period to make a second report following the payment of a ransom. We assume that most of the information that would be required under this obligation would be to help the government study the impact, or effectiveness (or rather, ineffectiveness) of making ransom payments to conduct further analysis and research into developing an appropriate policy and approach to ransomware attacks, rather than using such information to take any immediate action. In the event our assumption is correct, we consider it is not necessary for entities to be providing this sort of information as promptly as its first notification about the occurrence of an attack. For

example, if the government intends or anticipates that it would be producing quarterly reports (as stated in the Consultation Paper) on ransomware incidents in Australia, then the time period within which information must be reported to government should correspond with the periodic government's reports, rather than imposing an unnecessarily short period for entities to report.

Furthermore, another relevant consideration for setting time periods is its harmonisation with other reporting obligations. As also noted in the Consultation Paper, major and common feedback was about the duplicative reporting obligations under various regimes. It was previously noted in the Discussion Paper that stakeholders have encouraged government to streamline reporting obligations, for example via one reporting clearinghouse. It is unclear to what extent this is still a consideration for government, and if it is, what this means for time frames to report as it would need to be consistent with other reporting obligations, especially if a cyber incident triggers various reporting obligations under different frameworks.

IAA still strongly supports such calls for a streamlined regulatory approach to reporting obligations, such as via one clearing house body or portal to process incident reporting that can be shared with relevant agencies and/or departments, provided there are stringent rules, appropriate safeguards and restrictions to ensure the security of the data and protect against oversharing between agencies and departments. We believe this could also be a way to encourage greater voluntary reporting for entities that are not subject to obligations as it would be a simpler approach. We refer you to our submission to the Discussion Paper for further details.

13. ***To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident to Government?***
14. ***How can the Government ensure that the no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?***
15. ***What is an appropriate enforcement mechanism for a ransomware reporting obligation?***

IAA supports the proposed no-fault and no-liability principles and consider this could positively affect meaningful compliance by industry to increase genuine and detailed reporting of ransomware attacks. To that end, we primarily support an educative and collaborative approach to encourage compliance. At the least, we would recommend a safe harbour approach where enforcement mechanisms only apply in respect of entities that egregiously fail to take cyber security considerations into account in relation to their operation of their business. In addition, similar to the Consultation Paper's proposal of introducing a limited use purpose for other reporting or information sharing obligations, information shared under a mandatory ransomware incident reporting obligation could also be protected under a limited use principle.

MEASURE 3: LIMITED USE OBLIGATION

18. ***What restrictions, if any, should apply to the sharing of cyber incident information?***

In principle, we understand the need to allow for information sharing between the ASD and other government and/or regulatory bodies and agencies. However, from a practical perspective, we are concerned that such sharing with other agencies may still result in regulatory bodies making use of the information shared with the ASD to take enforcement action, in spite of the 'limited use' rule. In particular, we are concerned that despite the limited use rule, regulatory bodies may be able to circumvent such principles by conducting their own 'independent' research or investigations to take enforcement actions against entities after being, in effect, tipped off (even if unintentionally) by the ASD. In such cases, this is also likely to have a further unintended litigious consequence as entities and regulatory bodies enter disputes about how such bodies found out information, without relying on the information shared under the limited use obligation, which would not be in the best interest of any stakeholder.

Furthermore, we also note that the information sharing between ASD and other bodies would itself give rise to concerns about data security as increased data sharing poses greater risk of such data being subjected to unauthorised access and use by malicious actors.

19. ***What else can government do to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?***

We reiterate our recommendation for an alternative approach to enforcement. Penalties should only be applied where entities have contumeliously ignored their obligation, or only in cases of gross and/or wilful negligence, alongside safe harbour provisions.

MEASURE 4: CYBER INCIDENT REVIEW BOARD

20. ***What should be the purpose and scope of the proposed CIRB?***

In general, we question the need for the establishment of a new and separate review board such as the CIRB. While in principle, we understand and agree with the distinct purpose of a body such as the CIRB that would be independent from other existing bodies, we also consider it may still be possible to achieve the government's intentions regarding the CIRB by making use of existing processes and bodies. For example, reiterating our above-mentioned support for a streamlined reporting obligation mechanism, the responsible body processing and handling such reports may have a designated branch whose function is to conduct post incident review and analysis.

Otherwise, under the proposed measure, we are concerned this would introduce yet another body that entities would have to deal with. Furthermore, we consider setting up a new body would require greater resources and result in more delay. Indeed, there is an extensive list of questions under this measure 4,[1] reflecting what a big endeavour it would be to set up yet another body. We therefore consider it to be an inefficient approach compared to setting up a new division within a new body such as within the ASD, with clear terms of reference to ensure its sufficient independence.

[1] For emphasis, there are 14 questions in relation to this proposal, which is greater than under any other measure.

PART 2: AMENDMENTS TO THE SOCI ACT

MEASURE 5: DATA STORAGE SYSTEMS AND BUSINESS CRITICAL DATA

36. ***What would be the financial and non-financial impacts of the proposed amendments? To what extent would the proposed obligations impact the ability to effectively use data for business purposes?***

While the proposed measure is likely to result in greater regulatory burden for industry, in principle, we agree that reform is required to sufficiently protect 'business critical data'. However, we are concerned that making broader changes to definitions of certain terms, such as to the term 'asset' to include business critical data, may have far-reaching consequences on other obligations under the SOCI Act, for example, the asset register obligation. Therefore, we respectfully request that government undertake a thorough review and sense-check the workability of the reform prior to making any changes.

MEASURE 6: CONSEQUENCE MANAGEMENT POWERS

Again, in principle, we understand the intent behind this proposed measure. However, we are of the firm belief that there must be further consideration of the specific directions that may be made, especially as it relates to individual rights to privacy, such as the proposed power to authorise disclosure of protected information between the affected entity and third parties, or between third parties (whether government or industry). Furthermore, we reiterate our concerns that proliferation of information sharing between entities gives rise to further risk of such data being made further vulnerable.

As part of the safeguards and oversight mechanisms, prior to making a direction, the Minister must also undertake an impact analysis to satisfy him/herself that the benefits of making the direction outweighs the adverse impacts associated with or that may result from such a direction.

MEASURE 7: PROTECTED INFORMATION

We agree in principle that the proposed measure may be required to ensure entities and agencies are able to share information to relevant third parties in order to be able to practicably prompt actions that will mitigate the risk of harm following cyber security incidents. However, there needs to be further consideration about how again, the increased data sharing may result in further risk to data being misappropriated.

MEASURE 8: ENFORCING RISK MANAGEMENT OBLIGATIONS

42. ***How would the proposed review and remedy power impact your approach to preventative risk?***

It is likely that this proposed measure will prompt entities to be more proactive in their compliance with CIRMP obligations. While in general, this is positive, we believe that there needs to be greater oversight and safeguards that are provided during the drafting stage. For example, the provision should allow for the relevant entity to respond to the Minister's notice to justify its decision to not take certain actions, which the Minister must consider in its decision to make or

not make a direction. There also needs to be a proportionate penalty and enforcement regime such as where an entity fails to comply with a direction given under the review and remedy power. Again, we support a safe harbour approach, or for penalties to apply only in egregious cases, or causes of wilful non-compliance.

MEASURE 9: TELECOMMUNICATIONS SECTOR

45. What are the main barriers to engaging with government through the notification process as it is currently enforced? How can the obligation to notify be clarified?

47. How can outlining material risks help you adopt a more uniform approach to the notification obligation?

In its current form, the notification obligation is too broad and there is a lack of clarity on what information is actually required, as well as why such required information is so required. Similar to our above feedback on the lack of output from the government regarding the asset register, there is a lack of evidence to suggest that the notification obligation has been helpful in ensuring greater protections and resilience of telecommunications infrastructure, as evidenced by large scale breaches and network failures in recent years.

However, we are unconvinced at this stage that switching on the TSRMP rules will result in a clearer or better process as the two obligations are duplicative in nature, and likely to result in increased regulatory burden.

We look forward to continue working with government and relevant stakeholders to ensure the consolidation of security requirements in respect of the telecommunications industry with the SOCI Act results in a fit for purpose framework.

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper. As our threat environment continues to evolve, we are committed to working with government and relevant stakeholders to ensure the development of a comprehensive and effective framework to boost Australia's cyber security. To that end, we sincerely look forward to continue engaging with all stakeholders for that purpose in future consultation processes.

Yours faithfully,

Narelle Clark
Chief Executive Officer
Internet Association of Australia

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.