To: Australian Cyber Strategy Team
Department of Home Affairs
By email: auscyberstrategy@homeaffairs.gov.au

Friday March 1, 2024

Dear Australian Cyber Strategy Team,

The Digital Industry Group Inc. (DIGI) thanks you for the opportunity to provide our views on the *2023–2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper* (The Consultation Paper).

By way of background, DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia. DIGI's founding members are Apple, Discord, eBay, Google, Linktree, Meta, Microsoft, Snap, Spotify, TikTok, Twitch, X (f.k.a Twitter) and Yahoo. DIGI's vision is a thriving Australian digitally-enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected.

DIGI shares the Government's strong commitment to cyber security, and our members invest heavily in cyber and data security and the privacy of their users, through technical controls, user controls and strong accountability-based practices and policies. DIGI recognises the role that large-scale data breaches in the telecommunications and insurance sectors in recent years have played in underscoring the critical importance of data privacy and cyber security economy-wide, and the serious impact that any such event can have on Austalians. To that end, we applaud the Government's goal of improving cyber security incident response and communication channels between industry and Government as outlined in the 2023 - 2030 cyber strategy and its focus on delivering a strong cyber security response for Australian businesses and consumers.

In our submission below, DIGI has responded to several of the discussion questions that are most relevant to our members with a focus on regulation that drives better cyber security outcomes but avoids creating undue regulatory burden where it would not result in better protections for consumers. We also encourage consideration of our previous submissions in relation to wider initiatives that mitigate against cyber security threats, including non-regulatory and cyber security consumer awareness and targeted industry initiatives.

We thank you for your consideration of the matters raised in this submission. We look forward to future opportunities to continue our engagement, including on initiatives such as an app store code of practice, voluntary labelling scheme for IoT devices, and co-design of an incident response code of practice. Should you have any questions, please do not hesitate to contact my colleague Tahlia Davies via [redacted].

Best regards,

[redacted]

Sunita Bose
Managing Director, DIGI
[redacted]

Table of contents

Co-designing mandatory cyber security standards for IoT and smart devices

Discussion questions:

- Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?
- What alternative standards, if any, should the Government consider?
- Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard?
    - Should this be the same as the definition in the PTSI Act in the UK?
- What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?

Adopting a mandatory standard and the importance of global interoperability

DIGI welcomes and supports the Government's goal under Initiative 8 of the 2023 - 2030 cyber security strategy to 'adopt international security standards for consumer-grade smart devices'.[1] We also support

[1] 2023 - 2030 cyber strategy, p.30

the intention to closely collaborate with industry on its approach, which we have previously stated is essential to driving cyber security outcomes for business and consumers in Australia.

Given the complexity of cyber security and the wide range of technology applications, DIGI has previously supported the Government's approach in relation to setting voluntary standards through the *Code of Practice: Securing the Internet of Things for Consumers* (the Code of Practice), which sets out guidance for IoT manufacturers aligned to the international ETSI EN 303 645 standard.

Noting the Government's intention to progress to mandatory standards, DIGI supports the adoption of the ETSI EN 303 645 standard, as the world's first globally-applicable standard for the cyber security of consumer Internet of Things (IoT) devices. DIGI has previously emphasised and maintains our position on the importance of interoperability in Australia's approach to cyber security, especially the globalised nature of the manufacture and distribution of relevant products and services. We note The Consultation Paper's statement that it is critical that 'Australia remains in step with the international market to minimise regulatory burden for vendors'[2] while ensuring consumers in Australia have strong cyber security protections. Interoperability is essential to achieving this goal.

DIGI supports the first three principles of the ETSI EN 303 645 standard, namely to:

- Ensure that smart devices do not have universal default passwords;
- implement a means to receive reports of cyber vulnerabilities in smart devices; and
- provide information on minimum security update periods for software in smart devices.

In saying this, we also note that, in some cases, one company will be responsible for producing both the hardware and software; whereas, for other devices, there may be a multitude of companies playing a role – for example where one company develops a device, while another develops the operating system. If a standard is directed toward one actor in the ecosystem, there will be confusion as to how that standard is applied to a range of products that have varied supply chains. There could also be confusion about who is responsible for communicating the standard to consumers in relation to updates and other communication after the point of sale. We encourage the Department to carefully consider these challenges in development of a mandatory standard.

DIGI has previously supported the voluntary Code of Practice be in place for a longer period of time before assessing its full efficacy but, recognises that The Consultation Paper states its uptake has not met the Government's expectation. We also note that The Consultation Paper states 'although major IoT manufacturers generally demonstrated a strong commitment to cyber security' there was evidence suggesting that 'low-cost manufacturers were least likely to make more security-conscious design choices'.[3] DIGI supports the Government's intention to drive consistency across the market through a mandatory standard but considers that these goals should also be reached through targeting sector support, outreach and awareness raising initiatives to businesses who are contributing to the greatest cyber security risks. These types of activities will be essential to encourage compliance, noting that major manufacturers have already maintained a high level of commitment to cyber security in the context of a voluntary code.

[2] 2023–2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper, p.8
[3] Ibid.

Definitions

DIGI does not object to the application of the first three principles of the ETSI EN 303 645 standard to a broad definition of smart devices as outlined in The Consultation Paper; however, we also note that it would be inappropriate to include smartphones or general computing devices in the definition as security standards for these devices are already covered under other legislation.

It is also essential that any mandatory standard makes clear how it applies to different operators in the supply chain as defined under the standard. We further emphasise our point outlined above that it is critical any standard is properly scoped to ensure clarity in application and communication with consumers.

Implementation timeframe

In principle, DIGI supports a12-month timeframe to adjust to new security requirements for IoT devices, following appropriate consultation with industry during the development of a draft mandatory standard. We caveat that this support is dependent on the requirements set out under a mandatory standard. As previously stated, major manufacturers already maintain a high level of commitment to cyber security practices and these are already built into manufacturing processes; however, any obligations that would require additional engineering investment for industry might require a longer lead time to implement. In the case of a mandatory standard that is in line with international best practice and does not present overly burdensome challenges in the context of global manufacturing supply chains, DIGI supports a 12-month implementation timeframe.

The role of a voluntary labelling scheme

We understand that a voluntary, industry-led labelling scheme for consumer-grade smart devices is not in the scope of The Consultation Paper, but that such a scheme would be interoperable with the proposed standard. To that end, DIGI emphasises its previous positions on the principles that should underpin any approach to labelling (and is relevant to the approach of a mandatory standard). Any cyber security framework should ensure that singular approaches do not foster a false sense of security. Responses must remain flexible to respond to new challenges as they emerge and secure-by-design principles must complement, not replace, cyber security best practices and behaviours for all, including consumers.

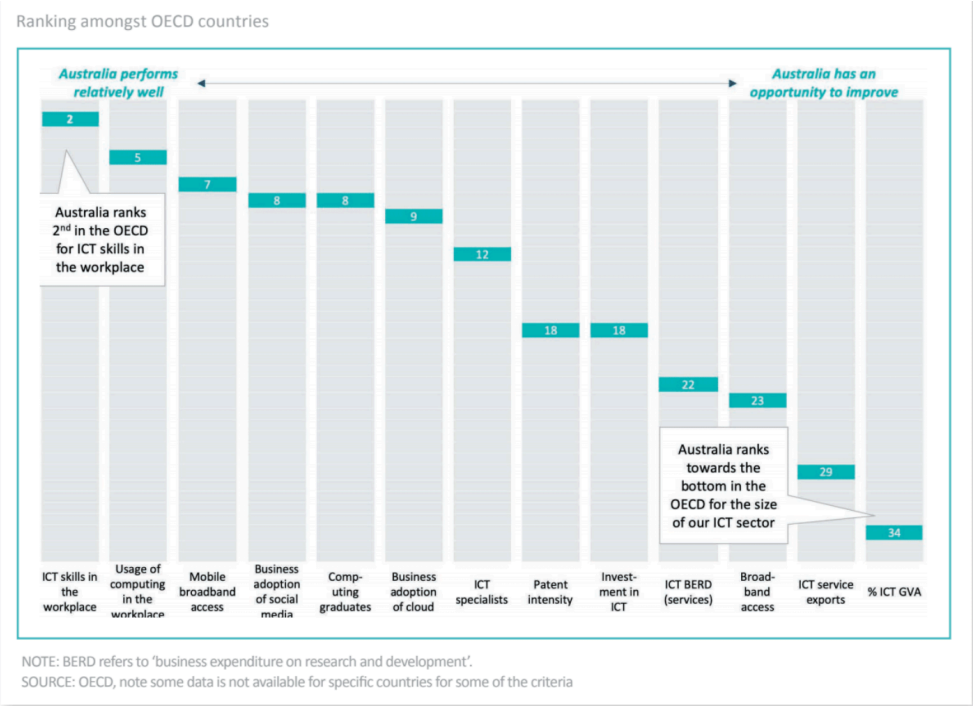
As we have previously noted, in a position paper titled *Cyber Security Labelling: A Guide for Policymakers,* ITI advances several points that we believe are pertinent to the discussion of labelling for smart devices in Australia.[4] In this paper, ITI states: '*Manufacturers can build the strongest capabilities into a device or service, but the likelihood that device or service is compromised by a cyber-attacks increases if end-users or operators do not undertake appropriate precautions*'. This sentiment is consistent with the experiences of DIGI members, and we agree with ITI's view that 'labelling should not convey a false sense of security'.

In this paper, ITI cautions that cyber security labelling is not a comprehensive or one-size-fits-all solution. They argue that, if not consulted upon properly, labelling schemes can cause barriers to trade in a global marketplace. In this context, it is worth remembering that Australia is a major importer of technology, and

[4] ITI, (April 2021), cyber security Labelling: A Guide for Policymakers

that we are toward the bottom of the OECD in relation to ICT exports, per 2019 research included in Figure 1 below.[5] We support The Consultation Paper's intention to align Australia with international standards, rather than adopt an Australia specific response that would present potential risks to trade and present a significant burden to manufacturers without clear evidence that it would result in stronger cyber security outcomes for consumers.

Figure 1



While labelling is not specifically in the scope of this discussion paper, we suggest these same principles are essential in considering the development of a mandatory standard. As previously noted, we must strive for interoperability with our cyber security consumer protections, otherwise we risk creating barriers to trade. We need to pull levers that maximise the business opportunities in creating and expanding technology companies in Australia, minimise their risk, and optimise global interoperability of regulatory settings. These three areas bear heavy on the minds of business leaders of small and large technology companies alike.

Improving cyber incident response

Discussion questions:

- What should be the purpose and scope of the proposed Cyber Incident Review Board (CIRB)?

[5] AlphaBeta (September 2019), *Australia's Digital Opportunity*

There is a shared responsibility to address cyber security risks across governments, industry, and the broader community. It is in the interest of companies to take action to ensure strong cyber security and DIGI members invest heavily in the cyber security of their services. We have previously expressed our support for improving communication between industry and government in cyber incident response and there is a continued willingness among industry to build capability and best practice economy-wide.

DIGI has long supported improving the communication channels between industry and Government after cyber security incidents and, to this end, DIGI welcomed the elevation of the cyber security portfolio to have an assigned Minister and the announcement of a coordinator for Cyber Security, supported by a National Office for Cyber Security within the Department of Home Affairs, and we see this as a logical office to lead its coordination, and we encourage its resourcing accordingly. Clarity regarding who is responsible for cyber security and coordination across other relevant government departments and stakeholders will improve incident response and evaluation.

While we support the intention of the Cyber Incident Review Board, DIGI cautions against the introduction of a parallel review process that introduces a new layer of complexity to the regulatory regime and falls outside the responsibilities of the Minister for cyber security and coordinator for Cyber Security, supported by a National Office for Cyber Security. Logistically, a Cyber Incident Review Board will require significant resourcing to both establish and maintain and it could prove difficult to determine the appropriate composition and output of its review.

DIGI supports the establishment of an incident review process that is led and managed by the National Coordinator and Office for Cyber Security, with appropriate input from independent experts. Noting the goal of the proposed incident review process as, 'to issue public recommendations that help uplift cyber security across Australia'[6] We also encourage further research into the most effective way of communicating lessons obtained from a review that would result in a measurable uplift in cyber security awareness and practices in Australian communities.

Ensuring clarity between cyber security and privacy regimes

In DIGI's submission to the *2023-2030 Australian Cyber Security Strategy Discussion Paper*, we supported a thorough gap analysis to inform the best approach to improve incident response[7]and we welcome the Government's approach in considering these gaps as outlined in The Consultation Paper, including in proactively addressing the appropriate division of responsibility across Government related to cyber security. In line with DIGI's support for overall clarity in the regulatory regime related to cyber security, we support and encourage the Department of Home Affairs' engagement with the Attorney-General's department, as outlined in The Consultation Paper.

There are notable areas of overlap between government responses to cyber security and privacy, such as in the regulation of data storage practices that, without clear consideration and guidance, could prove complex for industry to navigate and pose barriers to compliance. We equally recognise that there is an opportunity for increased mandatory cyber security and related obligations in the current reform of the Privacy Act that could result in a more coordinated approach and stronger cyber security outcomes. We note, for example, that the Government's response to the *Privacy Act Review Report* agreed in-principle

[6] 2023–2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper, p.26

[7] DIGI submission to *2023-2030 Australian Cyber Security Strategy Discussion Paper*, Accessed at: https://www.homeaffairs.gov.au/reports-and-pubs/PDFs/2023-2030-aus-cyber-security-strategy-discussion-paper/DIGI-submission.PDF

that entities should be required to comply with a set of baseline privacy outcomes, aligned with relevant outcomes of the Government's 2023–2030 Australian Cyber Security Strategy (proposal 21.2). DIGI has welcomed the inclusion of cyber security measures within the APPs, and considers this an effective approach to ensuring compliance across the wide range of entities subject to the APPs. For example, DIGI has long advocated for the importance of data minimisation, as the more information that is required to be collected and retained by companies can increase the severity of a potential breach. Data minimisation requires goods or service providers to not seek to collect data beyond what is reasonably needed to provide the good or service, or to employ adequate measures to anonymise data. We believe that privacy risks – such as inappropriate use or disclosure or poor security – can be reduced by resolving the tension between data retention requirements and data minimisation best practices. DIGI welcomes the fact that the universally accepted privacy best practice of data minimisation forms part of the existing APPs under the Privacy Act 1988 (Cth). This principle equally serves privacy and cyber security outcomes.

To ensure that cyber security and privacy regimes are cohesive, we support the approach outlined in The Consultation Paper, including in ensuring amendments to the SOCI Act are complementary to existing and proposed obligations under the Privacy Act, the provision of appropriate guidance material to assist industry in understanding the relevant set of obligations and regulating authority related to different practices, and the intent to manage the burden on industry of overlapping consultation processes by coordinating consultation on reforms to the SOCI Act and the Privacy Act. This will help achieve a response with clear obligations for industry that focus on cyber security outcomes without creating unnecessary regulatory burden or reporting procedures that are complex to navigate and that have the potential to conflict.

Conclusion and opportunities for future engagement

DIGI appreciates the opportunity to contribute our views on The Consultation Paper. We look forward to future opportunities to continue our engagement, including on initiatives such as an app store code of practice, voluntary labelling scheme for IoT devices, and co-design of an incident response code of practice. DIGI has extensive experience developing and implementing industry codes, including the mandatory codes enforced under the Online Safety Act, and *The Australian Code of Practice on Disinformation and Misinformation* (ACPDM) and our team is well placed to offer insights based on this experience to help shape an effective code development process. We thank you for the opportunity to contribute to this important area of policy reform.