Mr. Luke Muffett
a/Assistant Secretary Cyber Policy & Strategy
Digital Economy Resilience and Market Reform Team
Technology Policy Branch
Cyber, Digital and Technology Policy Division
Department of Home Affairs
By email: techpolicy@homeaffairs.gov.au

Friday September 3, 2021

Dear Mr. Muffet,

Thank you for the extended opportunity to provide views about how we strengthen Australia's cyber security regulations and incentives, in response to the Department of Home Affairs' discussion paper *Strengthening Australia's cyber security regulations and incentives* .

By way of background, the Digital Industry Group Inc. (DIGI) is a non-profit industry association that advocates for the interests of the digital industry in Australia. DIGI's members are Apple, eBay, Facebook, Google, Twitter, Yahoo, Redbubble, Linktree, Change.org and Gofundme. 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.

We recognise the importance of the issues raised in the discussion paper. In response to several of the discussion questions posed, this submission offers considerations for the Government in informing its areas for further analysis and investment.

DIGI's members invest heavily in cyber security. We encourage the Government to undertake further analysis of the particular sectors that are contributing to the greatest cyber security risk, and to target efforts related to this initiative to those areas. We recommend the Government fully explore the possibility of voluntary initiatives, such as the *Securing the Internet of Things for Consumers (Code of Practice)* the Government introduced in September 2020, before considering regulation. We also emphasise the importance of a whole-of-Government approach to cyber security across public service agencies and law reform processes to ensure that efforts in this important area are not inadvertently undermined.

DIGI looks forward to further engaging with the Department of Home Affairs' consultation process in relation to this particular initiative, and the broader Cyber Security Strategy. Should you have any questions about the representations made in this submission, please do not hesitate to contact me.

Best regards,

Sunita Bose
Managing Director
Digital Industry Group Inc. (DIGI)

1. Government action on cyber security

a. Addressing the cyber security skills gap

Discussion questions:
- *What are the factors preventing the adoption of cyber security best practice in Australia?*
- *What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights of consumers?*

Cyber security is an economy-wide issue in a digitally-enabled economy. It is both relevant to technology companies and to companies across all sectors that avail of technology. It is also of crucial importance to all government departments in light of the increasingly digital nature of service delivery. Additionally, mitigating cyber risks is also reliant on informed consumer behaviour at an individual level. Therefore, there is a strong need to promote cyber security as a shared responsibility across Government, industry and individuals, and clearly defining the role that each must play. A collaborative approach between governments, companies and individuals will be the most effective way to improve cyber security at a macro and macro level.

In posing the question about the factors preventing the adoption of cyber security best practice in Australia, the discussion paper does not present a global comparative picture for Australia's relative standing in relation to cyber security best practice. In the absence of such analysis, there is not a shared understanding of the premise of the question, and therefore it is hard to provide a rounded answer to this question about the factors that may be hindering best practice.

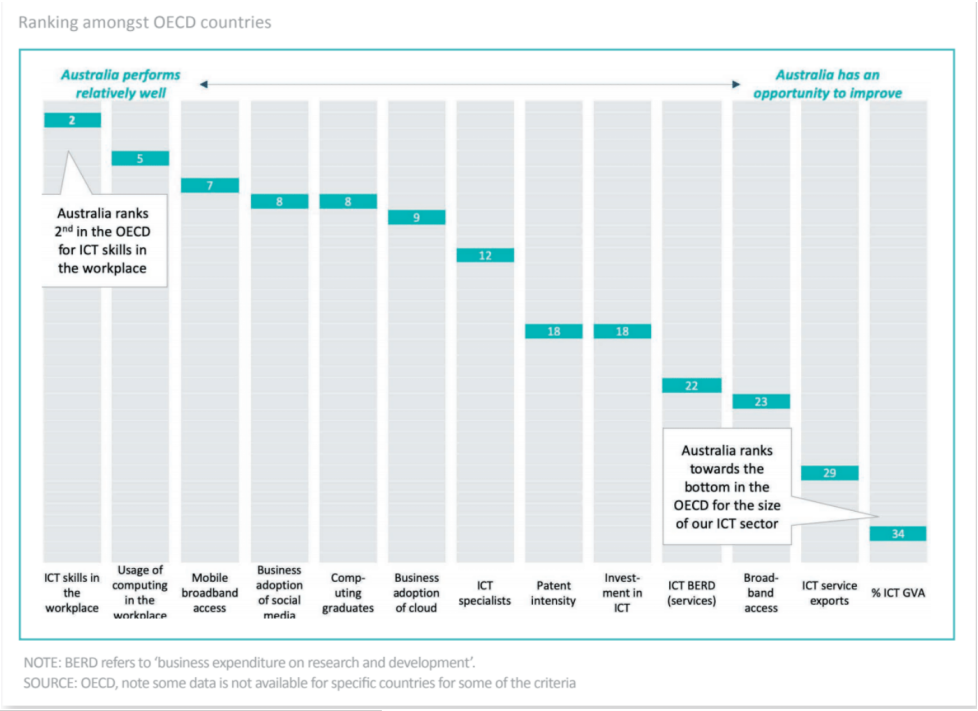
Having said that, one of the areas where we do have a comparative picture in relation to Australia's cyber security, is in relation to skills. DIGI commissioned a report in 2019, conducted by the economics firm AlphaBeta, titled *Australia's Digital Opportunity*, that examined the state of Australia's technology sector in comparison to other OECD countries. As Figure 1 overleaf shows, Australia ranks 12th in the OECD for ICT specialists. Among many other findings in the report, it included analysis of factors that impact the attraction of a talented technology workforce in Australia. The report found that:

The tech sector requires occupational skill sets that may not have existed even five years ago in areas such as data analytics, product development and management, artificial intelligence, machine learning, cybersecurity and robotic process automation. With a relatively limited domestic technology workforce and restrictions on skilled migration, difficulties in finding talented technology workers is leading to many firms restricting their operations in Australia.

Drawing on research from Deloitte Access Economics, the report also concludes that Australia's technology workforce in a number of areas including cyber security needs to grow at least twice as quickly in order for Australia to be globally competitive in this area. It identifies relevant barriers to talent acquisition in these areas, noting "bringing in experienced overseas talent is often necessary to help mentor and grow local talent. Australia's visa system makes this difficult. For example, the Temporary Skills Shortage visa defines occupations using ANZSCO codes, which do not include many new technology sector occupations. In this context, we welcome the Department of Home Affairs addition of ICT Security Specialist (ANZSCO code 262112) to the Priority Migration Skilled Occupation List (PMSOL) in June[1].

In addition, we welcome the Australian Government's announcement as part of its Digital Economy Strategy that it will commit $43.8 million for the Expansion of Cyber Security Skills Partnership Innovation Fund to fund additional innovative projects to quickly improve the quality and quantity of cyber security professionals in Australia[2]. If our goal is to see cyber security best practice in Australia, and given the economy-wide need for cyber security across almost all sectors, building capability in a wide range of sectors is crucially important in order to ensure widespread best practice.

Figure 1



[1]Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs Alex Hawke MP, "Supporting Australia's COVID recovery through Skilled Migration"(22/6/21), accessed at https://minister.homeaffairs.gov.au/AlexHawke/Pages/supporting-australia-covid-recovery-through-skilled-migration.aspx

[2] Department of Prime Minister & Cabinet, "Digital Skills | Australia's Digital Economy", accessed at https://digitaleconomy.pmc.gov.au/fact-sheets/digital-skills

b. The rationale for Government action

Discussion questions:

- *Why should Government take action?*
- *Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?*

There is a responsibility to address cyber security risks which is shared across governments, industry, and the broader community. A cyber security incident can have ramifications beyond the individual or organisation specifically targeted by the adversary.

In brief, there are a broad range and scale of cyber security threats with an important role for governments. These range from micro threats that typically target individuals -- such as identity theft or phishing scams to macro threats -- to macro threats to critical infrastructure, such as hacking and attacks of public and private institutions that have large volumes of data. Such micro threats require a combination of consumer awareness and encouraging industry best practice, through initiatives by Government and industry and collaborations between them. Certain macro threats, such as those that are state-sponsored will require a range of Government-led mitigation and response efforts; however, we understand from the discussion paper that the focus of this particular initiative is "on the social and economic impacts of widespread but lower sophistication threats".

It is very much in the interests of companies to take action to ensure strong cyber security. DIGI members invest heavily in the cyber security of their services. There is willingness among industry to collaborate and there is greater opportunity to explore what voluntary actions industry can take to build capability and best practice economy-wide.

The discussion paper advances a market failure lens, and we would question whether this is a helpful framework to further understanding of cyber security. It puts forward the argument:

> *In other markets, buyers might inspect a product or look at reviews from other customers to determine a product's quality. This is difficult in cyber security because most buyers don't have the technical capability to determine the security of a product…. The market power of major platforms and software companies may discourage or prohibit buyers from assessing product security, if contractual terms are 'take it or leave it'*

It is important to emphasise that consumers are able to, and routinely, consider reviews from other customers to determine a digital product or service's product quality. We would argue that most buyers, when purchasing a wide range of products, do not have the technical or other capability to determine the longevity and safety of a product. Furthermore, the contractual terms of products in other markets are also typically "take it or leave it". If anything, the digital nature of many products and services enables continued communication with customers, to communicate security updates for example, in a way that is not always possible for products in other markets. Furthermore, many digital services are also offered on a free or subscription basis that enables consumers to change services should security concerns arise after purchase.

Additionally, it is extremely important to apply a cautious approach with transparency in relation to cyber security, as information provided with this intention will be misused by malicious actors in their efforts to identify and exploit vulnerabilities. As such, offering consumers certain information in relation to cyber security may actually have a counterproductive effect by handing the playbook to those who are working to undermine consumers' cyber security.

Ultimately, data breaches and other security incidents are not in the business interests of companies as they cause serious, sometimes irrevocable, financial and reputational damage; in general, it is in most companies' commercial interests to prevent these through their own routine and specialised risk assessment processes. That is to say, there are market forces that encourage good cyber security practice, and DIGI recommends that voluntary initiatives to build a more widespread understanding of best practice be fully explored before considering regulation. The Government also has a key role to play to ensure improved education and awareness about the various responsibilities of different players across the diverse cyber security ecosystem.

2. Australia's current cyber security regulatory framework

Discussion questions:

- *What are the strengths and limitations of Australia's current regulatory framework for cyber security?*
- *How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?*

a. Assigning a lead agency or Minister

It is not clear today where the responsibilities for Australians' cyber security lie across Government, as many departments consider elements of it to fall under their remit. For example, it is understood that today responsibilities related to cyber security fall across the Australian Cyber Security Centre in the Australian Signals Directorate, the Attorney General's Department, the Office of the Australian Information Commissioner (OAIC), the Australian Competition and Consumer Commission (ACCC), the eSafety Commissioner, the Department of Communications and the Department of Home Affairs.

In light of this, It therefore is not apparently clear to industry nor individuals which government department would be the lead or appropriate port of call for enquiries relating to cyber security. In addition, a related limitation is that there are many different legislative instruments administered by different Government agencies that regulate cyber security. This further increases the risk of confusion amongst businesses, and makes it hard to glean a holistic view of the regulatory environment for cybersecurity.

In order to assist in creating this clarity and to elevate the importance of cyber security within Government, we would welcome the reintroduction of a Cyber Security Minister. Such a Minister can develop expertise on these issues, act as an advocate within Government for cyber security, and assist in the coordination of efforts across different departments.

In addition, a Minister or a lead agency may also be able to assist in weighing the cyber security considerations in legislation designed to achieve other aims. In relation to national security, for example, there is broad consensus among industry and digital rights civil society organisations that the Assistance and Access legislation poses potential threats to cyber security, as strong encryption serves Australia's national interests by protecting governments, communities, and the economy from criminal, terrorist, and state-sponsored attacks. The Department of Home Affairs may have an opportunity to weigh this in the Comprehensive Review of the Legal Framework of the National Intelligence Community that it is currently undertaking. In relation to privacy, the OAIC has advocated for the importance of effective end-to-end encryption with video teleconferencing services, in

response to their increased usage since the onset of the pandemic[3]. There are also major cyber security implications for the Government's online safety reform program that could result in the weakening of encryption, as well as other issues, as detailed below in Section 2b. A Minister or lead agency can ensure coordination and consistency across Government in relation to cyber security, and support a whole-of-Government approach.

b. Consideration of online safety reform

We note that this Section 3 of the discussion paper explains Australia's current regulatory environment in relation to cyber security but excludes "laws in adjacent areas like online safety". We would strongly caution against online safety being considered an adjacent area, but rather as an area that has increasingly important implications for Australia's cyber security.

In June 2021, the Australian Government requested the eSafety Commissioner develop an implementation roadmap for a mandatory age verification regime relating to online pornography, for which public evidence is currently being sought[4]. Related to this initiative, the eSafety Commissioner is also seeking input on Restricted Access System to limit the exposure of children and young people under 18 to some age-inappropriate online material. The instrument is intended to apply to "Designated internet services", which we understand is defined to include *all websites in Australia*; there are no meaningful exemptions. Additionally, the scope encompasses "social media services" that "enable online social interaction between 2 or more end users", "relevant electronic services" which encompasses all text and online messaging. It is our initial assessment that these two initiatives encourage the widespread collection of age data, potentially even identity verification documentation such as drivers' licences. This runs counter to the universally accepted privacy best practice of data minimisation; data minimisation is also a key principle of the consumer data right[5].

In addition to these two initiatives, the Department of Communications also has an open consultation process on a draft instrument called the Basic Online Safety Expectations (the BOSE). The BOSE would apply to these same three categories of services as well as hosting providers that states: *"If the service uses encryption, the provider of the service will take reasonable steps to develop and implement processes to detect and address material or activity on the service that is or may be unlawful or harmful.[6]"* There are fundamental impracticalities and impossibilities in relation to services detecting and addressing encrypted material; if this becomes law, a result could be the weakening of encryption, which is crucially important to ensuring adequate levels of cyber security across a wide range of services.

---

[3] OAIC, (22/7/2020), "Global privacy expectations of video teleconference providers", accessed at https://www.oaic.gov.au/updates/news-and-media/global-privacy-expectations-of-video-teleconference-providers/

[4] Office of the eSafety Commissioner, (16/8/2021), "Age verification call for evidence", accessed at https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification-call-for-evidence?utm_medium=email&utm_campaign=AGE%20VERIFICATION_CALL%20FOR%20EVIDENCE_PRIVATE%20LIST_%20AUG%202021&utm_content=AGE%20VERIFICATION_CALL%20FOR%20EVIDENCE_PRIVATE%20LIST_%20AUG%202021+CID_86c38611d002bc02d2b95cc79b62d819&utm_source=Email%20marketing%20software&utm_term=Share%20your%20insights

[5] OAIC, (09/06/21), "Chapter 3: Privacy Safeguard 3 — Seeking to collect CDR data from CDR participants", accessed at https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-3-privacy-safeguard-3-seeking-to-collect-cdr-data-from-cdr-participants/

[6] Department of Infrastructure, Transport, Regional Development, & Communications, (8/8/21), "Draft Online Safety (Basic Online Safety Expectations) Determination 2021 consultation", accessed at https://www.communications.gov.au/have-your-say/draft-online-safety-basic-online-safety-expectations-determination-2021-consultation

While the outcome of these three Australian Government online safety processes is, at time of writing, not known, it is a reasonable assumption that these reform programs will likely require potential additional data collection on the part of these services in Australia including 1) age data, perhaps including drivers' licenses or other documentation in order to verify age 2) personally identifiable data about people who visit websites that include online pornography, as well as 3) encouraging the weakening of encryption, or discouraging its use. DIGI predicts that this potential increase in data collection for all websites, and the sensitive nature of the data being collected, will cause widespread cyber security risks to a whole range of websites in Australia, reminiscent of the 2015 Ashley Madison data breach in the United States. In July 2015, user data was stolen from the company Ashley Madison, a commercial dating website associated with extramarital affairs, and threatened to be released if the company did not shut down. The following month, more than 60 gigabytes of company data was leaked, including user data such as real names, home addresses, search history and credit card transaction records[7]. It is a reasonable prediction that similar widespread attacks, intended to publicly shame through personally identifiable data, may occur if these reforms progress as currently proposed.

This example is used to highlight the cyber security implications of these particular online safety reforms, and to emphasise the critical importance of a whole-of-Government approach to assess where reforms in different areas might undermine cyber security in Australia. Not evaluating the online safety reform program for how it might serve to weaken Australia's cyber security is an enormous oversight; if this is not addressed, it may see the work of one arm of Government undoing the work of another. This is not an effective use of public resources.

3. Considerations for reform proposals

Discussion questions:

- *Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?*
- *What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes?*

a. Focus on sector specific approaches & privacy reform

In an increasingly digitised economy, where almost all institutions across Government and the private sector use digital technologies with varying levels of customer data, regulation plays an important role in relation to customer protections and the security of digital products and services. There are many related reform processes already underway.

We understand from the discussion paper that this initiative's "*focus is on all the other businesses that are not covered under sector-specific legislation. This includes most technology platforms and online services, most professional services, mining, manufacturing, hospitality, retail, wholesale and construction*." In light of that intended scope, and in order to avoid duplication with the extensive requirements that critical infrastructure asset holders will be subject to under the revised Security of

[7] Doffman, Zac, (23/8/2019), "Ashley Madison Has Signed 30 Million Cheating Spouses. Again. Has Anything Changed?", accessed at https://www.forbes.com/sites/zakdoffman/2019/08/23/ashley-madison-is-back-with-30-million-cheating-spouses-signed-since-the-hack/?sh=5aac67123878

Critical Infrastructure Act 2018 (SOCI Act), we request that all critical infrastructure asset holders are exempt from any of the measures that flow from the proposals from this initiative.

For technology platforms and online services that remain, we suggest a focus on voluntary codes (as discussed in Section 3b) and the existing privacy laws that already apply to cyber security, and the Government is already considering changes via existing reform currently underway. Under the Australian Privacy Principles (APP), APP11 relates to the security of personal information. This requires an APP entity to "take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure."[8] In addition, the OAIC has published a "Guide to securing personal information" that it uses to investigate whether an entity has complied with its personal information security obligations.

The discussion paper notes that it is common for cyber security risks to be captured through privacy legislation internationally, such as the approach taken by the European Union's General Data Protection Regulation (GDPR). As Australia's Privacy Act is currently under review, we recommend a similar approach, as privacy and security can be seen as two sides of the same coin, and are conceptually challenging to separate. In addition to the economy wide Privacy Act review, we understand that an Exposure Draft of amendments to the Privacy Act penalties regime will soon be published alongside a direction to industry to commence working on an enforceable code to be overseen by the Privacy Commissioner, which applies to social media and other online platforms. We would caution against an approach that sees two distinct sets of codes, one focused on privacy and the other focused on security; such a delineation will be hard to implement and may see gaps in the coverage of the two codes, particularly as technology evolves.

Building on the points made earlier about the importance of a whole-of-Government approach, we would recommend a focus on these two privacy reform initiatives underway. To the extent that there are specific sectors that the Department wishes to focus on this initiative, then we encourage the exploration of sector-specific approaches including support to those companies, complemented with education and awareness raising initiatives. Such an approach will be far more targeted than the proposal to cover "large businesses" advanced in the discussion paper. It is worth further noting that The Privacy Act covers organisations with an annual turnover of more than $3 million and some other organisations, meaning that "large businesses" would be covered under the reformed Act, unless this threshold changes.

In addition to the codes expected to be introduced for certain online businesses under the Privacy Act, industry associations representing the online industry (including DIGI) and retailers of online services are in the process of developing online safety industry codes in relation to Class 1 and Class 2 content under the Online Safety Act to be registered in 2022. We need to be mindful of the cumulative compliance burden implications of three distinct sets of industry codes, in relation to privacy, safety and security separately, and how this might impact the Australian Government's Digital Economy Strategy being advanced by the Digital Technology Taskforce of the Department of the Prime Minister and Cabinet. We suggest that any proposals being advanced as part of this initiative are discussed and assessed by this Taskforce.

---

[8] Office of the Australian Information Commissioner, "Chapter 11: APP 11 — Security of personal information", accessed at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information/#ftn1

b. Considerations in relation to standards for smart devices

Discussion questions:

- *What is the best approach to strengthening the cyber security of smart devices in Australia? Why?*
- *Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt for as a standard for smart devices?*

i) Current voluntary code of practice is still new

Given the complexity of cyber security and the wide range of technology applications, we support the Government's current approach in relation to setting voluntary standards. As the discussion paper notes, on 3 September 2020, the Australian Government released the voluntary Code of Practice: Securing the Internet of Things for Consumers (Code of Practice). The Code of Practice contains thirteen principles that signal Government expectations to manufacturers about the security of smart products. This voluntary code would have only been in operation for several months when the discussion paper was being prepared, during a pandemic that has had negative impacts on business collaboration within and across companies; We would argue that it is premature for a discussion about how the code might be replaced. Should the uptake of the code not meet the Government's expectations, particularly in any priority sectors of the market, we encourage targeting sector support, outreach and awareness raising initiatives about the code to those businesses who are contributing to the greatest cyber security risks, at a time where health orders enable this to be conducted in a comprehensive way.

Having the flexibility of a voluntary standard is particularly important in relation to smart devices, which include both hardware and software. 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 will 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. This is why voluntary codes that outline norms and best practice are a good approach, as they can be flexibly adapted in relation to a range of technology applications.

We emphasise 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 welcome the fact Australia's existing voluntary code aligns with the UK's Code of Practice European Telecommunication Standards Institute (ETSI) baseline standard on smart devices (ESTI EN 303 645). ETSI EN 303 645 is the world's first globally-applicable standard for the cyber security of consumer Internet of Things (IoT) devices.

Building upon this, DIGI echoes the principles put forward by The Information Technology Industry Council (ITI), a US trade association representing the technology industry, that advocates for public policies and industry standards that advance competition and innovation worldwide. In a submission dated August 17 2021 to the National Institute of Standards and Technology (NIST) on consumer labelling[9], ITI puts forward several recommendations relevant to this initiative, summarised as follows:

[9]ITI, (17/8/21), ITI Comments on Cybersecurity EO's Consumer Software Labeling Program, accessed at https://www.itic.org/documents/cybersecurity/ITICommentsonSoftwareLabelingFinalVersion.pdf

Ensure Labeling Does Not Convey a False Sense of Security: While labels may help incentivize the adoption of the underlying security practices, they should not be perceived as a substitute for processes to build security and trust.

Raise End-User Awareness and Balance Responsibility: The goal should be enabling consumers to make intelligent purchasing decisions rather than driving post-purchase behavior. Both consumers and manufacturers must understand their respective roles in maintaining cybersecurity.

Allow for Flexible Labeling Formats and Conduct Periodic Reviews: Any labeling scheme should be flexible to accommodate a range of formats, including e-labeling for digital listings in online marketplaces, machine-readable codes, and other forms of communication that effectively convey the security information to the intended audience.

Recognize Conformity Assessments by Suppliers/Vendors and Facilitate Mutual Recognition: We encourage the U.S. government to recognize conformity assessments by vendors, as well as third-party assessment labs, to facilitate the mutual recognition of labeling schemes across international jurisdictions.

Align with International Standards and Best Practices: Proposed guidelines, best practices, or standards must be technology-agnostic and account for the risk levels associated with software components that specifically focus on "consumer" products, not business products to protect enterprise software. This tiered and narrow approach will help companies tailor the guidelines, best practices or standards to different types of software[10].

We encourage the Department to fully consider each of these principles in the reform proposals that emerge from this initiative.

ii) Considerations for online marketplaces

Discussion questions:

- *[For online marketplaces] Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?*
- *What would the costs of a mandatory standard for smart devices be for consumers, manufacturers, retailers, wholesalers and online marketplaces? Are they different from the international data presented in this paper?*

Most major online marketplaces already have in place report and take down procedures for listed items that are in breach of Australian safety or other regulatory requirements, and voluntarily remove these under these policies. For major online marketplaces, we would expect that if a standard were to be introduced, listed devices that were in breach would be removed on a similar basis once referred to them.

It is worth noting that there is already extensive work and collaboration between major marketplaces and the Australian Government in order to ensure the removal of such products. For example, earlier

[10]ITI, (17/8/21), ITI: Regular Consumer Software Labeling Reviews Needed to Address Evolving Cyber Risks, accessed at https://www.itic.org/news-events/news-releases/iti-regular-consumer-software-labeling-reviews-needed-to-address-evolving-cyber-risks

this year, eBay recently launched a Regulatory Portal[11]. In a first for an online marketplace, the portal empowers trusted authorities from around the globe, including the ACCC, to efficiently report and remove listings for illegal or unsafe items. It allows a regulator to remove listings from the eBay marketplace without additional approval from eBay itself. In the event a standard was introduced, the Department of Home Affairs could similarly be onboarded as a regulator to eBay's Regulatory Portal so that it can work collaboratively in the reporting and take down of items.

In relation to the costs of a mandatory standard, with the breadth, scope and substance of such a mandatory standard still under consideration an accurate assessment of its relative costs is difficult to estimate. DIGI generally believes that the responsibility to communicate the standard should remain with the manufacturer, including when smart devices are offered for sale via an online marketplace. Having said that, there will be situations where the manufacturer is not responsible for the software that would determine a consumer's cyber security over time; again, this is why voluntary codes that can be flexibly adapted across a wide range of actors and supply chains across the ecosystem are a far more effective tool. We encourage exploration of such codes before any standard is contemplated.

For online marketplaces, the breadth of a possible standard (i.e. the number of goods to which it is applied) would have a substantial flow on costs in terms of monitoring and responding to take down requests and investments in building scale solutions, such as filters and blocks. Similarly, the substance of the standard and whether obligations are placed on online marketplaces to include warnings or other information would have significant cost impacts, as third party online marketplaces are not the party that offer or list an item for sale. Many third-party marketplaces enable consumers to sell second-hand smart devices directly to other consumers; this common consumer behaviour shows the limitations if a standard were imposed on retailers. This scenario highlights the importance of wider consumer education, rather than labelling or expiration dates, so as to increase consumers' awareness of the fact that software updates are critical to ensuring the ongoing security of smart devices.

c. Considerations in relation to labelling for smart devices

Discussion questions:

- Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?
- What is the best approach to encouraging consumers to purchase secure smart devices? Why?

Any sort of physical labelling of smart devices would be rendered obsolete by the time the device is sold. If a labelling scheme for smart devices is being considered, it would need to be digitally through an e-label or QR code that would communicate an up-to-date list of supported security features which can be updated as needed. This would be preferable to a static label that cannot be changed once applied to a device or packaging. It is important to note that not all devices will be able to carry a physical label because of their size or other attributes (e.g. wireless headphones), and also that consumers are likely to promptly discard a device's packaging.

[11]eBay, (24/5/2021), "eBay launches new Regulatory Portal to further protect consumers", accessed at https://www.ebayinc.com/stories/press-room/au/ebay-launches-new-regulatory-portal-to-further-protect-consumers/

Having said that, it is important to fully consider the ramifications of any labelling scheme introduced in Australia. In a position paper titled *Cybersecurity Labeling: A Guide for Policymakers*[12] that we encourage the Department to review, ITI advances several points that we believe are pertinent to the discussion of labelling for smart devices in Australia. In this paper, ITI cautions that cyber security labeling 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 that we are toward the bottom of the OECD in relation to ICT exports, per Figure 1 above[13].

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 "labeling should not convey a false sense of security". Furthemore, we are not aware of any evidence that labelling would serve to actually change consumer behaviour for cyber security.

It is in that context, that we strongly caution the Australian Government against the proposal of a cyber security expiry date. Such a proposal may encourage service providers and manufacturers to put forward an arbitrary date in order to fulfil such a requirement. It will not always be known to all service providers and manufacturers years in advance as to when, or whether, their cyber security support of a product will expire. In addition, relevant technology service providers will encourage their users to update their software or apps, in order to reflect the latest security protections; however, consumers often delay or ignore these updates, which creates security vulnerabilities. An expiration date may serve to further discourage the updating of software as consumers falsely believe that their devices are fully protected up until the expiration date provided at the point of purchase.

Furthermore, in relation to physical consumer goods, an expiration date would negatively contribute to e-waste in Australia as it could encourage consumers to discard their devices after that date. The label would likely be misunderstood by consumers who believe devices have expired, when all that is required is a software update to protect the user. Devices and software do not expire, if updated in a timely manner. Australia is the fifth the highest producers of e-waste per capita, producing 21.7kg per capita in 2019[14]. We need to be mindful of creating policy settings that further encourage this consumer behaviour and environmental impact.

Finally, as the discussion paper acknowledges, Australia would be the first country to mandate such an expiration label. As previously noted, we must strive for interoperability with our cyber security consumer protections, otherwise we risk creating barriers to trade. Whenever Australia contemplates a "world first" approach to technology policy, we need to fully evaluate why other jurisdictions may have rejected the approach. Additionally, we should also consider how it might impact the Australian Government's goal to be a leading digitally-enabled economy by 2030 under its Digital Economy Strategy. We need to be acutely aware of Australia's starting point in our efforts towards that goal, as today we have the second smallest technology sector in the OECD[15]. While the incentives under the

---

[12]ITI, (April 2021), Cybersecurity Labeling: A Guide for Policymakers, accessed at https://www.itic.org/documents/cybersecurity/ITI_CybersecruityLabeling_Final_Apr2021.pdf

[13] AlphaBeta (September 2019), *Australia's Digital Opportunity*, accessed at: https://digi.org.au/wp-content/uploads/2019/09/Australias-Digital-Opportunity.pdf

[14] Global E-waste Monitor data quoted in Tech Guide (8/7/21), "Australia among the highest producers of e-waste - and it's set to soar", accessed at https://www.techguide.com.au/news/gadgets-news/australia-among-the-highest-producers-of-e-waste-and-its-set-to-soar/

[15] AlphaBeta (September 2019), *Australia's Digital Opportunity*, accessed at: https://digi.org.au/wp-content/uploads/2019/09/Australias-Digital-Opportunity.pdf

Government's Digital Economy Strategy are extremely important, the strategy also needs to critically examine Australia's technology reputation, and the barriers to investment that we may inadvertently create through various Government initiatives. 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.