TELSTRA CORPORATION LIMITED

STRENGTHENING AUSTRALIA'S CYBER SECURITY REGULATIONS AND INCENTIVES

Public submission

27 August 2021

CONTENTS

EXECUTIVE SUMMARY

A digital economy built on a secure foundation is key to generating trust and confidence in the products and services that connect us all. Virtually every sector of the economy depends on the stable and secure functioning of the internet to deliver essential services to populations around the globe. Building this secure foundation is a shared responsibility for governments, the private sector and the community.

We support the government's desire to improve cyber security across the economy and believe there's a role for government in addressing the issues identified in *Strengthening Australia's cyber security regulations and incentives* (the Paper). In general, we believe the existing, principles-based and technology neutral frameworks cited by the Paper are fit for purpose and, while they do not provide for the direct application of specific cyber security standards, they do provide flexible and enforceable frameworks for addressing the issues of concern.

Improving governance standards for large business

We support the Government's intent to improve cyber security governance in larger businesses with a view to better cyber security outcomes for Australian businesses and the community. Directors and officers of listed companies already need to understand and continually reassess existing and emerging risks that may be applicable to the company's business, this includes cyber related risk. These existing obligations and liabilities are sufficient and provide appropriate enforcement mechanisms. We believe governance standards for cyber security risks can be raised within this existing framework by Government producing clear guidance on how company directors should consider cyber risk and in developing some 'best practice' approaches to mitigating cyber risk. Such guidance would be similar to the approach which has already been used for the management of climate-related risk, where the Australian Securities and Investment Commission has provided guidance on how directors should consider climate risk.

Minimum standards for personal information

We don't believe a mandatory code of practice for personal information under the Privacy Act would be effective in lifting the baseline cyber security precautions of small and medium businesses: coverage of the Privacy Act is limited to businesses with a turnover of at least $3 million. We believe a more effective way of achieving the desired outcome would be a targeted campaign promoting adoption of the Australian Signal Directorate's 'Top 4'. Adoption of the Top 4 would mitigate over 85% of adversary techniques used in targeted cyber intrusions.

Standards and labelling for smart devices

We support an industry led, voluntary, approach to standards and labelling for smart devices. Given the diversity of 'smart' devices, services, contexts, deployment and use scenarios, a 'one size fits all' statutory requirement that a device or service be 'secure' is unlikely to produce the desired security outcome, or to provide appropriate incentives for consumers and suppliers to provide appropriate instructions and support to address security vulnerabilities over time.

We support the IoT Alliance Australia's proposal for a consumer-informed, voluntary, market driven, industry-led certification and labelling scheme. We consider there is sufficient support for an industry-led scheme. That said, there is a role for government to assist with education and awareness of the scheme. Increasing community awareness of the scheme will ensure consumers and businesses will seek

devices that are certified and labelled, creating the market incentives for manufacturers to become certified under the scheme.

Responsible disclosure

We support the development and promotion of a toolkit (aligned with the relevant industry standard), similar to the excellent example available from the UK's National Cyber Security Centre, which provides guidance on what a policy should contain and how to help researchers who find a vulnerability to communicate with the relevant organisation. Such a toolkit should be accompanied by targeted awareness and promotion of the toolkit to make it simple for vendors to adopt.

Health checks

We support the introduction of optional cyber security health checks for small business and a 'trust mark model', similar to the UK's 'Cyber Essentials' program. If health checks were to become mandatory in certain situations, such as tendering for government contracts, consultation should take place with affected parties and sectors on the technical design of the trust mark, to ensure that it aligns with any existing and emerging security baseline regulations that may already exist for those businesses and sectors.

Legal remedies for consumers

In our view, the principles-based Australian Consumer Law (ACL) is sufficiently broad to address cyber security challenges. We think the most effective way to make Australia's digital economy more resilient to cyber security threats is to improve awareness and knowledge of cyber security issues.

A well-resourced Office of the Australian Information Commissioner (OAIC) is a more effective way of continuing to pursue the Privacy Act's objectives than the introduction of a direct right of action. This is because the current OAIC complaints process gives complainants a better result in a more timely and cost effective manner than direct court action. It is also our view that targeted cyber security awareness and education programs, with associated guidance materials, is the most effective way to incentivise businesses that haven't already implemented minimum security standards to improve their cyber practices and better protect personal information.

01 Introductory comments

Telstra welcomes the opportunity to make a submission in response to the Department of Home Affairs call for views *Strengthening Australia's cyber security regulations and incentives* (the Paper). We believe a digital economy built on a secure foundation is key to generating trust and confidence in the products and services that connect us all. Virtually every sector of the economy depends on the stable and secure functioning of the internet to deliver essential services to populations around the globe. Building this secure foundation is a shared responsibility for governments, the private sector and the community.

We are strong proponents of evidence-based public policy that is grounded in a fundamental understanding of both technology and threat. Our contribution to this important national discourse is grounded in the expertise of our internal cyber security team. Our people hold industry-leading technical and policy knowledge in areas including 5G, critical infrastructure protection, incident response, cyber threat intelligence, national security, strategic policy, cyber risk, cyber skills development, behavioural influence and diversity and inclusion.

We are proud to assist our customers in improving and securing the ways in which they live and work. Given our place in Australia's telecommunications past, present and future, we recognise that our role does not stop at our own networks. We know that we have an important role to play in securing the wider cybersecurity ecosystem and supporting our nation to be cyber resilient. As such, we have a long history of working alongside the Australian Government on both operational security and cyber policy issues.

We support the intention of improving cyber security and think the way to make Australia's digital economy more resilient to cyber security threats is to improve awareness and knowledge of cyber security issues and to provide strong incentives for Australian businesses to invest in cyber security. Our comments in response to each of the proposals put forward by the Paper are based on the fundamental premise that cyber security is a true partnership between Government and industry.

02 Why should government take action?

There is a role for government to provide best practice guidance and advice to organisations on how to best secure themselves against cyber threats. This advice should be informed by Australian Cyber Security Centre's (ACSC's) new Cyber Enhanced Situational Awareness and Response (CESAR) function and broader awareness of the types of threats impacting different sectors, and types of organisations.

Government has worked extensively this year to introduce cyber security legislative baselines for critical infrastructure. There is an opportunity to look across organisations not captured by these new laws to identify where and how an uplift in these organisations could take place. In the first instance, we believe there are a number of non-regulatory options which should be deployed to address inhibitors preventing these businesses from properly investing in cyber security and responding to cyber security incidents.

This should be supported by research to understand business behaviours and commercial drivers or barriers to increased investment in cyber security. The challenges facing organisations are both diverse and nuanced and will require varying policy approaches to address.

1 What are the factors preventing the adoption of cyber security best practice in Australia?

The factors contributing to low adoption of good cyber security practices in Australia can broadly be grouped into two categories; a confirmation bias (it won't happen to me) leading to apathy in seeking to understand and mitigate the risk of an attack, or if the risk and consequence of an attack is well understood, not knowing where to start. It is important to look at both broad categories in a business and a consumer context.

Starting with confirmation bias, businesses and consumers underestimate the potential consequences of an attack because their risk appetite (willingness to consciously or unconsciously take on risk) is clouded by a confirmation bias; "it won't happen to me". Businesses and consumers seek to lower cost, or value functionality and experience over security, driving markets to consider security as an add-on that comes in after the product or service has been designed, rather than seeking to develop or purchase products and services that have built in 'security-by-design'. While consumers may have an inherent expectation that a product or service is secure, it is not usually a high priority in the purchasing decision.

However, awareness of the number, sophistication and real-world impacts of cyber-attacks is starting to reduce this cohort, leading to the second category, knowing where to start and what to do about the risk of cyber-attack. Vulnerabilities, both in a corporate/business and a consumer sense are not well understood, and mitigation techniques are likely even less understood. There is a lack of simple, easy to implement guidance that is relevant to an organisation's overall business risks. This is compounded by an ever-evolving threat landscape that makes it difficult for businesses and consumers to stay current with risk mitigation techniques.

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

It is not necessarily the case that 'lax' cyber security practices or incidents merely result in negative externalities for the organisation concerned. There are significant reputational and potential financial risks associated with organisations failing to maintain good cyber security practices. Suppliers can lose major contracts and public trust if their products and services are seen to be 'insecure'. It would also be difficult in some circumstances for government to ascertain if organisations had been deliberately or consciously negligent if minimum standards and baselines had not yet been established for that type of product or service category.

Government's role should be to reinforce the market implications of poor cyber security practices and insecure products to key product, technology and service organisations. While larger organisations will most likely already be well attuned to these risks, more attention will need to be given to smaller organisations who may not fully understand the value of the data they hold and the potential implications from the misuse, loss or compromise of their data, systems or technology.

There is also a role for government in educating consumers on how to make informed cyber security purchases. This could include: what does a good product or service look like? What are the minimum standards that the government recommends they look for? Government could look to build this into the cyber awareness uplift announced in the 2020 Cyber Security Strategy.

03 The current regulatory framework

Chapter 3 of the Paper examines three cross sectoral regulations that impose cyber security obligations on Australian businesses, being the Privacy Act, the ACL and the Corporations Act, with a focus on improving the cyber resilience of those businesses that are not captured by sector specific cyber security regulations.

We agree that the limited coverage and the principles-based approach under these regulatory frameworks mean they are not vehicles for introducing prescriptive cyber security standards that would apply to all businesses. However, we do not consider these as limitations in the regulations that need to be 'fixed'.

These broad, principles-based and technology neutral frameworks have proven capable of effectively managing evolving risks, whether they be environmental, compliance or cyber risks. Where additional clarity is required, this can be effectively addressed through the development of guidance materials. For example, guidance by the Australian Securities and Investments Commission makes it clear that disclosing and managing climate-related risk is considered a key director responsibility under the Corporations Act.[1] Similarly, the OAIC guidance on the 'reasonable steps' required to protect personal information under APP 11 lists mitigating ICT risks as being relevant based on the circumstances and the nature of the personal information being held.

Rather than seek to impose prescriptive cyber security standards in addition to, or alongside, these existing principles-based frameworks, we believe the most effective way to incentivise the wider economy to invest in cyber security is through raising awareness of these existing obligations and introducing education programs to explain how cyber risks sit within these general frameworks.

3 What are the strengths and limitations of Australia's current regulatory framework for cyber security?

Current cyber-related regulation in the Australian landscape is either privacy-focused (e.g. the Mandatory Data Breach Notification scheme, Privacy Act) or sector-focused (e.g. APRA CPS234, TSSR). Strengths of CPS234 and TSSR are that they provide relatively high-level security requirements, giving mature organisations the flexibility to tailor their approach, the 'how' of meeting those requirements, to their organisational context, threat environment and risk appetite, and take ownership of managing those cyber risks and communicating with the regulator.

For less cyber-mature organisations including small businesses, it is more difficult to take this same risk-based approach because there is generally not the in-house expertise to understand and respond to the threat environment. For example, applying the Essential Eight maturity framework currently requires organisations to understand what types of cyber threat actors may be targeting them.

When cyber risk is framed in terms of business risk (i.e. as a key factor in financial, reputational, operational risk), then the incentive to the business to have good cyber security is partly the impact that realisation of these risks can have across its operations. If security requirements are not articulated in a way that clearly links their success to key business risks to an organisation (e.g. financial loss) it will merely create extra work for the business alongside their existing operations, which will be deprioritised or result in little impact to improving security.

Therefore, for the wider economy, clearer baseline guidance and support with implementation is needed, and baseline security measures should be tied to the positive business impacts they will have. This type of information should include practical 'toolkits' for small business and should outline where these businesses can go for help or additional information.

[1] https://aicd.companydirectors.com.au/membership/company-director-magazine/2021-back-editions/february/managing-climate-risk-for-directors

4 How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

As we have outlined above, we believe there are appropriate principles-based and technology neutral regulations which can be leveraged to improve cyber security across the economy. If new regulatory obligations are to be introduced, they should be easy to remember and communicate: a small number of baseline measures translated into clear, high-level guidance that applies across sectors, is easy to understand and implement for all entities including small business, and explicitly linked to positive economic and consumer impact.

However, as an alternative, we suggest the government consider whether the desired outcomes could be achieved through non-regulatory approaches including:

- Increased, targeted awareness coordinated across industry and government for smaller businesses.
- Guidance and toolkits.
- Targeted board education (linked to existing Board duties) particularly guiding Boards on which questions to ask of the business on cyber issues, and how to interpret the answers.
- 3P cyber maturity assessments for organisations to identify gaps and prioritise investment.
- Some large enterprise organisations already work with strategic partners to supply product and service offerings that have security mechanisms built in and turned on by default to protect their customers, including small businesses. This is a model that could be further developed and aligned with best-practice guidance e.g. Top 4, Essential Eight.

04 Improving governance standards for large businesses

We support the Government's intent to improve cyber security governance in larger businesses with a view to delivering better cyber security outcomes for Australian businesses and the community. However, cyber risk (like other risks) need to be considered as part of an enterprise wide risk management framework. Directors and officers of listed companies need to understand and continually reassess existing and emerging risks that may be applicable to the company's business. These existing obligations and liabilities are sufficient and provide appropriate enforcement mechanisms.

With the exception of the proposed Critical Infrastructure—Systems of National Significance (CI-SoNS) reforms, we do not consider there is any need to impose cyber security specific obligations on large business. Instead, we believe an uplift in cyber security outcomes would best be achieved by increasing awareness and increasing the availability of clear guidance material related to cyber security.

The generic (and principles-based) approach of director's obligations provides an appropriate, and sufficiently flexible framework to assess cyber security risks and their appropriate mitigations. This framework and approach has already been used for the management of climate-related risk, with the Australian Securities and Investment Commission providing guidance on how directors should consider climate risk.[2] This flexible approach has allowed the guidance to vary as climate risk has evolved and we believe a similar approach would be appropriate for the ever changing cyber security environment.

[2] https://asic.gov.au/about-asic/news-centre/articles/managing-climate-risk-for-directors/

In addition to awareness raising and the development of guidance on 'best practice' cyber security mitigations, we believe implementation of the proposed CI-SoNS reforms will play a role in further raising awareness of cyber risk. While the application of the proposed CI-SoNS reforms is limited to the owners and operators of critical infrastructure, we expect increased awareness of cyber security issues driven by proposed obligations will flow to other businesses through the supply chain.

5 What is the best approach to strengthening corporate governance of cyber security risk? Why?

As noted above, rather than impose a prescriptive standard (either voluntary or compulsory) to cyber security as suggested by the Paper, we consider there is some 'middle ground' between option 0 (status quo) and option 1 (a voluntary standard). We believe there is a role for Government in producing clear guidance on how company directors should consider cyber risk and in developing some 'best practice' approaches to mitigating cyber risk.

Of the options presented, we favour option 1, the introduction of a voluntary standard incorporated into existing duties, backed up by targeted awareness, support and guidance. Any standard would need to be flexible enough to evolve with changes in the cyber threat landscape.

6 What cyber security support, if any, should be provided to directors of small and medium companies?

Similar to our suggestions for large business, clear consistent guidance should be provided. For small and medium enterprises, this should focus on where to go for additional help or assistance. The ACSC could hold awareness workshops and produce self-assessment guides.

7 Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

As noted above, we believe guidance similar to that provided by ASIC for climate risk could be provided for cyber risk.

05 Minimum standards for personal information

The Paper proposes two policy options to increase the adoption of technical standards; option 0 (status quo) and option 1 (a mandatory cyber security code for personal information). We support raising the cyber security resilience of Australian businesses by accelerating the voluntary adoption of technical cyber standards.

According to the ASD, properly implementing application whitelisting, patching applications, patching operating systems and restricting administrative privileges (the Top 4) mitigates over 85% of adversary techniques used in targeted cyber intrusions.[3]

Many larger organisations are well aware of these cyber risks and already comply with global standards (such as ISO27001) or sector specific cyber security standards (APRA CPS-234), so would be excluded from the application of any minimum standard under the Privacy Act. Smaller organisations generally have less awareness about cyber security risks and require a higher level of guidance and support, however the Privacy Act does not apply to small businesses with an annual turnover of less than $3 million. Given these limitations, we do not believe codifying baseline cyber standards under the

[3] https://www.cyber.gov.au/sites/default/files/2019-03/Mitigation_Strategies_2017.pdf

Privacy Act (option 1) will be an effective way to raise cyber security resilience amongst Australian businesses.

The Privacy Act also presents several other limitations. A prescriptive mandatory code goes against the principles-based nature of the Privacy Act and risks becoming quickly outdated unless regularly reviewed. A mandatory code would also require proactive oversight by the OAIC, and the development of assurance and enforcement mechanisms to ensure the code is implemented across all relevant APP entities. The OAIC does not currently have the resources or skill set to manage a mandatory cyber code and there would also be inhibitive compliance costs for AAP entities.

Nor do we agree with option 0 (status quo). Instead, we support targeted cyber awareness and education programs, and guidance on minimum cyber standards, that are not tied to the Privacy Act or APP entities. These could leverage the existing resources and expertise of the ACSC and be targeted towards specific services or industries (such as the suppliers of digital products and services).

For APP entities, the current principle-based APP 11 already provides an adaptable and flexible mechanism to address an evolving threat landscape and promote the uptake of cyber security practices. Its effectiveness could be further bolstered by the targeted awareness and education programs suggested above, coupled with more OAIC guidance about what 'reasonable steps' means for APP 11 in the context of cyber security, existing ACSC resources and the nature of the relevant personal information.

8 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?

As noted above, we do not agree that a mandatory cyber security code under the Privacy Act is the most effective way to raise cyber security resilience. A mandatory code with prescribed technical controls would go against the principle-based nature of the Privacy Act and importantly it wouldn't capture small businesses with less than $3 million turnover. The OAIC does not currently have the resources or skill set to develop, maintain and enforce a mandatory cyber code and there would also be inhibitive compliance costs for AAP entities.

Instead, we support targeted cyber awareness and education programs, and guidance on minimum cyber standards, that leverages the expertise of the ACSC and is not tied to the Privacy Act. We also believe the current principle based APP11 provides an adaptable and flexible mechanism to address an evolving threat landscape and promote the uptake of cyber security practices for APP entities.

9 What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?

As noted above, we do not agree that a mandatory cyber security code under the Privacy Act is the most effective way to raise cyber security resilience. However, we agree that any guidance about minimum cyber standards should address the risks identified in Chapter 5 of the consultation paper, being encryption of data in transit and at rest, strong passwords, multi-factor authentication and timely application of critical patches.

We agree with the observations in the consultation paper that Essential 8 is not an appropriate minimum standard and that it is important to avoid any conflict with existing best practice cyber standards and regulations.

10 What technologies, sectors or types of data should be covered by a code under the Privacy to achieve the best cyber security outcomes?

Due to the limitations flagged above, we do not believe that a mandatory cyber security code under the Privacy Act will achieve the desired cyber security outcomes.

Cyber security awareness and education programs and guidance material could be effectively targeted at specific sectors or technologies, including the digital economy or smart devices.

06 Standards for smart devices

Chapter 6 of the Paper commences with a brief definition of smart devices that are "*… given extra functionality to connect to the internet …*", citing examples such as smart-TVs, baby monitors and Wi-Fi routers. We agree with this definition, and as a leading supplier of telecommunications products and services to both consumer and business markets, we consider the range of devices encompasses much more, including mobile phone handsets, fixed line (nbn) gateway routers in residential houses and small businesses, and the myriad of "dumb" IoT sensors that are nonetheless connected to the internet.

The Paper proposes two policy options in relation to standards for smart devices; option 0, status quo and option 1, mandatory standards such as ETSI EN 303 645. We consider neither of these approaches is optimal. Simply maintaining the status quo will not improve Australia's security position which is clearly not acceptable, and mandating compliance under a "one-size-fits-all" approach involving one or more standards fails to recognise the diversity and complexity of cyber security risks, and is unlikely to be able evolve quickly enough to adapt to the constantly changing threat landscape.

For clarity, in this statement we are not saying that standards such as ETSI EN 303 645 will not play a role in improving Australia's cyber-security posture; on the contrary, standards such as this will play a foundational role. Other publications such as the NISTIR 8259 suite on Foundational Cybersecurity Activities for IoT Device Manufacturers[4], or ENISA's Baseline Security Recommendations for IoT[5] are further examples of complementary (not competing) approaches that could also play an important role in strengthening cyber security for smart devices in Australia.

The NISTIR 8259 publication is germane in that it encourages manufacturers of devices to directly consider the *context* in which devices will be used. Context is multi-faceted, including several devices operating in combination or solutions comprising both devices and other system components such as cloud storage and analysis of data. As NIST note, "*Some IoT devices may be dependent on specific other devices (e.g., an IoT hub) or systems (e.g., a cloud) for some functionality. IoT devices will be used in systems and environments with many other devices and components, some of which may be IoT devices, while others may be conventional information technology (IT) equipment*."[6] Importantly, NIST goes straight on to observe that all parts of the IoT ecosystem other than the IoT devices themselves are out of scope of the publication, highlighting the point that a single standard cannot encompass the full end-to-end service or solution that a smart device resides in. Similarly, ETSI EN 303 645 specifically excludes any devices not considered to be "consumer IoT devices".[7]

Our point here is mandating compliance with one or more standards or publications in isolation of context, deployment scenarios or an end-to-end consideration of the service that the smart device resides in will be insufficient to change Australia's cyber security posture, or to manifestly change attitudes within the vendor or consumer communities toward cyber security, as we discussed in section 02. While a specific standard such as ETSI EN 303 645 in its specific context (consumer IoT

[4] National Institute of Standards and Technology Interagency/Internal Report (NISTIR) suite of publications including NISTIR 8259, NISTIR 8259A and NISTIR 8228 on **Foundational Cybersecurity Activities for IoT Device Manufacturers**, May 2020, available at https://csrc.nist.gov/publications/detail/nistir/8259/final

[5] The European Union Agency for Cybersecurity, ENISA. **Baseline Security Recommendations for IoT**, November 2017, available at https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[6] NISTIR 8259, section 1.1, p.1.

[7] ETSI EN 303 645, section 1, p.6, "*Devices that are not consumer IoT devices, for example those that are primarily intended to be used in manufacturing, healthcare or other industrial applications, are not in scope of the present document*."

devices) is essential, cyber security must be assessed holistically, and failure to take this approach is likely to lead to false sense of security.

In essence, given the diversity of IoT devices, services, contexts, deployment and use scenarios, a 'one size fits all' statutory requirement that a device or service be "secure" is unlikely to produce the desired security outcome, or to provide appropriate incentives for consumers and suppliers to provide appropriate instructions and support to address security vulnerabilities over time.

11 What is the best approach to strengthening the cyber security of smart devices in Australia? Why?

We consider that neither approach proposed in the Paper (option 0 or option 1) is preferable. Instead, we recommend an approach that will provide incentives to both manufacturers and consumers (including business and government) to improve security is the preferred approach to strengthening cyber security of smart devices in Australia. This means a scheme where manufacturers are driven by market incentives to build in appropriate security measures into their devices to competitively differentiate their products from those of their competitors. On the demand-side, consumers are already aware of the risk and potential cost of being victim to a cyber-attack, and hence have the incentive to seek out secure devices, however they need to be informed as to which devices are secure. To do this, devices must be labelled to show that they have been tested and certified against current and appropriate industry standards for cyber security, such that consumers can make informed choices.

We observe the IoT Alliance of Australia (IoTAA) proposes a consumer-informed, voluntary, market driven, industry-led certification and labelling scheme. We agree with and support their proposal as the preferred option to strengthening the cyber security of smart devices in Australia.

12 Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt as a standard for smart devices? If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate? If not, what standard should be considered?

This question tackles two concepts: *adopting* a standard for security of smart devices and *mandating* a standard. We respond to each concept individually.

Considering the adoption of a standard for the security of smart devices, ESTI EN 303 645 is a very good starting point and is likely to form a cornerstone of a regime to strengthen the cyber security of smart devices, although we see a role for other standards such as NISTIR 8259. As we have noted, standards such as these are necessary, but not sufficient.

The second part of this question looks at whether parts of a standard should be mandated. We consider it is not practical or useful to mandate any part of a standard for the security of smart devices in Australia. The fifth requirement in the ETSI standard, "Communicate Securely" provides a straightforward example. Provision 5.5-1 says "*The consumer IoT device shall use **best practice** cryptography to communicate securely*." (emphasis added). ETSI then go on to observe that secure communication is *context specific*, implying that no one specific type of cryptography would be considered "best practice" in every scenario, and then note that "*As security is ever-evolving it is difficult to give prescriptive advice about cryptography or other security measures without the risk of such advice quickly becoming obsolete*."

ETSI are saying that "best practice" is both context specific and temporal. If the fifth provision of ETSI EN 303 645 was "mandated", how would compliance be determined in the absence of documenting every context and prescribing the requisite level of cryptography for that context, as well as keeping the list up to date as cryptography evolves?

In short, we consider it is not practical or helpful to *mandate* any part of a standard as a requirement for the security of smart devices.

13 Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?

All devices sold by Telstra, either discretely or as part of a service (e.g., a nbn gateway modem supplied as part of a fixed broadband service) are rigorously tested before being sold to market, either on-line or through physical stores. Secondly, we consider that simply removing a device from a marketplace does nothing to resolve a potential security flaw for existing customers. Thirdly, as we've noted, compliance with specific standards should be context specific, and not a mandated requirement.

That said, if a device was determined to have security flaws after its release for sale, we would take action to mitigate the flaw from a range of possible activities, including remotely patching the software or firmware in the device itself, providing instructions to the user of the device to take action, providing remediation at a different point in the solution[8], or in the event no other remediation options exist, recall the device. Some of these actions, such as remotely patching the device, could be triggered on the first activation of the device (when it first connects to the internet) such that there is no need to remove a smart product from sale.

14 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?

No response.

15 Is a standard for smart devices likely to have unintended consequences on the Australian market? Are they different from the international data presented in this paper?

Devices operating in combination, including solutions comprising both devices and other system components such as cloud storage and analysis of data, are difficult architectures for a single (or even multiple) standards to encompass. While a specific standard (e.g., ETSI EN 303 645) in its specific context (devices) may not have any gaps or unintended consequences per se, consumers may nevertheless obtain an inflated sense of security from simple compliance to a standard.

07 Labelling for smart devices

Chapter 7 of the Paper contemplates a labelling scheme for smart devices. The chapter commences by observing that "*consumers do not currently have the tools to easily understand whether smart devices are cyber secure*…". We agree with this observation. Labelling devices that have been independently tested and certified is a method to inform and empower purchasers of smart devices to choose devices and services that are certified against good security practices. We support the introduction of a labelling scheme for smart devices in Australia, so long as the labelling scheme provides *meaningful* advice to consumers and is *cost effective* for vendors and retailers to implement.

As we noted in chapter 6, defining security for smart devices should not be against a rigid standard, but rather, is a context relevant, fit-for-purpose assessment of the device or end-to-end service against an appropriate level of security, which as we have outlined, is likely to change over time as the threat landscape changes and evolves. It is therefore important that any labelling scheme enables a diversity of security settings to be accommodated and updated over time, recognising that products may be "secure" in some contexts or at a particular point in time, but may be insecure in others. Herein lies the challenge.

[8] For example, individual sensors in an agricultural monitoring solution may not have to be individually patched if the hub device can be updated to compensate for the issue.

We have no objection to a labelling scheme that conveys different levels of security certification, such as the Cybersecurity Labelling Scheme (CLS) for manufacturers developed by Singapore's Cyber Security Agency (CSA) which is a "star-rating" scheme. At the same time, we urge some caution. Unlike star-rating schemes for energy and water efficiency,[9] measuring cyber security is not a simple, linear, objective measurement. By way of example, consider a simple single-vector IoT sensor (e.g., a temperature sensor or soil moisture sensor) being certified under the CLS. A self-assessment and declaration by the developer is entirely appropriate for this type of device, and assuming the developer also meets the lifecycle requirements of Tier 2 in the CLS, then the device earns a two-star rating on the four-star rating scale. Does two-stars out of four mean it is only "50 percent secure"? Not at all. If the vendor has been diligent in their assessment and used a standard such as ETSI EN 303 645 as the baseline for built in security-by-design during the sensor's development, its security will be best practice. But it only earns two-stars because it hasn't been independently tested by a third party. This is potentially misleading for consumers who may conclude that two-stars means the device isn't as secure as it could be.

We fully recognise that any labelling scheme is a simplification designed to convey information in an easy-to-understand format for average consumers, and the "simplification" in the message necessarily means a loss or abstraction of underlying information. It is therefore possible to illustrate examples where the message the scheme conveys is less than ideal, as we have just done. We are in no way saying Singapore's CLS is a bad scheme; on the contrary, the CSA (i.e., the Singapore Government) is to be congratulated for taking the lead and being one of the first countries globally to launch a labelling scheme. What we are saying, is that if a star-rating scheme is to be used in Australia, it is likely to require careful thought as to the information the stars convey and may require considerable education. The stars in the CLS show the level of *testing* (self-assessment, independent third party, and penetration testing); which acts as a proxy to the *level of security* of the device.

Nonetheless, in our view it is better to launch some form of scheme to convey some form of information to consumers, than abandon the idea of introducing labelling altogether (throwing the proverbial baby out with the bathwater). Health-star rating schemes for food are regularly criticised[10] along these lines, and there are probably lessons from this scheme that could assist with the development of a cyber security labelling scheme for smart devices in Australia.

We have stronger reservations about the second labelling option proposed in the Paper, the mandatory expiry date label. As the Paper explains, "*A mandatory label could take the form of an expiry date label, which would display the length of time that security updates will be provided for the smart device (as a proxy indicator for the device's overall level of security)*."[11] A label such as this raises a series of further questions as to what is expected happen once this date is passed. Will the vendor prevent the device having further access to the internet? Will it be the responsibility of the consumer to disconnect and dispose of the device?

A further assumption implicit in the expiry date label approach is that the device *can* be communicated with in order to be patched or updated. This may be fine for devices such as smart phones and broadband gateways that are constantly and directly connected to the Internet, such that they can be identified by a manufacturer and remotely upgraded. However, devices such as Wi-Fi access point, or smart home devices such as smart lightbulbs, smart TVs, security monitors and the like, sit behind gateway access points, may not be accessible remotely by the vendor to upgrade or patch a

[9] For example, the Energy Rating Label scheme used in Australia which measure energy or water consumed with scaling factors for the type of machine. See https://www.energyrating.gov.au/label

[10] A Google search will reveal numerous articles, but to pick just one, this news.com.au article identifies several drawbacks. https://www.news.com.au/lifestyle/health/diet/why-the-health-star-rating-system-is-flawed/news-story/1cbe4887a9ff832a4e03af496a580705

[11] The Paper, p.39.

vulnerability. These devices then rely on the user checking for updates and installing those updates, as it is unlikely the vendor would have the consumer's contact details[12] in order to alert them to a new update. If the user does not patch the device, it is vulnerable, but the example label on p.39 of the Paper shows, the device has "Cyber Protection until 2025".

Digital labels are mentioned in the Paper, but only in the context of understanding implementation costs. We recommend digital labels require greater consideration. A quick-response (QR) code that can be scanned with a mobile phone to be directed to a webpage providing up-to-date information on the security of that device would be a convenient way for security-minded consumers to check the status of their devices. We're not saying a QR code would magically make consumers update their devices, however, expanding on the previous point of devices that sit behind a gateway being inaccessible for remote patching, if consumers are security-minded, today they'd have to find the model number and search the internet, hoping to find information. A labelling scheme that incorporates a digital label with a QR code to a centralised website containing details of certified devices would be a quick and convenient mechanism for consumers to check the security status of devices they own.

Therefore, we consider option 1, some form of voluntary labelling scheme with an embedded digital label containing a QR code is the best approach for informing consumers and purchasers of smart devices, and for the reasons we have outlined, we strongly recommend careful consideration is given to what the label conveys, and how consumers are educated on its meaning. We fully endorse the IoTAA's proposal for a consumer-informed, voluntary, market driven, industry-led certification and labelling scheme, which will meet these objectives.

Finally, as the Paper observes, Singapore and Finland have implemented voluntary security labels for smart devices, the US President issued an Executive Order on 12 May 2021 calling for IoT labelling to be piloted (and *"… consider ways to incentivize manufacturers and developers to participate in these programs*")[13], and the UK has recently launched three different voluntary assurance schemes for smart products, meaning Australia is lagging international progress in this space. We implore the government to work with industry with a renewed urgency to launch a security labelling scheme for smart devices in Australia as soon as possible.

16 What is the best approach to encouraging consumers to purchase secure smart devices? Why?

Consumers and businesses are already aware of the financial and non-financial cost of cyber security incidents. While perhaps there is some fatigue creeping in because of the volume of events reported, we consider that consumers and businesses have the encouragement they need to purchase secure smart devices. The problem is accessible and relevant information on the level of security in the smart device, and competitive pricing for devices that incorporate better levels of security. A security certification and labelling scheme will address both of these problems, by providing the information consumers and businesses need, and providing market-driven competition to encourage developers and manufacturers to compete to install better security while remaining cost-competitive.

[12] If a consumer purchases a smart home device such as a connected lightbulb, it is unlikely that they will leave contact details such as an email address that can be passed on to the manufacturer in order for the manufacturer to alert the consumer of a patch or upgrade.

[13] Executive Order on Improving the Nation's Cybersecurity. 12 May, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/#:~:text=consider%20ways%20to%20incentivize%20manufacturers%20and%20developers%20to%20participate

17 Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?

A certification and labelling scheme will operate against standards to ensure benchmarking against international best practice and to ensure consistency in the certification of smart devices. In short, standards will underpin a certification and labelling scheme.

18 Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not? If so, which existing labelling scheme should Australia seek to follow?

We support the IoTAA's proposal for a consumer-informed, voluntary, market driven, industry-led certification and labelling scheme. As the Paper notes,[14] a voluntary scheme would need to be industry led, and we consider there is sufficient support for an industry-led scheme. That said, there is a role for government to assist with education and awareness of the scheme. Increasing community awareness of the scheme will ensure consumers and businesses will seek devices that are certified and labelled, creating the market incentives for manufacturers to become certified under the scheme.

19 Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?

As we noted at the start of this section on Chapter 7 of the Paper, we have considerable reservations about an expiry date label. Our concern is that many smart devices will sit behind a gateway modem or firewalled device that may restrict remote updates to patch the device if a flaw is identified, thereby relying on the owner/user to perform the upgrade to ensure the device is secure.

While this criticism can be levelled at other labelling schemes (including star-rating schemes), we consider a labelling scheme primarily intended to convey a date to which patches will be provided is more susceptible to creating a false sense of security than other labelling schemes.

We consider a credible solution to this challenge is a digital label such as a QR code, where security-minded consumers can check the status of devices and implement patches or updates if required. Of course, this is no guarantee that consumers will conduct updates in a timely manner, but it does lower the friction for those inclined to perform such updates.

20 Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?

We have some reservations about including 'higher-order' devices such as mobile phones, tablets, laptops and computers in a security labelling scheme for smart device. While these devices may be able to be certified by the original equipment manufacturer (OEM) at the point in time where the device was first sold, devices that are 'open platform' devices quickly evolve into an ecosystem of applications and services as user requirements evolve. It is not reasonable for the OEM's certification to extend to all future possible permutations of application or software installed on the device, or to the combinations of applications and services that may arise. In this context, we are concerned that a security label on a 'open platform' smart device may provide a false sense of security where users assume that because the original operating system and software was certified, the device will remain certified.

In addition, a possible unintended consequence of introducing a labelling scheme for these devices may be that the vendor restricts capabilities to a limited set of known applications at the time the device was developed, thereby potentially triggering early obsolescence with users wanting to add more recent applications.

[14] The Paper, p.41.

21 Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?

Yes, we consider quick-response codes (QR codes) to be a great idea. It enables the security status of smart devices to be maintained online in a centralised location associated with the certification and labelling scheme. Online information can include information on when the device was last compliance tested, current firmware version number, any reported vulnerabilities and available security updates. As we have noted, employing QR codes is not an automatic guarantee that consumers will conduct updates in a timely manner, but it does lower the friction for those inclined to perform such updates.

08 Responsible disclosure policies

Stronger communications and guidance to drive the uptake of responsible disclosure policies by more Australian businesses could contribute to addressing the stigma around companies publicly disclosing that they have a vulnerability or a cyber incident. This transparency supports greater cyber security through understanding of the threat environment and can disincentivise opportunistic attackers.

22 Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

We support the development and promotion of a toolkit aligned with the relevant industry standard (ISO/IEC 29147:2018), such as the excellent example available from the UK's National Cyber Security Centre, which provides guidance on what a policy should contain and how to help researchers who find a vulnerability to communicate with an organisation. A toolkit should be accompanied by targeted awareness and promotion of the toolkit to make it simple for vendors to adopt.

The problem a toolkit solves: when a security researcher identifies a vulnerability in a product or service, the easiest approach is for them to contact the vendor directly by a standard, streamlined mechanism to report it effectively and safely. The issue comes when the vendor in question does not have a responsible disclosure policy and therefore does not have an effective mechanism in place to receive and protect this information and does not know what to do with it once received.

We encourage the ACSC to formally recognise or adopt a toolkit, and then to dedicate resources to a program to proactively engage ASX200 organisations to raise awareness of the toolkit and run workshops and CISO briefings to help organisations build and test policies and process including defined fix/turnaround times and legal and communications protocols.

09 Health checks for small business

We are support the introduction of optional cyber security health checks for small business and a 'trust mark model', similar to the UK's 'Cyber Essentials' program.

If health checks were to become mandatory in certain situations, such as tendering for government contracts, consultation should take place with affected parties and sectors on the technical design of the trust mark, to ensure that it aligns with any existing and emerging security baseline regulations that may already exist for those businesses and sectors. Guidance should also be provided up front as to what size organisations these tendering requirements would apply.

23 Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?

International experience would indicate that, if implemented well (i.e. with good support for businesses and consistent, high quality certifying authorities), security behaviours and outcomes could improve. A baseline review of the UK Cyber Essentials program indicated that it had increased certified organisations' awareness of cyber risks, driven increased implementation of security controls, and boosted investor confidence in certified businesses.

24 Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

A health check program may stimulate small business growth (e.g. new providers of the accreditation), and the accreditation itself may assist small business access to supply chains/tenders.

25 Is there anything else we should consider in the design of a health check program?

Setting the cost of certification at an accessible level to incentivise uptake; providing free or lower-cost certification to not-for-profit organisations.

010 Clear legal remedies for consumers

The Paper's stated objective is to make Australia's digital economy more resilient to cyber security threats by incentivising Australian businesses to invest in cyber security. A specific focus is on low sophistication threats that could be prevented by basic cyber security measures and on businesses not already covered by sector specific legislation, such as most technology platforms and online services, many professional services and mining, manufacturing, hospitality, retail, wholesale and construction.

Chapter 10 of the consultation paper explores stronger legal recourse for individuals following a cyber incident, through both the ACL) and the Privacy Act. In the case of the ACL, there is a specific focus on digital products along with an acknowledgement that the general protections under the ACL and the consumer guarantees already apply to such products. We agree with this conclusion and note the ongoing reviews in relation to improved compliance with the ACL consumer guarantees (Treasury) and a direct right of action for privacy breaches under the Privacy Act (Attorney General's Department).

As noted in our submission to the Attorney General's Department review of the Privacy Act[15], we believe a well-resourced OAIC is a more effective way of pursuing the Privacy Act's objectives than a direct cause of action. The current OAIC complaints process gives complainants a better result in a more timely and cost effective manner than court action. It is also our view that targeted cyber security awareness and education programs and associated guidance materials, are the most effective way incentivise businesses to improve their cyber practices and protect personal information.

As noted above, the consultation paper contemplates recourse through the ACL for cyber incidents in relation to digital products, and identifies three challenges with this approach, including determining what went wrong. Here, the consultation paper notes aspects such as determining whether the good (i.e., the device or service) was fit-for-purpose or not in the context of appropriate security. As we noted in section 06 of our submission, context is vitally important, and there is no one-size-fits-all approach to cyber security. We consider an extension of product safety requirements of ACL to mandate that

[15] Telstra's submission is available via the Attorney General's Department website https://www.ag.gov.au/sites/default/files/2020-12/telstra-corporation-ltd-and-telstra-health-ltd.PDF

products must be "secure" or "safe" does not enable a prospective purchaser to know that the manufacturer or other supplier has taken account of and ensured compliance with any such new ACL requirement, or that the assessment is appropriate for the context in which the device is used.

26 What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?

Chapter 3 of the Paper notes that Australia's privacy, consumer and corporations laws were not originally intended to address cyber security. While we acknowledge this may be the case, it does not necessarily follow that there are gaps in the ACL as it applies to digital products and cyber security. The ACL is a principles-based, technology neutral regulatory framework that has proven itself to be sufficiently broad to address emerging challenges, such as cyber security.

27 Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?

In our view, the principles based ACL is sufficiently broad to address cyber security challenges. We think the most effective way to make Australia's digital economy more resilient to cyber security threats is to improve awareness and knowledge of cyber security issues. For example, where a labelling scheme for smart devices is introduced, there could also be specific ACL guidance developed in relation to the scheme and cyber security claims more generally to increase business and consumer awareness. This could be similar to the 'green marketing' guidance[16] issued by the ACCC in response to product environmental claims and the introduction of the energy and water efficiency labelling scheme.[17]

The Paper notes that Treasury is leading the development of a regulatory impact assessment of specific options to improve compliance with the ACL consumer guarantees and that consultation will commence in the coming months. We welcome the opportunity to participate in this consultation process at the appropriate time.

A well-resourced OAIC as a more effective way of continuing to pursue the Privacy Act's objectives than the introduction of a direction right of action. This is because the current OAIC complaints process gives complainants a better result in a more timely and cost effective manner than direct court action. It is also our view that targeted cyber security awareness and education programs, with associated guidance materials, is the most effective way to incentivise businesses that haven't already implemented minimum security standards to improve their cyber practices and better protect personal information.

A direct right of action will offer individuals another avenue via the Federal Courts to seek to enforce their rights, but that avenue is more likely to be drawn-out, costly, and less flexible than the current complaints process offered by the OAIC. In contrast, the OAIC is a specialist body that can finalise complaints relatively quickly and cheaply for consumers and facilitate a range of remedies.

Even if a small proportion of complaints are diverted away from the OAIC as a first port of call then that could result in a significant imposition on court resources, which is likely to be unjustified in light of the monetary awards under consideration – the OAIC's most recent annual report[18] shows that only a small

[16] Green Marketing and the Australian Consumer Law is available on the ACCC website at https://www.accc.gov.au/system/files/Green%20marketing%20and%20the%20ACL.pdf

[18] https://www.oaic.gov.au/assets/about-us/our-corporate-information/annual-reports/oaic-annual-reports/annual-report-2019-20/OAIC-Annual-Report-2019-20.pdf

proportion of privacy complaints result in compensation, and where compensation is paid in most cases it is less than $10,000.

APP 11 requires relevant entities to take 'reasonable steps' to protect the personal information they hold, whether online or physically. While good guidance already exists about these reasonable steps, we recommend updating the OAIC guidance to include what 'reasonable steps' means in the context of cyber security, existing ACSC resources and the nature of the relevant personal information.