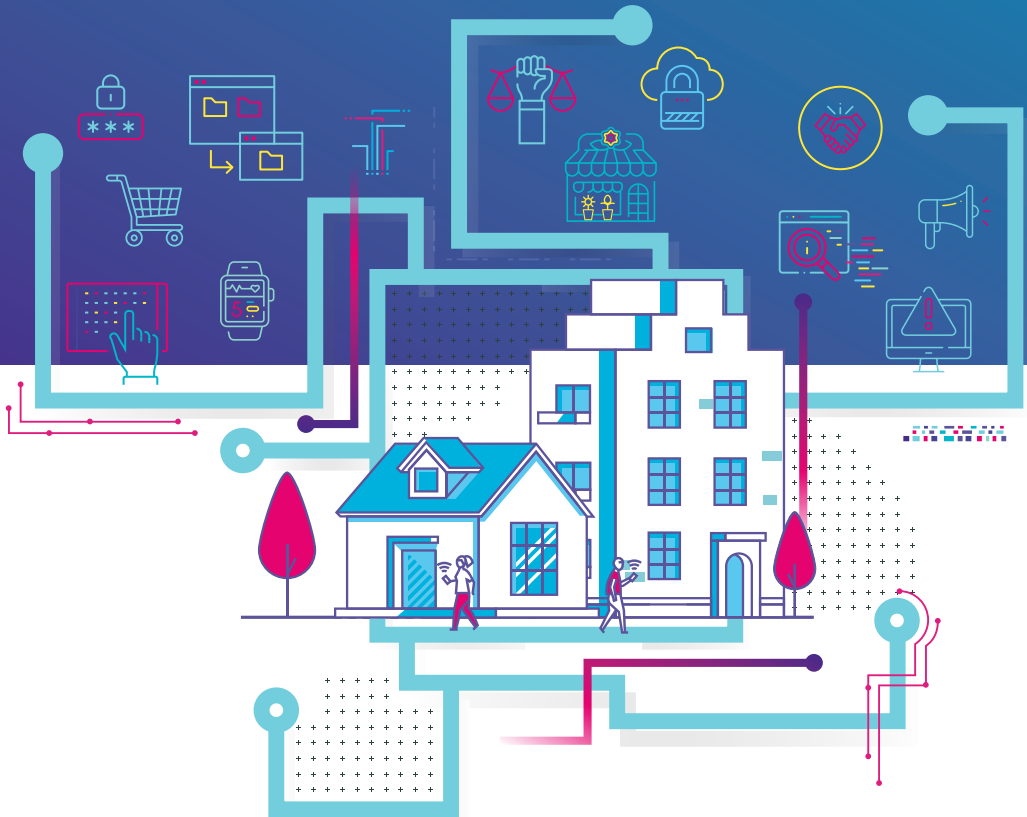




Australian Government

Strengthening Australia's cyber security regulations and incentives

An initiative of Australia's Cyber Security Strategy 2020



A call for views

© Commonwealth of Australia 2021

With the exception of the Commonwealth Coat of Arms, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license at <https://creativecommons.org/licenses/by/4.0/legalcode>.

This means this license only applies to material as set out in this document.



The details of the relevant license conditions are available on the Creative Commons website at <https://creativecommons.org/> as is the full legal code for the CC BY 4.0 license at <https://creativecommons.org/licenses/by/4.0/legalcode>.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed at the Department of Prime Minister and Cabinet website—<https://www.pmc.gov.au/government/commonwealth-coat-arms>.

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Cyber, Digital and Technology Policy Division
Department of Home Affairs
techpolicy@homeaffairs.gov.au

Strengthening Australia's Cyber Security
Regulations and Incentives



A call for views

Table of Contents

Quick overview	2
Executive summary	3
1. What problem are we trying to solve?	5
2. Why should government take action?	9
3. The current regulatory framework	12
Part 1 – Set clear minimum expectations	17
4. Governance standards for large businesses	18
5. Minimum standards for personal information	24
6. Standards for smart devices	29
Part 2 – Increase transparency and disclosure	35
7. Labelling for smart devices	36
8. Responsible disclosure policies	43
9. Health checks for small businesses	47
Part 3 – Protecting consumers	52
10. Clear legal remedies for consumers	53
Other issues	56
Next steps	57
Appendix A: List of discussion questions	58
Appendix B: Best practice principles for effective policy and regulation	60
Annex A: Understanding the cyber security of smart devices in Australia	61

Quick overview

Our goal

To make Australia's digital economy more resilient to cyber security threats

How will we get there?

Create stronger incentives for Australian businesses to invest in cyber security

Key areas of action

Set clear expectations

There should be clear minimum expectations for businesses to manage cyber security risks.

Increase transparency and disclosure

Businesses and households should have clear information about the security of technology products.

Protect consumer rights

Consumers should have clear legal remedies after a cyber security incident occurs.

Possible new policies

Governance standards for large businesses
(Chapter 4)

Minimum standards for personal information
(Chapter 5)

Standards for smart devices
(Chapter 6)

Labelling for smart devices
(Chapter 7)

Responsible disclosure policies
(Chapter 8)

Health checks for small businesses
(Chapter 9)

Clear legal remedies for consumers
(Chapter 10)



Executive summary

A growing digital economy offers significant opportunities for all Australians, whether through new jobs, new business ventures or better ways to connect with each other. The COVID-19 pandemic has accelerated our transition to a digital economy and demonstrated the importance of the internet for our prosperity. However, as we become more connected, there are growing opportunities for cyber criminals to target Australians. It's clear that government, businesses and the community need to take steps to protect Australia from cyber security, privacy and online safety threats.

This paper seeks your views about how the Australian Government can incentivise businesses to invest in cyber security, including through possible regulatory changes.

This work is an initiative of *Australia's Cyber Security Strategy 2020* (the Cyber Security Strategy) and progresses recommendations of the 2020 Cyber Security Strategy Industry Advisory Panel. It will build on the Government's security of critical infrastructure reforms¹ by uplifting the cyber security of all digitally enabled businesses, and will ultimately support the Government's goal of being a leading digital economy by 2030.

As outlined in the quick overview, we are proposing three areas of action – setting clear cyber security expectations; increasing transparency and disclosure; and protecting consumer rights. To set clear minimum expectations we are considering greater use of cyber security standards for corporate governance, personal information and smart devices. To increase transparency we are considering initiatives on cyber security labelling for smart devices, vulnerability disclosure and health checks for small businesses. In the area of consumer rights we are seeking your views about appropriate legal remedies for victims. We also welcome feedback on any other policies you would like us to explore.

Cyber security is a shared responsibility between governments, businesses and the community, and we are committed to working with you on the design of any new policy. We strongly encourage you to make a submission on any of the issues covered in this paper. We will consider all submissions and meet with a wide range of stakeholder groups to fully understand the best ways to grow a prosperous and secure digital economy, before advising Government on next steps.

¹ Further information is available from <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems>.

How we got here: The Government's cyber security initiatives

2016

The Australian Cyber Security Centre opened

2017

The Critical Infrastructure Centre is established

1st Annual Update of Australia's Cyber Security Strategy 2016

The Department of Home Affairs is established

Joint Cyber Security Centres partnership program

\$230m 2016 Cyber Security Strategy released

\$300–\$400m commitment to cyber security in 2016 Defence White Paper

2018

Notifiable Data Breach Scheme is established

Expansion of the Australian Signals Directorate's cyber security mandate to combat offshore cyber criminals

2019

2020 Cyber Security Strategy discussion paper released

Industry Advisory Panel for the Cyber Security Strategy led by Telstra CEO Andrew Penn appointed by the Minister for Home Affairs

Review of the *Privacy Act 1988* announced

The National Cyber Security Committee (Commonwealth States & Territories) is established

2020

The \$1.35b Cyber Enhanced Situational Awareness and Response (CESAR) package announced

The Industry Advisory Panel Report released

Cyber Security Strategy 2020 released

Industry Advisory Committee led by Telstra CEO Andrew Penn appointed by the Minister for Home Affairs

Review of the *Privacy Act 1988* issues paper released

Security Legislation Amendment (Critical Infrastructure) Bill 2020 introduced in Parliament

2021

Cyber Security Connect & Protect for SMEs opens

Cyber Security Skills Partnership Innovation Fund opens

Digital Economy Strategy released



1. What problem are we trying to solve?

Chapter summary

- Cyber security incidents are increasing in frequency, scale and sophistication, and are a threat to Australia's economic prosperity and national interests.
- Actors of all levels of sophistication are exploiting basic vulnerabilities in Australian networks and smart devices.
- By one estimate, the cost of cyber security incidents to the Australian economy is \$29 billion per year, or 1.9 per cent of GDP.

In brief, we are seeking to reduce the social and economic impacts of cyber security incidents to Australia's digital economy and society.

Cyber security incident

A single event or series of events that threatens the integrity, availability or confidentiality of digital information.

Advice from the Australian Cyber Security Centre (ACSC) is that cyber security threats targeting Australia's national and economic interests are increasing in frequency, scale and sophistication. This conclusion aligns with your feedback to the Cyber Security Strategy. Cyber security threats are now widely acknowledged to be a serious business risk and a handbrake on economic growth.

For example, in 2019 the World Economic Forum rated data fraud or theft and cyber-attacks as the fourth and fifth most likely business risks.² Further, the COVID-19 pandemic has accelerated the uptake of technology and exposure to cyber security risk.

² World Economic Forum 2019, *The Global Risks Report 2019*, available at <https://www.weforum.org/reports/the-global-risks-report-2019>.

Your feedback on the threat environment

During consultation on *Australia's Cyber Security Strategy 2020* you told us that the threat environment has evolved and is worsening. Ernst and Young told us cyber security breaches are a matter of 'when, not if'. Sapient Cyber noted the 'consequence of attacks are increasing in severity, as information systems become more central to business and society'.

Microsoft told us that 'cyberattacks from increasingly sophisticated actors threaten organisations across every sector'. The Commonwealth Bank of Australia observed that 'cyber threats are evolving into new forms as threat actors increase their capabilities and evolve their tactics, techniques and procedures'. At the same time many citizens and small businesses are still falling victim to simple tools and techniques like phishing.

Many stakeholders noted that as new internet-connected technologies come online – such as smart cities, automated vehicles and Internet of Things devices – networks will become harder to defend.

Our focus is on the social and economic impacts of widespread but lower sophistication threats, noting that Government is taking separate action to respond to sophisticated and persistent threats, including through updated critical infrastructure legislation.

Who is targeting us and how are they doing it?

Vulnerabilities in Australia's networks and smart devices are being exploited by actors of all levels of sophistication. Malicious actors target businesses and individuals who have not implemented basic cyber security measures (regardless of size of the business or the value of data held), and are constantly scanning network services to build a list of future potential vulnerabilities. The availability of simple, low-cost cybercrime tools on the dark web has made it easier to commit cyber-attacks. The most common categories of incidents currently reported to the ACSC are cyber-enabled fraud and identity crime.

According to the ACSC, in the 2019–20 financial year, ransomware posed the highest cyber security threat as it requires minimal technical expertise, is low cost and can result in significant impacts to a business.³ In the last year, we saw large corporations reportedly suffer from the impacts of ransomware including Toll Group (January and May 2020), logistics company Henning Harders (March 2020), Bluescope Steel (May 2020), budgeting service MyBudget (May 2020) and food and beverage company Lion (June 2020).

Phishing and spear phishing are the most common methods employed by cyber criminals to harvest personal information or user credentials to gain access to networks, or to distribute malware.⁴ Other threats include malicious insiders and supply chain compromises. Any element of a supply chain can be targeted, including people, software and hardware.

³ ASD, ACIC and AFP 2020, *ACSC Annual Cyber Threat Report, July 2019 to June 2020*, available at <https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf>.

⁴ Ibid.

How many Australians are impacted by cyber security incidents?

Estimating how many Australians are impacted by cyber security and cybercrime incidents each year with a high degree of confidence is difficult because official data is collected infrequently and reporting of incidents to authorities is voluntary.

- In 2016–17, official statistics showed that 9 per cent of home internet users had experienced damage or loss caused by a virus or other computer infection.⁵
- In 2015–16, official statistics showed that 16 per cent of businesses experienced a cyber security incident. Large businesses (27.5 per cent) were breached more frequently than small (18.7 per cent) and micro businesses (13.5 per cent).⁶
- In Australian Industry Group's 2019 CEO Survey of Business Prospects, 32 per cent of businesses reported they had experienced a cyber security incident in the preceding year.⁷
- In 2019–20, 59,806 cybercrime reports were made to the ACSC, or approximately one every 10 minutes.⁸
- In the second half of 2020, 58 per cent of data breaches reported to the Office of the Australian Information Commissioner (OAIC) were due to malicious or criminal attack – the leading cause of all notifications.⁹

The ACSC assesses that the frequency of cyber security incidents is growing over time (taking into account classified and unclassified sources of intelligence). In 2020, the ACSC received 65,617 cybercrime incidents in ReportCyber, a 33 per cent increase over 2017 figures (49,238 cybercrime reports). In 2020, the ACSC received 2,223 cyber security incident reports, an 86 per cent increase over 2017 figures.¹⁰ Between October 2019 and October 2020, demand for cyber security support services from IDCARE (a non-government organisation) also increased by 75 per cent, suggesting a growing threat environment that is often not reported to authorities.¹¹

Updated official statistics on the number of businesses being impacted by cyber security incidents will be published by the Australian Bureau of Statistics in July 2021, providing more insight into whether the overall threat to Australia's economy is growing. The ACSC plans to release the 2020–21 ACSC Annual Cyber Threat Report in September 2021, which will provide an overview of the key trends and threats in the cyber security environment for this reporting period.

5 ABS 2018, *Household use of information technology survey*, available at <https://www.abs.gov.au/statistics/industry/technology-and-innovation/household-use-information-technology/latest-release>.

6 Ibid.

7 Australian Industry Group Public Submission to the Cyber Security Strategy 2020, available at <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020>.

8 ASD, ACIC and AFP 2020, *ACSC Annual Cyber Threat Report, July 2019 to June 2020*, available at <https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf>.

9 OAIC 2021, *Notifiable Data Breaches Report*, available at <https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/2020-2/Notifiable-Data-Breaches-Report-July-Dec-2020.pdf>.

10 There were multiple agencies working within the ACSC prior to the ACSC becoming a statutory agency on 1 July 2018. The ACSC is unable to provide statistics around other organisations' incident data, and all incident statistics prior to 1 July 2018 relate to ASD's incident statistics only.

11 IDCARE 2021, *Submission to the Commonwealth Government's 2020 Privacy Act Review*, available at <https://www.ag.gov.au/sites/default/files/2020-12/idcare.PDF>.

What do cyber security incidents cost our economy?

Cyber security costs to society include ransom payments, lost revenue from business interruption, business recovery costs, lost shareholder value, reputational damage and costs to the taxpayer from any Government support and assistance. Beyond the direct economic costs, there are a range of social and psychological impacts that are difficult to quantify.

Private sector estimates of total societal costs are as high as \$29 billion per year (or 1.9 per cent of GDP)¹², but there can be wide variation in estimates due to limited data and generally small sample sizes. Self-reported financial losses to the ACSC as a result of cybercrime were \$316 million in 2019–20, but this only represents a very small part of the problem because not all incidents are reported, and victims don't always tell authorities the cost. Home Affairs has commissioned a consultant to provide advice on the best way to estimate the economic impact of cyber security incidents to Australia.

If no action is taken, the costs and consequences of cyber security incidents are likely to rise over time as more economic activity moves online and the number of connected devices grows. COVID-19 is just one factor driving this trend.

¹² Frost and Sullivan 2018, *Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World*, available at <https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats-to-cost-organizations-in-asia-pacific-us1-75-trillion-in-economic-losses/>.



2. Why should government take action?

Chapter summary

- Businesses don't always make the right investments in cyber security because of weak commercial incentives.
- There is evidence that businesses find it difficult to compete on the basis of cyber security and that cyber risks are often transferred to third parties like customers and suppliers.
- Government intervention could be effective in encouraging businesses to better manage cyber risk and promoting 'secure by design' principles.

We need to identify the core drivers of Australia's cyber security challenges so that we can understand what policies will have the greatest impact and the appropriate role for Government. We have conducted desktop research and reviewed feedback provided during development of the Cyber Security Strategy to understand why there isn't more widespread adoption of effective cyber risk management by businesses.

Two key market failures act against more widespread adoption of effective cyber risk management by business: negative externalities and information failures. Feedback during development of the Cyber Security Strategy indicated that these market failures are unlikely to be corrected without action by Government (see call out box).

Your feedback on Government's role in cyber security

A number of stakeholders we consulted for the Cyber Security Strategy told us that market forces alone haven't, won't or aren't able to uplift the cyber security of the economy at scale. Many parties told us that 'until there's regulation and consequences it's hard to drive change'.

Stakeholders told us that technology and threats are advancing faster than regulation and law reform. Many stakeholders asked us to implement a 'secure by design' principle in law or to ensure that basic controls like patching are implemented consistently. Businesses told us that without this action it is very difficult for an organisation to know if third-party suppliers are adequately controlling risks.

We heard consistent calls for some kind of baseline cyber security standards or regulations outside of those applying to critical infrastructure, either for digital goods and services in general or in specific areas like smart consumer devices.

Negative externalities

Negative externalities occur when a business makes a decision that creates a cost for someone else. This happens in cyber security when a decision by a business to underinvest in cyber security negatively impacts that business' customers and suppliers.¹³ When the impact of a cyber security incident is felt by someone else, it reduces the incentive to invest in cyber security.¹⁴ This was reflected in your previous feedback that there are weak incentives for many businesses to invest in cyber security.

A business also may not understand how its decisions on cyber security affect others, or it might think that an incident is too unlikely to prepare for.¹⁵ It is very difficult for a business to estimate the likelihood and consequence of a cyber incident and therefore the optimal level of cyber security investment.¹⁶ Ignoring cyber security advice and doing nothing is rational where the expected cost of investing in cyber security (including the cost of working out what to do) is greater than the likely loss to the business from a cyber incident.¹⁷ This was reflected in your previous feedback that company boards will sometimes deprioritise cyber security as a business risk.

Sometimes negative externalities result in cyber security risk being passed down the supply chain, from suppliers of technology to end users (both businesses and individuals). Unfortunately, end users almost always have less capability to manage cyber security risk compared to the technology companies that supplied the software or device.

To demonstrate this effect we reviewed the terms of use for 10 major software platforms. All terms of use disclaimed liability for cyber security incidents to the extent permitted by the law, with the exception of electronic payments platforms, where financial sector entities accept liability for unauthorised transactions as part of an industry code.

Finally, technology companies may prioritise their own reputation and commercial interests over the interests of their customers, further demonstrating how the costs of an incident can flow down from technology companies to end users.

13 Tyler Moore 2010, *The economics of cyber security: principles and policy options*, International Journal of Critical Infrastructure Protection, Volume 3, pp. 103-117, available at <https://www.sciencedirect.com/science/article/pii/S1874548210000429>.

14 UK Government 2020, *Cyber security incentives & regulation review: summary of responses to the call for evidence*, available at <https://www.gov.uk/government/publications/cyber-security-incentives-regulation-review-government-response-to-the-call-for-evidence/cyber-security-incentives-regulation-review-summary-of-responses-to-the-call-for-evidence#commercial-barriers-and-incentives-for-investing-in-effective-cyber-risk-management>.

15 Council of Economic Advisers 2018, *The Cost of Malicious Cyber Activity to the U.S. Economy*, available at <https://www.hsdl.org/?view&did=808776>.

16 UK Government 2020, *Cyber security incentives & regulation review: summary of responses to the call for evidence*, available at <https://www.gov.uk/government/publications/cyber-security-incentives-regulation-review-government-response-to-the-call-for-evidence/cyber-security-incentives-regulation-review-summary-of-responses-to-the-call-for-evidence#commercial-barriers-and-incentives-for-investing-in-effective-cyber-risk-management>.

17 Cormac Herley 2009, *So long, and no thanks for the externalities: The rational rejection of security advice by users*, available at <https://doi.org/10.1145/1719030.1719050>.

Information asymmetries

An information asymmetry occurs when the sellers of technology products have more information about cyber security than buyers. 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.¹⁸ Even with technical capability, it is costly and time-consuming for buyers to independently verify the security of products. Consistent feedback from the Cyber Security Strategy was that small businesses struggle to find time to understand and address cyber security risks.

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'. During consultation on the Cyber Security Strategy we spoke to a number of stakeholders that experienced difficulty in negotiating stronger cyber security protections with global technology suppliers.

For consumer products, buyers often incorrectly assume that security is built in, which leaves them vulnerable to cyber incidents. A survey of Australian consumers by Data61 showed that around half (46 per cent) incorrectly assumed that cyber security is already built in to all smart devices sold in Australia.¹⁹

Information asymmetries ultimately mean there are few incentives for sellers to offer secure products, as customers cannot distinguish between high and low security offerings. This erodes incentives to build security in by design.²⁰ Home Affairs has previously received industry feedback that it is difficult to compete on security grounds.

Other issues

Some stakeholders point to cost, complexity and the difficulty in building a skilled workforce as key drivers of the cyber security problem.²¹ We recognise that these factors are real challenges in cyber security. Australia's Cyber Security Strategy 2020 contains a range of initiatives to build Australia's cyber security workforce and educate businesses and individuals about cyber security risk. Addressing information asymmetries and negative externalities may also assist in addressing these problems by strengthening commercial incentives to invest in cyber security workers and education.

We also recognise that holistic cyber security solutions are never cheap nor easy. We are not suggesting that businesses should invest in cyber security no matter the cost. The goal of the policies outlined in this paper is to ensure that investments are made where the benefits for our society outweigh the costs, and that any market failures are addressed, leaving the market free to do its job.

Seeking your views

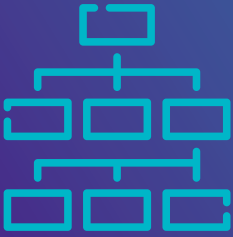
- 1 What are the factors preventing the adoption of cyber security best practice in Australia?
- 2 Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?

18 Tyler Moore 2010, *The economics of cyber security: principles and policy options*, International Journal of Critical Infrastructure Protection, Volume 3, pp. 103-117, available at <https://www.sciencedirect.com/science/article/pii/S1874548210000429>.

19 Data61 2020, *Results of the IoT Consumer Focused Survey*. Unpublished report produced for the Cyber Security Cooperative Research Centre.

20 Ross Anderson and Tyler Moore 2007, *Information Security Economics – and Beyond*, Advances in Cryptology–CRYPTO 2007: 27th Annual International Cryptology Conference, available at https://doi.org/10.1007/978-3-540-74143-5_5.

21 Cyber Security Strategy 2020 Feedback; UK Government 2020, *Cyber security incentives & regulation review: summary of responses to the call for evidence*, available at <https://www.gov.uk/government/publications/cyber-security-incentives-regulation-review-government-response-to-the-call-for-evidence/cyber-security-incentives-regulation-review-summary-of-responses-to-the-call-for-evidence#commercial-barriers-and-incentives-for-investing-in-effective-cyber-risk-management>.



3. The current regulatory framework

Chapter summary

- The most relevant Australian laws related to cyber security that apply broadly across the economy are the *Privacy Act 1988*, Australian Consumer Law and *Corporations Act 2001*.
- Critical infrastructure operators and businesses in safety-critical industries usually have additional cyber security obligations.
- There is opportunity to create a stronger digital economy through clear, consistent and enforceable cyber security rules.

This chapter explains Australia's current regulatory environment for cyber security, to assist you to provide feedback about where changes might be beneficial. We undertook a scan of Commonwealth, state and territory legislation and court cases to identify the obligations that businesses currently have to protect themselves or their customers from cyber security threats. This non-comprehensive scan did not include criminal offences or laws in adjacent areas like online safety.

We identified at least 51 Commonwealth, state and territory laws that create, or could create, some form of cyber security obligation for businesses. In most cases, the application of these laws to cyber security is theoretical

and unlikely to occur in practice. However, it does illustrate the complicated regulatory environment for cyber security. Our analysis found that these laws are either sector-specific or cross-sectoral. Sector-specific legislation applies only to certain industries while cross-sectoral legislation applies across multiple industries.

We recognise that regulation is only one reason why businesses may choose to invest in cyber security. While we are interested in all types of incentives that contribute to strengthening cyber security, we see the regulatory framework as an important basis for understanding cyber security in Australia.

Sector-specific legislation

A number of industries are subject to security or safety standards unique to their sector of the economy. We estimate that approximately one third of ASX 200 companies are covered by this kind of regulation.²² This includes businesses in 11 critical infrastructure sectors who will be covered under the Positive Security Obligation

included in reforms to the *Security of Critical Infrastructure Act 2018* (SOCI Act) introduced to Parliament on 10 December 2020. Home Affairs is currently working with industry peak bodies, existing regulators, state and territory governments, and critical infrastructure entities to co-design sector-specific Rules to underpin the Positive Security Obligation, which could include cyber security standards.²³

Case study: Cyber security obligations in the financial sector

An example of a mature regulatory regime for cyber security is in the finance sector. Banks, insurers and superannuation funds (regulated by the Australia Prudential Regulation Authority – APRA) and clearing and settlement facilities (regulated for financial stability risks by the Reserve Bank of Australia – RBA) are subject to standards that deal specifically with operational risks, including cyber security. These standards apply to over 680 entities and are supported by close supervision of entities' adherence with the standards.

Regulation of other licensed financial services and credit providers by the Australian Securities and Investments Commission (ASIC), numbering around 11,000, relies on general licensee obligations in s912A of the *Corporations Act 2001* to manage cyber risk.²⁴ Market infrastructure providers, such as exchanges, are also subject to similar obligations under the *Corporations Act 2001*. Certain APRA-regulated firms are subject to carve-outs from these obligations.

APRA's *Prudential Standard CPS 234 Information Security*, which took effect in July 2019, is a flexible, risk-based standard that requires a regulated entity to take proportionate steps to manage information security risk. During consultation for *Australia's Cyber Security Strategy 2020*, some stakeholders told us that this standard provided a useful and appropriate framework for management of cyber security risks that other businesses could consider adopting.

Case study: ASIC v RI Advice

ASIC has commenced proceedings in the Federal Court against an Australian financial services licence (AFSL) holder, RI Advice, alleging failure to implement and maintain adequate cyber security and cyber resilience measures in contravention of its obligations under s912A of the *Corporations Act 2001*.

This is the first time that litigation has been initiated by ASIC alleging deficient cybersecurity practices and the outcome will provide judicial guidance about the cyber security standards required of Australian financial services licence holders in a similar position to that of RI Advice.

²² Current as at 16 February 2021.

²³ Further information on the reforms is available at <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems>.

²⁴ Specifically, s912A of the *Corporations Act 2001* requires licensees to have adequate risk management systems and have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the licence and to carry out supervisory arrangements.

Cross-sectoral legislation

Our focus is on all the other businesses that are not covered under sector-specific legislation.

By numbers alone, the vast majority of businesses in Australia would fall into this category, including around two thirds of ASX 200 companies. This includes most technology platforms and online services, most professional

services, mining, manufacturing, hospitality, retail, wholesale and construction. It is important that these parts of our economy invest in strong cyber security, in addition to critical infrastructure entities.

The most relevant laws that apply broadly across the economy are the *Privacy Act 1988*, Australian Consumer Law and *Corporations Act 2001*. The table below details how these laws apply to cyber security.

Law	Application to cyber security
<i>Privacy Act 1988</i> (Privacy Act)	<ul style="list-style-type: none"> Under Australian Privacy Principle 11, entities covered by the Privacy Act are required to take 'reasonable steps' to protect personal information from misuse, interference and loss and from unauthorised access, modification or disclosure. Under the Notifiable Data Breaches scheme, entities covered by the Privacy Act are also required to report eligible data breaches, including those which occur due to cyber security incidents, to the Office of the Australian Information Commissioner (OAIC) and affected individuals.
Australian Consumer Law	<ul style="list-style-type: none"> Suppliers are prohibited from engaging in misleading or deceptive conduct or making a false or misleading representation that goods or services are of a particular standard. This may include a false representation of security standards or specific security measures. Suppliers are required to meet certain guarantees in supplying goods and services to consumers. These include that goods (including digital goods) are of acceptable quality and fit for purpose, and that services (including digital services) provided with due care and skill, and be fit for purpose. The relevant Minister may make information standards and impose product safety obligations through safety standards, bans or compulsory recalls.
<i>Corporations Act 2001</i>	<ul style="list-style-type: none"> Company directors and officers have a duty to act in good faith in the best interests of the company and for proper purpose. This involves considering the interests of shareholders, creditors and other stakeholders. Company directors and officers are also required to act with the degree of due care and diligence that would be applied to a person in the director or officer's circumstances.

What's happening internationally?

Internationally, it is common for cyber security risks to be captured through privacy and critical infrastructure legislation. For example, the European Union has implemented the General Data Protection Regulation (GDPR), an EU-wide law on data protection and privacy, and the Directive on Security of Network and Information Systems (NIS Directive), an EU-wide directive designed to protect essential services and digital service providers. A 2020 review of the impact of the GDPR in the United Kingdom (UK) found that eighty-two per cent of organisations reported improvements to their cyber security as a result of the introduction of the GDPR, at least to some extent.²⁵

In contrast, the United States (US) does not have a centralised federal approach to cyber security. Rather, cyber security responsibilities are split across concurrent state and federal regulations. The Federal Trade Commission has taken action against businesses with unreasonable cyber security or who have made deceptive security claims.^{26,27} Some states have taken action to implement specific cyber security legislation, such as California and Oregon who have introduced laws that set baseline security requirements for smart devices.

Limitations

Australia's privacy, consumer and corporations laws were not originally intended to address cyber security. This has led to the current framework having a number of limitations in effectively addressing cyber security threats.

Limitation	Explanation
Clarity	Current laws do not provide sufficient clarity about cyber security expectations. For example, the broad scope and principles-based nature of obligations like director's duties under the <i>Corporations Act 2001</i> , consumer guarantees under the Australian Consumer Law and security requirements under APP11 in the Privacy Act mean these mechanisms are limited in incentivising the uptake of uniform cyber security standards.
Coverage	Cross-sectoral cyber security laws have limited coverage. For example, director's duties focus on protecting the interests of shareholders, rather than customers, who are likely to bear some of the costs of a cyber security incident. The consumer guarantees under the Australian Consumer Law do not apply, in general, to business-to-business transactions over a certain monetary threshold. The Privacy Act does not apply to businesses with a revenue less than \$3 million.

25 RSM 2020, *Impact of the GDPR on Cyber Security Outcomes*, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/906691/Impact_of_GDPR_on_cyber_security_outcomes.pdf.

26 Federal Trade Commission 2016, *ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy at Risk*, available at <https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put>.

27 Federal Trade Commission 2020, *FTC Requires Zoom to Enhance its Security Practices as Part of Settlement*, available at <https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement>.

Limitation	Explanation
Enforcement	<p>There are limited examples of enforcement of these laws in a cyber security context. For example, consumer guarantees under the Australian Consumer Law can be enforced only through private action, which potentially requires time, money and expert knowledge. The prohibition on misleading and deceptive conduct can be enforced by the Australian Competition and Consumer Commission (ACCC) and state and territory regulators but will generally not apply if no representation is made about cyber security.</p> <p>The OAIC does have a range of enforcement powers under the Privacy Act, but your previous feedback told us too much focus has been put on conciliation over strong penalties. Specifically, while the Privacy Act confers a range of regulatory powers on the Commissioner, these powers are based on an escalation model, including a requirement for the OAIC to attempt to conciliate a complaint if there is a reasonable possibility that this conciliation would be successful. Civil penalties are only available under the Privacy Act where there have been serious or repeated interferences with privacy by an entity. A Review of the Privacy Act is considering this issue.</p>

So what?

Despite current limitations, there is opportunity to use Australia’s legal framework to support the Government’s goal of being a leading digital economy by 2030. We know that when we get the policy settings right investment confidence and economic activity increase. The risk of poor regulatory settings is that regulatory burden makes it difficult for businesses to operate in Australia, which costs our economy.

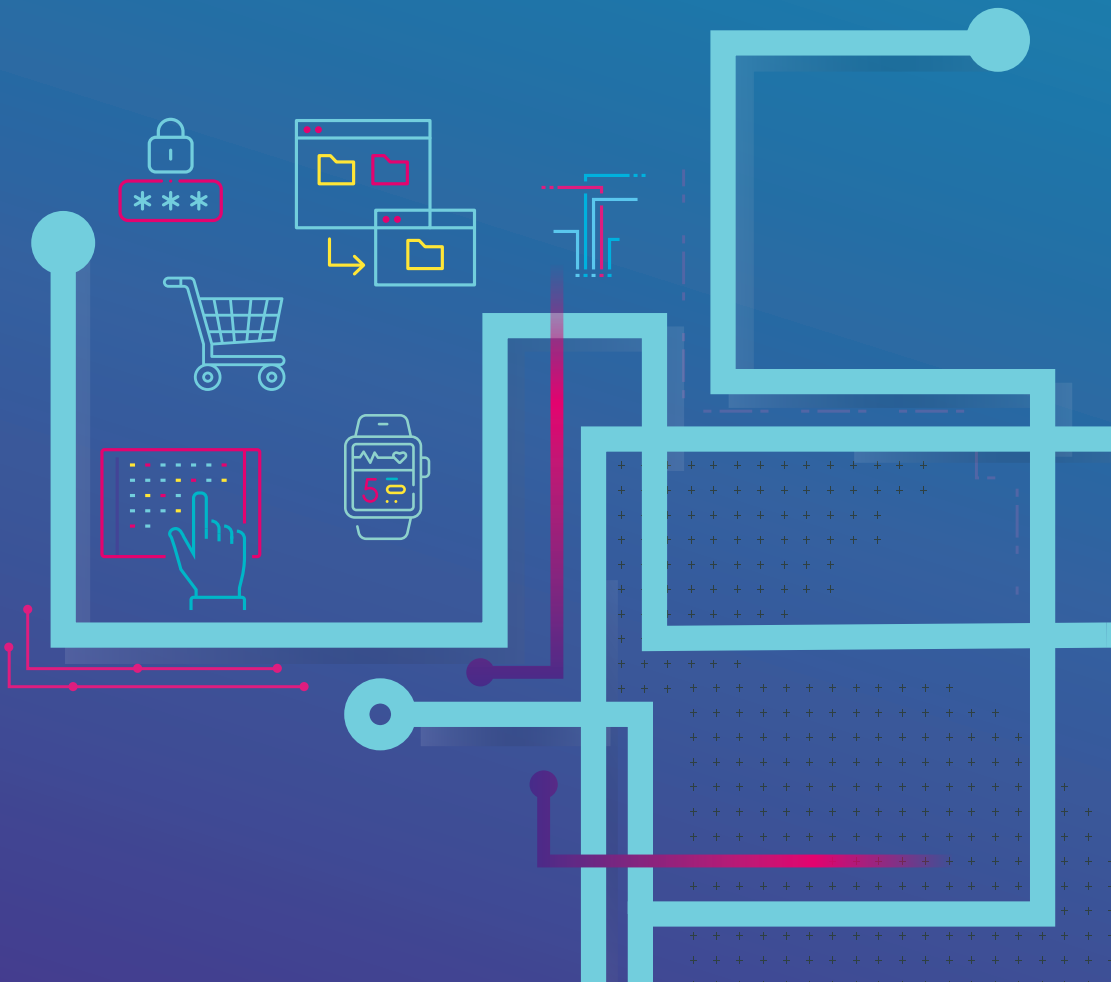
This paper provides specific suggestions about how to avoid unnecessary regulatory burden and realise the economic benefits of strong cyber security. We welcome your views about how to get the balance right, and how we can make things simple for all businesses in Australia.

Seeking your views

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

Part 1 – Set clear minimum expectations

Clear minimum expectations for businesses to manage cyber security risks





4. Governance standards for large businesses

Consistent feedback to Government has been that large businesses need to improve their management of cyber security risk. For companies, there is wide variation in the level of cyber security knowledge, including at the board level. In 2017, only 7 per cent of directors in ASX 100 companies said they clearly understood the cyber security environment

their company operates in.²⁸ Almost two-thirds said their understanding of the biggest IT security exposures was limited or nonexistent. In 2018, 40 per cent of medium and large sized Australian businesses did not have any cyber security governance or adopt any cyber security frameworks.²⁹

Within a company cyber security is everyone's job. The board must do their part in ensuring the cyber risk is managed just as it does with all other key corporate risks.

Robyn Denholm

Board Chair, Tesla and member of the 2020 Cyber Security Strategy Industry Advisory Panel

While cyber security remains the responsibility of the IT department in organisations and has a low risk profile it will not attract the funding and resources needed.

Governance Institute of Australia

Public submission to *Australia's Cyber Security Strategy 2020*

28 ASIC 2017, *ASX 100 Cyber Security Health Check Report*, available at [ASX-100-Cyber-Health-Check-Report.pdf](#).

29 Security-in-depth 2018, *State of Cyber Security In Australia 2018*, available at <https://securityindepth.com.au/>.

...there is still a significant cohort of Board members who remain uncertain of what information and technology governance really is, or why it is needed.

ISACA

Public submission to Australia's Cyber Security Strategy 2020

Although the cyber skills and awareness of directors on the boards of Australia's listed companies has increased in recent years, there is opportunity for further support and development.

2020 Cyber Security Strategy Industry Advisory Panel Final Report

We consider cyber security governance to primarily concern larger businesses, noting that smaller businesses are much less likely to have risk management processes in place or employ dedicated cyber security teams. Incidents affecting larger businesses are also more likely to have significant implications for national economic development, resilience and security.

Action so far

Significant gains in improving the cyber security capabilities of businesses have been made since the release of Australia's 2016 Cyber Security Strategy. Sustained efforts have been made to strengthen engagement between senior members of the intelligence community and senior business leaders. There is a wide range of guidance for business leaders available from industry and government sources, including best practice guidance from ASIC.³⁰ The Australian Institute of Company Directors offers formal training for company directors on cyber security risk management.

There has also been an increase in formal regulatory obligations for large businesses in higher risk settings. The Security Legislation Amendment (Critical Infrastructure) Bill 2020 introduces mandatory cyber security incident reporting and Enhanced Cyber Security Obligations for those assets deemed 'systems

of national significance' (those most critical to the nation). The Bill will also require boards that are responsible for regulated critical infrastructure assets to sign off on risk management programs as part of their Positive Security Obligations. The Australian Prudential Regulation Authority's prudential standard CPS 234: Information Security, which came into force in 2019, sets out requirements for banks, insurers and superannuation funds to take certain measures to be resilient to information security incidents.

Outside of critical infrastructure, all company directors have an obligation to act in good faith in the best interests of the company and for a proper purpose (alongside their other duties discussed in Chapter 3). It is widely accepted that cyber security risks are an increasingly important set of risks that most large businesses, including those established in the corporate form, need to oversee and manage. However, there is no explicit requirement that cyber security forms part of many existing obligations including those applicable to directors.

30 ASIC 2020, *Cyber resilience*, available at <https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/>.

Further action

To further protect the economy from cyber security threats, it is desirable to further improve cyber security risk management practices in large businesses. There is room for cyber security governance standards to be articulated in respect of a wider range of businesses than the critical infrastructure owners and financial institutions covered by the *Security of Critical Infrastructure Act 2018* and APRA's prudential standard respectively. Such a standard would need to apply across the various forms business structures can take including companies, partnerships, trusts, and sole traders, recognising that the corporate structure is the most dominant form.

We are seeking your feedback about the best way to encourage stronger cyber security risk management within large businesses. This could include setting voluntary or mandatory standards for large businesses, further education and capability raising, or both. Any action we take in this area would seek to be proportionate, achievable, and internationally consistent (see our best practice principles at [Appendix B](#)).

Option 0 – Status quo

Large businesses will continue to manage cyber security risk as they see fit. While some businesses will continue to have regulated risk management obligations, the majority of large businesses will have broad discretion about the level of cyber security risk they accept. It is likely this will create significant variance about how cyber risk is managed, depending on the engagement of the senior management and their perspective of cyber security risk to the business.

Senior management awareness may grow as incidents continue to be reported in the media and existing education efforts continue. The outcome of current and future court cases may influence behaviour, such as ASIC proceedings against RI Advice Pty Ltd (see [Chapter 3](#)).

For companies, it is possible that judicial expectations of what a reasonable director

might do to oversee the management of cyber security risk might rise without intervention from Government, as awareness of cyber security threats rises over time.

As this option does not impose new obligations, there will be no additional cost to business.

Option 1 – Voluntary governance standards for larger businesses

This option proposes the development of a voluntary cyber security governance standard for larger businesses. A governance standard would describe the responsibilities of large businesses and processes for managing cyber security risk, supporting the role of company boards overseeing cyber security risk, but would not require specific technical controls to be implemented. This would complement existing regulatory requirements.

Government could work with industry to co-design the requirements of a voluntary governance standard. A co-design process is more likely to result in a standard that is realistic and has industry buy-in. It would also ensure that Australia aligns with internationally developed standards.

As part of this co-design process, consideration would be given as to the best vehicle for communicating the voluntary standard to industry. We could seek to learn from the experience of other industry-led standards, such as the ASX Corporate Governance Council's Corporate Governance Principles and Recommendations.

Benefits

Improved governance of cyber security risk has strong potential to lead to better cyber security outcomes for Australian businesses and the community. The advantage of a voluntary governance standard is that it would communicate to industry that government and public expectations regarding the management of cyber security risks are

increasing, without creating unnecessary regulatory burden.

A voluntary standard would strengthen and complement existing director's duties under the Corporations Act, because a voluntary standard could be considered by a court when determining whether failures relating to the oversight of cyber risk constituted a breach of directors' duties.

This policy would also complement other obligations for large businesses. For example, compliance with a voluntary governance standard may constitute a 'reasonable step' under the Privacy Act for protecting personal information.

Large businesses would retain flexibility about how to manage cyber security risk. This would be particularly beneficial for businesses who operate across multiple sectors with varying sector-specific requirements. We recognise that there are many reasons why a business may choose not to adopt a voluntary standard, including if they are already subject to sector-specific regulations. Small businesses would not be directly impacted, but could adopt the voluntary standards if they considered them beneficial.

The co-design of a voluntary standard enables industry buy-in, and also gives industry time to understand the shifting expectations around cyber security governance and improve its capability in the most cost effective way. It may also ensure that potential duplication with other regulatory frameworks can be considered and mitigated.

Costs

As a voluntary measure, the regulatory burden of this option would be zero. Voluntary costs to industry would vary on the situation of the business and its existing maturity. Investment in governance is lower cost, but could lead to more substantial investments in cyber security. Implementing a voluntary standard would remain a business decision and we would only expect businesses to implement this approach

if they assess the benefits to outweigh the costs.

Minor costs may be borne by Government in coordinating with industry and industry bodies to develop the voluntary standards, and any associated awareness campaign and education resources.

Implementation issues and risks

The main drawback is that industry may not substantially adopt the standards and could continue to manage cyber risk as it currently does. This risk would be mitigated by the co-design process, as industry would be engaged to help develop standards that are reasonable and meaningful, and be made increasingly aware of shifting government and public expectations on cyber security governance. Care needs to be taken to ensure that a voluntary standard does not promote a 'tick-a-box compliance culture', where businesses rely too heavily on standards and do not critically assess their security requirements.

Not all businesses will have the organisational capability to adopt the standard initially. This option could be supported by enhanced cyber security education to build organisational capabilities. We are seeking your feedback about whether this is necessary and how it might work in practice.

Consistent with the best practice principles (see [Appendix B](#)), Government could consider additional steps if the uptake of the voluntary approach is low.

Option 2 – Mandatory governance standards for larger businesses

This option would involve a standard similar to Option 1, however, large businesses would be required to achieve compliance within a specific timeframe. Entities covered by existing regulation, such as responsible entities for critical infrastructure, would not be covered by this policy.

Benefits

Compared to Option 1, more large businesses would achieve improvements to their cyber security governance in a timely manner, which would result in improved management of cyber security risk. This would flow through to the broader economy, including consumers and smaller businesses, who would benefit from reduced costs of cyber security incidents.

Costs

Costs associated with mandating governance standards would be high, as a large number of businesses would be required to comply. Considering the variance in current cyber security governance, companies would be impacted differently depending on current maturity. Government would have to allow a significant amount of time for businesses to shift their governance structures and ensure they were able to comply with the mandatory standards. This would likely also include awareness and education costs borne by government and industry. Regulatory costs may be passed onto consumers.

Careful consideration would need to be given to interactions with existing cyber risk management standards that apply to parts of the economy, such as APRA's prudential standards and the expansion of the *Security of Critical Infrastructure Act 2018*. Mandatory standards could also interact poorly with other jurisdictions' regulation of cyber security, with the potential for multinational corporations to be less likely to invest in providing goods and services in the Australian market.

We also note that a mandatory standard would have a cumulative impact on the level of regulatory burden faced by Australian businesses.

Currently, there is no regulator with the relevant skills, expertise and resources to develop and administer a mandatory standard that applies to all large businesses. Any process to assign these responsibilities to a current regulator, would take significant time and cost, which would ultimately be borne by industry and the Australian public.

On balance, a mandatory standard may be too costly and onerous given the current state of cyber security governance, and in the midst of an economic recovery, compared to the benefits it would provide.

Summary of policy options

Option	Benefits	Costs	Net Impact
Option 0 – Status quo	Nil.	Nil.	– Ongoing cyber security incidents due to inconsistent management of risk by large businesses.
	Zero	Zero	Status quo
Option 1 – Voluntary governance standard	<ul style="list-style-type: none"> – Stronger management of cyber security risks by larger businesses. – Voluntary approach provides flexibility. 	<ul style="list-style-type: none"> – Co-design costs including industry engagement. – Awareness and educational costs. – Voluntary costs to industry to invest in cyber security. 	– Seeking your feedback. Benefits may outweigh the costs.
	Medium	Low	Positive
Option 2 – Mandatory governance standard	<ul style="list-style-type: none"> – Stronger, enforced management of cyber security risk by industry. 	<ul style="list-style-type: none"> – Increased compliance costs for a large number of businesses and government. 	– Seeking your feedback. Costs may outweigh the benefits
	Medium-High	High	Negative

Seeking your feedback

- 5** What is the best approach to strengthening corporate governance of cyber security risk? Why?
- 6** What cyber security support, if any, should be provided to directors of small and medium companies?
- 7** Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?



5. Minimum standards for personal information

Earlier in this discussion paper (Chapter 1), we identified that Australians continue to fall victim to known cyber security threats, enabled by a lack of baseline cyber security precautions. If these conditions remain, cyber criminals will continue to use simple, low-cost offensive tools available on the dark web to conduct cyber-attacks, without needing a high level of technical expertise.

During previous industry engagement, you told us that established and cost effective technical controls could mitigate a significant proportion of unsophisticated cyber-attacks. Your advice was to prioritise adoption of controls such as encryption of data in transit and at rest, strong passwords, multi-factor authentication and timely application of critical patches.

Our desktop research supports this advice. A Lancaster University study found that five elementary technical controls mitigated 99% of unsophisticated cyber-attacks.³¹ Analysis by Microsoft and Google shows that around 99% of automated attacks can

be successfully blocked by multi-factor authentication.^{32,33} Increasingly, organisations around the world are focusing on these kinds of cyber security controls. For example, Google announced in May 2021 that it is moving towards multifactor authentication by default for all users.³⁴ The US Government announced in May 2021 that all Federal Government agencies will implement multifactor authentication and encrypt data in transit and at rest.³⁵

Many organisations and platforms are already applying these kind of security best practices, but there are still many who don't. In a 2018 US survey, only 53 per cent of organisations with IT teams had a formal patch management process, which reflects that patching can be expensive and require expert knowledge.³⁶ The average time to patch was 102 days, which provides time for malicious actors to exploit the vulnerability and indicates there is room for most organisations to improve their patching maturity. A 2019 analysis of 47,000 organisations found that 57% had adopted multi-factor

31 The technical controls were firewalls and gateways, secure configuration, access control, malware protection and patch management. Vidler, J Seabrook T, Rashid A 2015, *Cyber Security Controls Effectiveness: A Qualitative Assessment of Cyber Essentials*, available at [http://www.research.lancs.ac.uk/portal/en/publications/cyber-security-controls-effectiveness\(a09a2d28-d121-41dc-86d6-cc24595d8968\)/export.html](http://www.research.lancs.ac.uk/portal/en/publications/cyber-security-controls-effectiveness(a09a2d28-d121-41dc-86d6-cc24595d8968)/export.html).

32 Microsoft 2018, *Password-less protection White Paper*, available at <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2KEup>.

33 Google 2019, *New research: How effective is basic account hygiene at preventing hacking*, available at <https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html>.

34 Wired 2021, *Google Gets Serious About Two-Factor Authentication. Good!* available at <https://www.wired.com/story/google-two-factor-a-authentication-default/>.

35 President Biden 2021, *Executive Order on Improving the Nation's Cybersecurity*, available at <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>.

36 Ponemon Institute 2018, *State of Endpoint Security Risk*, available at <https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf>.

authentication, up 12 percentage points from 2018.³⁷

One way to encourage the uptake of these cyber security best practices is through technical standards, which has been a consistent theme of stakeholder feedback, including the Cyber Security Strategy Industry Advisory Panel (see below). There is evidence that Australia has been slow to adopt cyber security standards.³⁸ Common barriers to standards adoption include uncertainty about which standards to adopt, low commercial and regulatory incentives for adoption, and

costs (particularly for technical changes and third party audits). Another barrier is that if standards are overly prescriptive they can have the unintended consequence of driving 'tick-a-box compliance culture'. This may result in organisations becoming complacent and not critically assessing their cyber security requirements.

We are seeking your feedback on whether cyber security resilience could be raised across the economy by accelerating the adoption of technical standards, and how this would work in practice.

"A first priority is to work with industry to accelerate the adoption of cyber security standards in Australia. Noting that standards are only valuable if adopted widely, Government should use its convening power to build industry consensus around what standards should be used in Australia".³⁹

2020 Cyber Security Strategy Industry Advisory Panel

Option 0 – Status quo

If no action was taken to improve the update of cyber security standards, Australia would continue to bear the economic and social costs of preventable cyber security incidents.

Option 1 – Cyber security code for personal information

Creating an enforceable code under a federal piece of legislation is one option to increase the adoption of cyber security standards across the economy by providing a strong regulatory incentive and directly addressing some of the common barriers identified above. However, there is no single existing act that governs cyber security expectations across the whole economy. Of current Commonwealth laws, the Privacy Act has the greatest potential

to set broad cyber security standards (albeit only in relation to personal information). Establishing a code under the Privacy Act could drive the adoption of cyber security standards across the economy by creating regulatory incentives for uptake.

As explained in Chapter 3, the Privacy Act contains a requirement at APP 11 for entities covered by the Privacy Act to take reasonable steps to protect personal information. It is expected that entities will actively monitor the cyber risk environment for emerging threats and take reasonable steps to protect personal information by mitigating those risks, in order to comply with APP 11. This responsibility scales proportionately to the volume and type of personal information held by an entity.

³⁷ LastPass 2019, *The Third Annual Global Password Security Report*, available at <https://www.lastpass.com/state-of-the-password/global-password-security-report-2019>.

³⁸ International Standards Organisation 2019, *The ISO Survey 2019*, available at <https://www.iso.org/the-iso-survey.html>

³⁹ Industry Advisory Panel 2020, *Industry Advisory Panel Report 2020*, available at <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2020-cyber-security-strategy-iap-report.pdf>.

Privacy Act Code

An Australian Privacy Principles (APP) code is a mechanism that can be used to enhance the requirements of an existing APP by setting out how it is to be applied or complied with, therefore enabling entities to better meet their obligations under the Privacy Act. An APP code can be developed by entities (industry) of their own initiative, or at the request of the Information Commissioner and includes a broad public consultation process.⁴⁰

The current Review of the Privacy Act is, at a high level, looking at the connection between cyber security and the protection of personal information, and whether APP 11 should be amended to provide greater clarity for entities about what 'reasonable steps' means in practice.⁴¹ The Review is also considering whether improvements could be made to the code making power under the Privacy Act. Irrespective of whether changes are made to the Act, a Privacy Act code could be established to provide clear expectations about how Privacy Act entities should meet their existing cyber security obligations under APP 11.

Our intent would be for a code to specify minimum, rather than best practice approaches, and could be a combination of specific and principles-based requirements. This will ensure the code strikes the right balance between clarity and flexibility (in line with our best practice principles at Appendix B).

The code could target specific kinds of technology, sectors or kinds of data. We are particularly interested in your feedback about high-impact lower-cost cyber security controls that could be included in a code. We are also interested in whether a code could be targeted towards higher risk entities or technology providers that service large numbers of other businesses.

The Australian Taxation Office's Digital Service Provider Operational Framework (co-designed with industry) could provide an example of the kinds of requirements that could be realistically required as minimum expectations in a cyber security code (see call out box below). We do not believe that it would be realistic to mandate the Australian Signals Directorate's Essential 8 through a cyber security code, but it would be important to avoid conflicts between a future code and existing best-practice guidance.

Australian Taxation Office Digital Service Provider Operational Framework

The Digital Service Provider (DSP) Operational Framework (the Framework) is an existing example of a mandatory technical standard that could be modelled for application across the digital economy. Developed by the Australian Taxation Office (ATO) and the Australian Businesses Software Industry Association, the Framework requires digital service providers interacting with the ATO to complete a self-assessment to show they have implemented a number of mandatory technical controls including encryption, audit logging and strong authentication. The ATO has assessed that the DSP Operational Framework has enabled significant uplift in the uptake of cyber security standards across digital service providers. Digital service providers have reported greater awareness and appreciation of the importance of cyber hygiene and cyber standards.⁴²

40 OAIC 2013, *Guidelines for developing codes*, available at <https://www.oaic.gov.au/privacy/guidance-and-advice/guidelines-for-developing-codes/>.

41 Further information available at <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>.

42 Further information on the requirements of the Framework available at <https://softwaredevelopers.ato.gov.au/RequirementsforDSPs>.

A cyber security code would have some limitations. It could only apply to the protection of 'personal information' (although in practice improvements in cyber security might 'trickle down' to other types of data held by Privacy Act entities). A code would also only apply to entities who are covered by the Privacy Act (generally organisations with an annual turnover of more than \$3 million).

Benefits

The main benefit of a code is that it would provide a strong incentive to improve security across the digital economy by entities covered under the Privacy Act (see Chapter 3). It would also have the benefits of standardising the approach businesses employ to protect personal information and provide clarity on how businesses can meet their cyber security obligations. Technical controls included in the code could be targeted, flexible, scalable and achievable. A cyber security code could harmonise international standards and offer opportunities to Australian businesses to market their security credentials internationally.

Costs

Costs could depend on the exact content of the code. Our intent is to prioritise achievable, cost effective, high impact controls. Industry would design the code and would therefore lead the process for determining what this looks like in practice.

There would be costs for Government to resource the Office of the Australian Information Commissioner to oversee the code as the regulator of the Privacy Act.

Implementation issues and risks

In mandating a new code, the Government would need to remain mindful of existing and emerging cyber security obligations to limit burden on industry. Design of the cyber security code would need to ensure that businesses subject to other regulatory requirements are not overburdened. We are seeking your feedback on the optimal scope of a code, so as to maximise economic and cyber security benefits.

Technology evolves at a rapid pace and technical controls that are effective today may not be relevant in the future. A principles-based approach would keep the code current and reduce the risks of 'tick-a-box compliance culture'. The introduction of a code would also require periodic reexamination and adjustment of the technical controls to ensure they are sustainable and effective against future technological threats.

Despite these issues, implementation of a cyber security code under the Privacy Act may drive meaningful improvements in Australia's cyber security, if it is appropriately balanced against cost. We are interested in your views about costs and benefits and whether you agree with our preliminary view that the benefits of this option could outweigh the costs.

Summary of policy options

Option	Benefits	Costs	Net Impact
Option 0 – Status quo	Nil.	Nil.	– Inconsistent adoption of cyber security standards continues.
	Zero	Zero	Status quo
Option 1 – Minimum standards for personal information	<ul style="list-style-type: none"> – More consistent implementation of cyber security standards. – Increased certainty for industry. – Can be targeted to the greatest risks. 	<ul style="list-style-type: none"> – Low costs to design the code. – Moderate but variable implementation costs. – Moderate costs for oversight by OAIC. 	– Seeking your feedback. Benefits may outweigh the costs. However, impact will depend on which entities are covered under a code.
	Medium–High	Medium	Positive

Discussion questions:

- 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?
- 9 What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?
- 10 What technologies, sectors or types of data should be covered by a code under the Privacy to achieve the best cyber security outcomes?



6. Standards for smart devices

Consumer grade smart devices are quickly growing in popularity and availability, with approximately 21 billion smart devices worldwide today.⁴³ Our need for interconnectivity and convenience in day-to-day life is growing rapidly, increasing our dependence on these devices. It is predicted that there will be as many as 75 billion smart devices globally by 2025.⁴⁴

What is a smart device?

Smart devices, sometimes referred to as consumer Internet of Things (IoT) devices, are products that are given extra functionality to connect to the internet. Examples include smart lights, smart TVs, smart watches and baby monitors, as well as the equipment that connects these devices, like Wi-Fi routers.

Research from around the world has shown that the rapid growth in smart devices has outpaced the adoption of good cyber security practices. Research by the University of New South Wales showed that in a sample of 20 popular devices, every product had some form of vulnerability.⁴⁵ These vulnerabilities are being exploited in the real world, with impacts on cyber security, privacy and online safety (see case studies below).

Our smart devices are vulnerable

In 2020, UK consumer group *Which?* and security engineer Paul Marrapese discovered a critical security flaw affecting smart security cameras, baby monitors and doorbells. They estimated that there are over 3.7 million of these vulnerable devices worldwide.⁴⁶ Hackers are able to exploit flaws in these features to rapidly find vulnerable cameras, then launch attacks to access them. It is believed that 47 wireless camera brands worldwide may have been affected

43 Centre for Strategy & Evaluation Services 2020, *Framing the nature and scale of cyber security vulnerabilities within the current consumer Internet of Things (IoT) landscape*, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900327/Framing_the_nature_and_scale_of_cyber_security_vulnerabilities_within_the_current_consumer_internet_of_things__IoT_landscape.pdf.

44 Ibid.

45 The University of New South Wales and the Australian Communications Consumer Action Network 2017, *Inside job: Security and privacy threats for smart-home IoT devices*, available at https://accan.org.au/files/Grants/UNSW-ACCAN_InsideJob_web.pdf.

46 Paul Marrapese 2020, *Security cameras vulnerable to hijacking*, available at <https://hacked.camera/>.

by this security flaw. Many of these devices are produced by less well known brands and sold mainly through online marketplaces.⁴⁷

Other incidents have shown that security flaws can allow attackers full access to, and control of devices. In 2018, a hacker took over a camera being used as a baby monitor and broadcast threats, including threatening to kidnap the baby.⁴⁸

Smart devices key to network compromise

As well as affecting the security and privacy of individuals, smart devices can be used as the initial entry point to compromise the larger networks they are connected to. In a well-known 2017 report, data was stolen from a North American casino using an internet-connected fish tank thermometer as the initial point of compromise.⁴⁹ It is likely that many attacks against smart devices are never discovered.

We believe that one reason that many smart devices are vulnerable is because competition in the market is primarily based on new features and cost. Unfortunately, consumers often aren't able to tell the difference between a secure and insecure device, which limits commercial incentives to compete on cyber security and leads consumers to unknowingly adopt cyber security risk. This is part of the broader problem of *information asymmetries* and *negative externalities* that we discussed in [Chapter 2](#). We discuss policies to better inform consumers in [Chapter 7](#).

Current Government action on security for smart devices

On 3 September 2020, the Australian Government released the voluntary *Code of Practice: Securing the Internet of Things for Consumers* (Code of Practice).⁵⁰ The Code of Practice contains thirteen principles that signal Government expectations to manufacturers about the security of smart products. These principles align with international approaches, such as the UK's Code of Practice⁵¹ and the European Telecommunication Standards Institute (ETSI) baseline standard on smart devices (ESTI EN 303 645).⁵² The Australian Cyber Security Centre has also developed complementary IoT guidance to help individuals, families and small and medium businesses buy, use and dispose of IoT devices securely.⁵³

47 Andrew Laughlin 2020, *More than 100,000 wireless security cameras in the UK at risk of being hacked*, available at <https://www.which.co.uk/news/2020/06/more-than-100000-wireless-security-cameras-in-the-uk-at-risk-of-being-hacked/>.

48 Amy Wang 2018, *'I'm in your baby's room': A hacker took over a baby monitor and broadcast threats, parents say*, available at <https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/>.

49 Alex Schiffer 2017, *How a fish tank helped hack a casino*, <https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/>.

50 Australian Government 2020, *Code of Practice: Securing the Internet of Things for Consumers*, available at <https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf>.

51 UK Department of Digital, Culture, Media and Sport 2018, *Code of Practice for Consumer IoT Security*, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf.

52 European Telecommunication Standards Institute (ETSI) 2020, *Cyber Security for Consumer Internet of Things: Baseline Requirements*, available at https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf.

53 ACSC 2020, *Internet of Things devices*, available at <https://www.cyber.gov.au/acsc/view-all-content/advice/internet-things-devices>.

In March 2021, we completed research on how industry has responded to the Code of Practice six months since it was released (see [Annex A](#)). Major manufacturers we interviewed told us that voluntary, principles-based guidance has a limited impact on business decision-making and that they would prefer Australia to point to internationally aligned standards. While major brands we spoke to had good intentions to

implement strong cyber security, we were able to identify some high priority, low cost parts of the Code of Practice that had not been implemented consistently (see callout box below). We found it very difficult to engage manufacturers from the lower-cost end of the market in our research, which suggests that our voluntary guidance is likely to have had less impact on that part of the market.

Our research on the security of smart devices

The Australian Government has undertaken in-depth qualitative research into industry uptake of the voluntary Internet of Things Code of Practice. Key findings include:

- Many firms are aware of the Code of Practice, but found it difficult to implement high-level principles. Participants preferred Government to communicate its expectations of industry through internationally-recognised standards.
- While all participants stated a commitment to strong cyber security, many had not yet implemented a vulnerability disclosure policy, which is one of the low cost, high priority recommendations of the Code of Practice. A key challenge moving forward is how best to ensure that firms' intentions to implement good cyber security are matched by their actual practices.
- Products sold at the lower end of the market can have less reputation to protect and thus less incentive for high cyber security. These devices could compromise the security of other devices when connected to a larger IoT ecosystem or network.

Internationally, some jurisdictions are moving beyond voluntary measures towards mandatory standards or product labelling. The UK⁵⁴, Singapore⁵⁵, California⁵⁶ and Oregon⁵⁷ have, or are in the process of, introducing legislation that requires manufacturers of smart devices to make sure their products have basic cyber security features, such as unique passwords.

The European Union has indicated that it is considering a regulatory approach to smart devices.⁵⁸ As these changes are implemented in international markets, it is likely to drive further standardisation domestically.

54 UK Department for Digital, Culture, Media and Sport 2021, *New cyber security laws to protect smart devices amid pandemic sales surge*, available at <https://www.gov.uk/government/news/new-cyber-security-laws-to-protect-smart-devices-amid-pandemic-sales-surge>.

55 Cyber Security Agency of Singapore 2021, *Cybersecurity Labelling Scheme (CLS)*, available at <https://www.csa.gov.sg/programmes/cybersecurity-labelling/about-cls>.

56 *SB-327 Information privacy: connected devices*. Available at https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

57 *House Bill 2395*. Available at <https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/HB2395/Enrolled>.

58 Council of the European Union 2020, *Council Conclusions on the cybersecurity of connected devices*, available at <https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/en/pdf>.

International exemplar: UK Code of Practice

The UK decided to introduce a legislated standard for smart devices after finding that its *Code of Practice for Consumer IoT Security*,⁵⁹ which was released in October 2018, did not have sufficient uptake.⁶⁰

Research found that five of every six companies do not have a mechanism for vulnerability reporting, which is a high priority recommendation. A lack of strong passwords and clear expectations on security updates were also areas of concern.⁶¹ The legislation will mandate the first three principles of UK's Code of Practice, which are key provisions within the ESTI standard EN303 645.⁶²

This chapter discusses options for implementing cyber security standards for smart devices in Australia.

Option 0 – Status quo

The status quo option would maintain Australia's voluntary and market-driven approach to smart device security and the existing Code of Practice would be relied upon to drive cyber security outcomes. Industry education about the Code of Practice would continue, but industry response to the Code of Practice would likely be limited, particularly for lower-cost manufacturers.

If action is not taken, many of the 371 million smart devices forecast to be operating in Australia by 2024 could be insecure.⁶³

Option 1 – Mandatory standard for smart devices

This option involves establishing a mandatory product standard for smart devices.

The standard would require manufacturers to implement baseline cyber security requirements for smart devices. To ensure international consistency and adoption of best practice, we propose that Australia consider adopting ETSI EN 303 645.

The whole of the ETSI standard could be mandated or we could follow the footsteps of the UK and mandate only its top 3 requirements. The former would ensure that all aspects of cyber security are captured through the standard, while the latter would capture the highest priority principles but would place less burden on industry in the short-term.

We propose that a standard would cover the same definition of smart devices specified in the ETSI standard. This includes "consumer Internet of Things devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services". The UK has decided to include smartphones in the scope of their new reforms.⁶⁴ Mobile phones could be included, depending on your feedback.

The standard would need to be established in legislation. Our analysis is that there is no

59 UK Department for Digital, Culture, Media and Sport 2018, *Code of Practice for Consumer IoT Security*, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf.

60 UK Department for Digital, Culture, Media and Sport 2020, *Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation*, available at <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation>.

61 IoT Security Foundation 2020, *Consumer IoT: Understanding the Contemporary Use of Vulnerability Disclosure – 2020 Progress Report*, available at <https://www.iotsecurityfoundation.org/wp-content/uploads/2020/03/loTSF-2020-Progress-Report-Consumer-IoT-and-Vulnerability-Disclosure.pdf>.

62 UK Department for Digital, Culture, Media and Sport 2021, *Government response to the call for views on consumer connected product cyber security legislation*, available at <https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation>.

63 Telsyte 2020, *IOT@HOME gathers pace with home-bound Australians*, available at <https://www.telsyte.com.au/announcements/2020/10/20/iohome-gathers-pace-with-home-bound-australians>.

64 UK Department for Digital, Culture, Media and Sport 2021, *Government response to the call for views on consumer connected product cyber security legislation*, available at <https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation>.

convenient way to implement a standard for smart devices under current Australian laws and that new legislation would likely be required. An existing (yet to be determined) regulator would be responsible for educating manufacturers about the standard and taking enforcement action if needed.

Benefits

This option would mean consumers could rely on stronger cyber security in consumer grade products and would be less vulnerable to cyber security threats. The UK modelled that the probability of attacks on smart devices could be reduced by between 20 and 70 per cent through a basic mandatory standard for smart devices (the top three principles of the UK's Code of Practice). It was estimated this could result in economic benefits of ~A\$3.6 billion over ten years.⁶⁵

A standard would directly respond to our research findings that voluntary, principles based guidance has had a limited impact on smart device security and that major manufacturers prefer clear technical standards.

Costs

Compared to voluntary, market-driven approaches, a mandatory standard would involve higher regulatory burden. However, consistent with our best practice principles (see Appendix B), this burden could be managed through a gradual implementation of new requirements

The cost of manufacturers implementing a standard will depend on its scope. The UK estimated the costs of implementing a basic

mandatory standard (the top three principles of the UK's Code of Practice and the ETSI standard) to be relatively low – a one-off cost of 1.35 per cent of product value, with an annual ongoing cost of 0.31 per cent.⁶⁶ This equates to a one-off cost of 67.5 cents for a \$50 device and an ongoing cost of 15.5 cents annually.

Retailers and wholesalers of devices would likely carry some responsibility for ensuring that products that do not meet the standard are not sold in Australia. There would be some costs for retailers and wholesalers in informing themselves of new requirements and ensuring security standards are met by their suppliers.

Implementation issues and risks

A mandatory standard may result in reduced product availability or increased costs for consumers if industry cannot or chooses not to absorb the costs of a mandatory standard. Industry feedback and analysis by the UK indicated that reductions in product choice from a basic standard or increases in costs for consumers are likely to be low.⁶⁷

Given that 74 per cent of smart devices are sold online,⁶⁸ it would be particularly important to ensure that online marketplaces assist in implementing the standard. Currently, online marketplaces voluntarily remove products from the market that don't meet Australia's product safety standards. We are seeking your feedback about whether this would be a viable approach for any new cyber security standard.

It would be difficult to prevent all direct imports of insecure smart devices. However if costs are low, there would be little incentive for consumers to intentionally circumvent the mandatory standard through direct imports.

65 UK DCMS 2019, *Mandating security requirements for consumer 'IoT' products: Consultation stage impact assessment*, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798722/Secure_by_Design_Consultation_Stage_Regulatory_Impact_Assessment.pdf.

66 UK DCMS 2020, *Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT*, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900330/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things__IoT__products.pdf.

67 Centre for Strategy & Evaluation Services 2020, *Framing the Nature and Scale of Cyber Security Vulnerabilities within the Current Consumer Internet of Things (IoT) Landscape*, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900327/Framing_the_nature_and_scale_of_cyber_security_vulnerabilities_within_the_current_consumer_internet_of_things__IoT__landscape.pdf.

68 UK DCMS 2020, *Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT*, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900330/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things__IoT__products.pdf.

Summary of policy options

Option	Benefits	Costs	Net Impact
Option 0 – Status quo	Nil.	Nil.	– Ongoing cyber security, privacy and online safety incidents involving smart devices.
	Zero	Zero	Status-quo
Option 1 – Mandatory standard for smart devices	<ul style="list-style-type: none"> – Consistent and timely improvements in security. – Probability of breaches involving smart devices could be reduced by ~20-70 per cent. 	<ul style="list-style-type: none"> – Relatively low implementation costs to industry. – Some resourcing costs for Government enforcement. 	– Seeking your feedback. Benefits may outweigh the costs.
	Medium-High	Low-Medium	Positive

Seeking your feedback

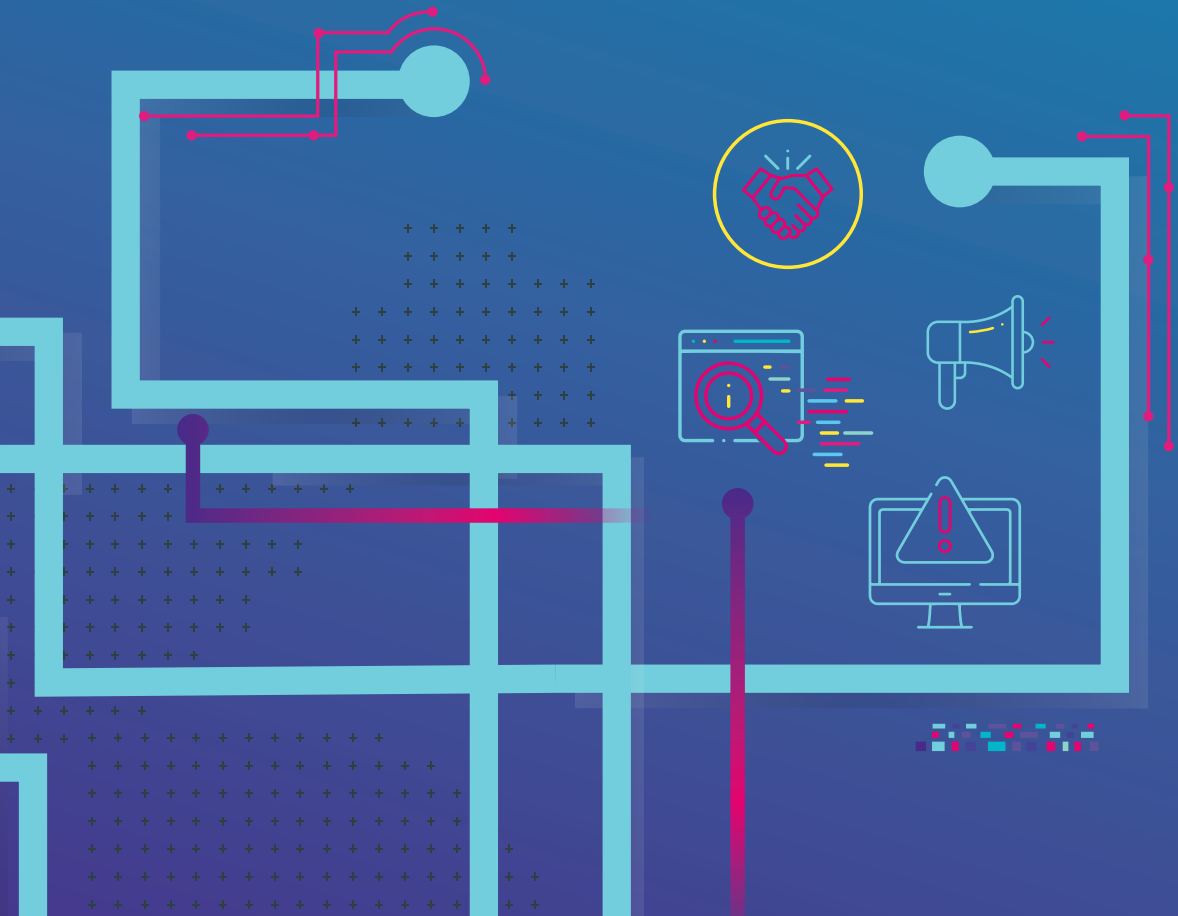
- 11** What is the best approach to strengthening the cyber security of smart devices in Australia? Why?

Mandatory standards (Option 2)

- 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?
- 13** *[For online marketplaces]* Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?
- 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?
- 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?

Part 2 – Increase transparency and disclosure

Clear information for businesses and households about the security of technology products





7. Labelling for smart devices

Consumers do not currently have the tools to easily understand whether smart devices are cyber secure as there is often a lack of clear, accessible information available to them. This is problematic because, as we discussed in Chapter 6, many smart devices have poor cyber security. A study by Data61 found that nearly 50 per cent of consumers incorrectly believe that cyber security is built-in to all smart devices sold in Australia.⁶⁹

Labelling schemes can be effective in changing consumer behaviour (see case study below) and are widely used in Australia for nutritional information and energy, water and fuel efficiency. There is evidence that consumers think that cyber security is an important buying consideration and worth paying for.^{70,71} For these reasons, we think that a cyber security labelling scheme could be successful in Australia.

Impactful labelling

Star safety ratings for road vehicles have driven the uptake of safer vehicle technologies in Australia (above minimum standards). Over 17 years, the percentage of vehicles achieving a 5 star rating has increased from zero to above 80 per cent.⁷² A 2018 evaluation of the Australian Government's mandatory Water Efficiency Labelling Scheme found that the program substantially reduced energy and water consumption between 2006 and 2016, with net economic benefits of \$5 billion.⁷³

Though these other labelling schemes have been successful, they are quite different to cyber security. For example, consumers gain a direct financial benefit by purchasing more water efficient products, but this would not be the case for cyber security. Another difference is that vehicles are expensive products so manufacturers can afford to undertake costly testing, while smart devices are comparatively much cheaper so there is often not a built-in budget for independent testing. These factors may influence the effectiveness of labelling for smart devices.

69 Data61 2020, *Results of the IoT Consumer Focused Survey*, unpublished report produced for the Cyber Security Cooperative Research Centre.

70 Data61 2020, *Results of the IoT Consumer Focused Survey*, unpublished report produced for the Cyber Security Cooperative Research Centre; Atif Ahmad et al., *Towards responsive regulation of the Internet of Things: Australian perspectives*, available at <https://policyreview.info/articles/analysis/towards-responsive-regulation-internet-things-australian-perspectives>.

71 Shane D. Johnson, John M. Blythe, Matthew Manning, Gabriel T. W. Wong 2020, *The impact of IoT security labelling on consumer product choice and willingness to pay*, available at <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0227800>.

72 Australasian New Car Assessment Program 2019, *The Facts Behind ANCAP 2018-19*, available at <https://s3.amazonaws.com/cdn.ancap.com.au/app/public/assets/a84852929a284a662230389fea18f5cc8282e6f0/original.pdf?1588891487>.

73 Institute for Sustainable Futures 2018, *Evaluation of the environmental and economic impacts of the WELS scheme*, available at <https://www.waterrating.gov.au/sites/default/files/documents/evaluation-wels-scheme-final-report-2018.pdf>.

Option 0 – Status quo

Without action, many consumers will continue to purchase smart devices with a limited understanding of that product’s cyber security. While some consumers will consider best practice guidance available from the Australian Cyber Security Centre and the Internet of Things Alliance Australia,⁷⁴ insecure smart devices will continue to cause privacy, cyber security and online safety harms to Australians.

Option 1 – Voluntary star rating label

Cyber security labels for smart devices are becoming more common. Singapore and Finland have implemented voluntary security

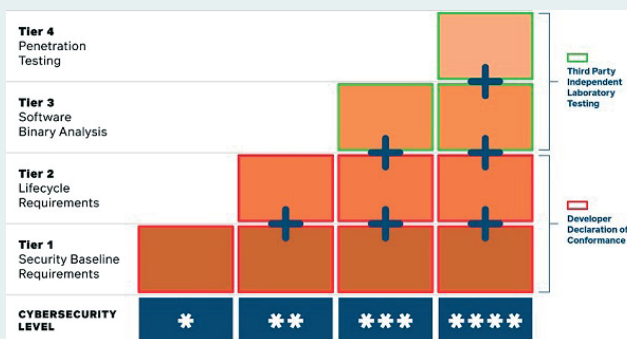
labels for smart devices (see case study below). Three voluntary assurance schemes for smart products have been launched recently in the UK, two of which provide participating manufacturers with a trust mark for their products.⁷⁵ In 2020, the US Cyberspace Solarium Commission recommended that Congress establish a National Cybersecurity Certification and Labelling Authority to develop a labelling program for technology products.⁷⁶ On 12 May 2021, President Biden signed an Executive Order which included piloting a graded cyber security labelling scheme for consumer smart devices, modelled after existing government programs if applicable.⁷⁷ The Internet of Things Alliance Australia (IoTAA) is developing a Security Trust Mark primarily for commercial and industrial applications.⁷⁸

International exemplar: Singapore’s labelling scheme

The Cyber Security Agency of Singapore introduced a voluntary labelling scheme for smart devices in October 2020. The scheme consists of four cyber security levels, with each indicating a higher level of security and/or additional security testing.⁷⁹

Tier 1 and 2 require a manufacturer to undertake a self-assessment of their products and make a declaration of how the device conforms to the requirements. Manufacturers seeking to achieve Tier 3 or Tier 4 are required to undergo third party laboratory testing. The requirements of the scheme align with the international standard ETSI EN 303 645.

Figure 1. CSA Singapore 4 Level Cyber Security Labelling Scheme⁸⁰



74 ACSC 2020, *Tips to secure you Internet of Things device*, available at <https://www.cyber.gov.au/sites/default/files/2020-08/Tips%20to%20secure%20your%20Internet%20of%20Things%20device%20%28AUG%202020%29.pdf>; IoTAA 2021, *Ensuring your IoT is secure: A user's guide*, available at <https://iot.org.au/wp-content/uploads/2021/02/IoTAA-IoT-Users-Security-Awareness-Guide-Ebook.pdf>.

75 UK Department for Digital, Culture, Media and Sport 2021, *New cyber security laws to protect smart devices amid pandemic sales surge*, available at <https://www.gov.uk/government/news/new-cyber-security-laws-to-protect-smart-devices-amid-pandemic-sales-surge>.

76 Cyberspace Solarium Commission 2020, *Final Report*, available from <https://www.solarium.gov/report>

77 President Biden 2021, *Executive Order on Improving the Nation's Cybersecurity*, available at <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>.

78 Full details are available from the Internet of Things Alliance Australia's submission to the Cyber Security Strategy at <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020>.

79 Cyber Security Agency of Singapore 2021, *About the Cybersecurity Labelling Scheme*, available at <https://www.csa.gov.sg/programmes/cybersecurity-labelling/about-clis>.

80 Cyber Security Agency of Singapore 2020, *Cybersecurity Labelling Scheme for Manufacturers*, available at <https://www.csa.gov.sg/programmes/cybersecurity-labelling/for-manufacturers>.

How would a voluntary labelling scheme work in Australia?

The practical details of how a voluntary labelling scheme would work in Australia could be based on an existing scheme or shaped by industry through a co-design process. For discussion purposes, we suggest that a label have the following features:

- *Coverage* – any consumer smart device intended to be connected to the internet or a home network. This would include devices such as children’s toys, smart home devices, smart appliances and wearables. Mobile phones could be excluded, depending on your feedback.
- *Labels* – labels could be used in online marketing material and/or physical packaging. There is evidence that star rating labels (like Singapore’s) are the most effective in guiding consumers through complex choices.⁸¹
- *Requirements and enforcement* – an existing international framework would be used, such as Singapore’s scheme which aligns with the requirements of ESTI standard EN303 645. Self-certification and/or independent testing could be used to ensure compliance. Any self-assessments would be approved by an administration body. The Australian Consumer Law would deter manufacturers from making misleading or deceptive claims about security.
- *Complement standards* – a voluntary labelling scheme could complement mandatory standards for smart devices (Chapter 6) because it would allow businesses to highlight where they have chosen to go above minimum requirements. This is an approach that is adopted for other products like road vehicles, where mandatory safety standards and voluntary labelling complement each other.

Benefits

The UK estimates that on average 15 per cent of consumers would switch to more secure devices over a 10-year period as a result of a mandatory label.⁸² A voluntary label is likely to take longer to have a similar effect, or may have a lower impact overall. Real-world implementation data from jurisdictions like Singapore will provide additional insight about the benefits of security labels, and this could be a reason to take a ‘wait and see’ approach.

A labelling scheme is likely to be attractive to businesses that want to differentiate their products from less secure competitors. If cyber security labelling became popular, the rest of the market would have an incentive to uplift their cyber security to remain competitive.

Costs

This would be a voluntary measure, and businesses would only label their smart products if the benefits outweigh the costs. For businesses that choose to participate, there would be costs to fund the administration body, testing costs (if independent testing is required), and marketing costs. IoTAA estimates that certification through independent testing facilities would cost manufacturers between A\$7,000 to A\$12,000 for most products.⁸³ Administrative costs to industry under Singapore’s scheme are approximately A\$50–\$A3,700 per device (depending on the rating level being sought). Marketing costs could be low, especially if labels are displayed online.

Implementation issues and risks

It is uncertain whether there would be sufficient industry participation in a voluntary labelling scheme. Uptake would take time,

81 Shane D. Johnson, John M. Blythe, Matthew Manning, Gabriel T. W. Wong 2020, *The impact of IoT security labelling on consumer product choice and willingness to pay*, available at <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0227800>.

82 UK Department for Digital, Culture, Media and Sport 2019, *Mandating security requirements for consumer ‘IoT’ products: Consultation stage impact assessment*, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798722/Secure_by_Design_Consultation_Stage_Regulatory_Impact_Assessment.pdf.

83 Jeremy Kirk 2020, *Coming Soon: ‘Trust Mark’ Certification for IoT Devices*, available at <https://www.bankinfosecurity.com/australia-developing-trust-mark-for-connected-devices-a-14459>.

require sustained government promotion and will be affected by the actions of other countries. Without sufficient uptake of labelling, businesses with the lowest levels of cyber security would continue to have low incentives to improve cyber security.

Like all labelling schemes, a cyber security label would have the limitation of displaying the security of a device at one point in time. Some labels include the date they were awarded to make sure that consumers understand this limitation.

Option 2 – Mandatory expiry date label

This option considers a mandatory label for smart devices, which would meet a recommendation of the Cyber Security Strategy Industry Advisory Panel. 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). This kind of label would not require independent security testing, and therefore would be a lower cost approach compared to a star rating label.



Figure 2: Example expiry date label

An expiry date label has the advantages of being objective and easy to understand. New reforms in the UK will require manufacturers of smart devices to inform consumers about a

device's support period at the point of sale.⁸⁴ However, Australia would be the first country to mandate this in the form of a specific label. Some companies already provide cyber security expiry dates, so this policy would expand an approach already being undertaken by some market participants (see Figure 2).



Safe, simple and always up to date.

Thanks to Android One, the new Nokia models Nokia 5.3 and Nokia 8.3 5G are regularly supplied with software innovations and security updates.



****Confirm exact duration of support for phones in your territory with smartphone manufacturer. Monthly security updates to be supported for at least 3 years after initial phone release.**

Figure 3. Advertisements for new Nokia smart phones promote regular security updates.⁸⁵

A mandatory label would be implemented in a similar fashion to a voluntary label. It could cover most or all consumer smart devices intended to connect to the internet or a home network, potentially including mobile phones. It could be required in online marketing, physical packaging, or both. Instead of an administration body, a regulator would enforce the labelling requirements. Similar to a voluntary label, it could complement mandatory standards for smart devices (Chapter 6).

An expiry date label would complement a standard for smart devices (see Chapter 6) by building on the requirements of ETSI EN 303 645. The ETSI standard specifies that the support period of a device should be clear and

⁸⁴ UK Department for Digital, Culture, Media and Sport 2021, *Government response to the call for views on consumer connected product cyber security legislation*, available at <https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation>.

⁸⁵ See https://www.android.com/intl/en_au/one/.

transparent to consumers.⁸⁶ A mandatory labelling scheme would prescribe the way this information is displayed to consumers.

Benefits

A mandatory label would ensure uptake of the scheme. The UK modelled that a mandatory 'trust mark' label would reduce the probability of breaches on smart devices by between 10 and 50 per cent and that 15 per cent of consumers would switch to more secure devices over a 10-year period. It was estimated this would result in economic benefits of ~A\$645 million.⁸⁷ While these findings are not directly comparable to an expiry date label, they provide illustrative findings.

Similar analyses of Australian labelling schemes, such as country of origin labelling and button battery warnings, have also found positive net economic benefits.⁸⁸ These results give us confidence that a cyber security label in Australia would be beneficial.

Costs

We estimate that the costs of this policy would be low for both Government and industry. The main costs are those that businesses face in familiarising themselves with enhanced regulatory requirements (particularly given these requirements would not apply in other markets) and updating marketing materials. The UK assessed the cost of implementing a physical labelling to be approximately 1.54 per cent of revenue derived from sales of smart devices (77 cents for a \$50 device). This one-off cost could be reduced if labelling was built into regular packaging redesign or

if a digital only label was used. The annual cost of implementing a labelling scheme was assessed to be 0.06 per cent, equating to 3 cents for a \$50 device.⁸⁹ It was assessed that these costs are not likely to be passed onto consumers. The costs for a digital label would be even lower.

There would also be some costs for retailers who would need to ensure that their products meet the labelling requirements.

There would be some moderate costs to a government regulator to enforce the scheme, including educating industry participants and consumers.

Implementation issues and risks

If implemented, Government would need to determine what kinds of vulnerabilities must be patched while a device is 'in date', and how quickly those patches should be provided. Government would need to provide clear guidance about legal interactions with consumer guarantees under the Australian Consumer Law.

There would be challenges in requiring online retailers operating entirely overseas to use a label. Currently, online marketplaces voluntarily remove products from the market that don't meet Australia's product safety standards. We are seeking your feedback about whether this would be a viable approach for a mandatory cyber security label. It would be difficult to prevent consumers directly importing products without a label.

This policy could potentially result in reduced product availability if providers decide to discontinue supplying to Australia. At this stage, we consider the risks of reduced product

86 European Telecommunication Standards Institute (ETSI) 2020, *Cyber Security for Consumer Internet of Things: Baseline Requirements*, available at https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf.

87 UK Department for Digital, Culture, Media and Sport 2019, *Mandating security requirements for consumer 'IoT' products: Consultation stage impact assessment*, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798722/Secure_by_Design_Consultation_Stage_Regulatory_Impact_Assessment.pdf.

88 Department of Industry, Innovation and Science 2016, *Country of origin labelling: Decision Regulation Impact Statement*, available at <https://ris.pmc.gov.au/sites/default/files/posts/2016/04/Country-of-Origin-Labeling-Decision-RIS-1.pdf>; Australian Competition and Consumer Commission 2020, *Button Battery Safety: Final Recommendation to the Minister*, available at https://ris.pmc.gov.au/sites/default/files/posts/2020/12/25774_-_button_battery_safety_-_independent_review_report.pdf.

89 UK Department for Digital, Culture, Media and Sport 2020, *Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT*, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900330/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things_._IoT_._products.pdf.

availability and increased costs for consumers to be low, because we expect costs for industry to be low.

On balance, both voluntary labelling and mandatory security expiry dates may be low cost and low risk policies that could improve Australia's cyber security. Both a label and standard for smart devices ([Chapter 6](#)) could be implemented simultaneously.

We recognise that a voluntary label would need to be industry-led. The Government can only do so much to encourage uptake of voluntary measures, so the success of this

policy would rely on strong buy-in from industry, both in Australia and internationally. If there is a strong industry commitment to a voluntary approach, government and businesses could work together to determine the most appropriate scheme for the Australian context.

If there is not strong industry support for this policy, then a mandatory label may be a better approach. However, there might be merit in waiting until real-world implementation data is available from other jurisdictions before implementing either kind of cyber security label.

Summary of policy options

Option	Benefits	Costs	Net Impact
Option 0 – Status quo	Nil.	Nil.	– Consumers would continue to purchase insecure smart devices.
	Zero	Zero	Status-quo
Option 1 – Voluntary star rating label	– Benefits will depend on uptake. We are seeking your views about likely uptake of a voluntary label.	– Low administrative and marketing costs. – Moderate testing costs, if and when required.	– Impact will depend on uptake.
	Unclear	Medium	Unclear
Option 2 – Mandatory expiry date label	– Probability of breaches involving smart devices could be reduced by ~10-50 per cent. – ~15 per cent of consumers could switch to more secure devices over 10 years.	– Low costs for industry – Moderate administration costs for a government regulator.	– Seeking your feedback. Consumers may be empowered to make better purchasing decisions. Likely net economic benefits.
	Medium	Low	Positive

Seeking your views

- 16** What is the best approach to encouraging consumers to purchase secure smart devices? Why?
- 17** Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?

Voluntary star rating (Option 1)

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

Mandatory expiry date label (Option 2)

- 19** Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?
- 20** Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?
- 21** Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?



8. Responsible disclosure policies

Almost all software contains some vulnerabilities which can be exploited by malicious actors. Some of these vulnerabilities could be critical to address, where others might only be minor issues. Timely development and distribution of patches to fix vulnerabilities is an important part of cyber security. However, US research indicates that 50 percent of vulnerabilities remained without a patch for more than 438 days and that vendors did not always prioritise the highest risk vulnerabilities.⁹⁰ This section explores the role of responsible disclosure policies to support software developers and businesses to identify and resolve vulnerabilities, and what Government can do to help.

What is responsible disclosure and how does it work?

Responsible vulnerability disclosure is a process where security researchers find and report vulnerabilities to software developers, businesses or agreed third parties, including Government.⁹¹ This allows the software owner to develop a patch before the vulnerability is discovered by a malicious actor. Ordinarily, vulnerabilities and mitigations are disclosed to the public after patches are developed.⁹² In some cases, a public disclosure after between 45 and 90 days may be considered to encourage a reluctant vendor to patch systems or software. This process provides benefits to businesses, security researchers and end users.

⁹⁰ US Cyberspace Solarium Commission 2020, *Final Report*, available at http://fdd.org/wp-content/uploads/2020/03/CSC-Final-Report.pdf?bcsi_scan_25ee14e37a8217d2=xVMRM37MwwOSxVDL8/U4KPIT7W40AAAAo3jXbQ==&bcsi_scan_filename=CSC-Final-Report.pdf.

⁹¹ European Union Agency for Network and Information Security 2015, *Good Practice Guide on Vulnerability Disclosure – from challenges to recommendations*, available at <https://www.enisa.europa.eu/publications/vulnerability-disclosure>.

⁹² Ibid.

Benefits of responsible disclosure

Businesses	Security researchers	End users
<ul style="list-style-type: none"> – Cost effective way for businesses to find and address vulnerabilities in software and systems. – Businesses can market their commitment to cyber security. 	<ul style="list-style-type: none"> – Financial benefits through bug bounty schemes.⁹³ – Career development opportunities and the possibility to enhance standing in online communities.⁹⁴ – Altruistic motives.⁹⁵ 	<ul style="list-style-type: none"> – Access to more secure products. – Greater assurance that businesses will act to address vulnerabilities in software and systems. This can inform purchasing decisions.

What is our current approach to responsible disclosure?

The Australian Government already encourages responsible disclosure through the Information Security Manual (which provides guidance to all federal agencies). The Australian Cyber Security Centre (ACSC) also encourages security researchers, customers and members of the public to responsibly report security vulnerabilities directly with organisations, vendors and service providers. However, in instances where attempts at communication are impractical or unsuccessful, security vulnerabilities can be reported to the ACSC

via [cyber.gov.au](https://www.cyber.gov.au). ACSC can pass on unverified vulnerabilities to other agencies where appropriate.⁹⁶

Similarly, the US Cybersecurity and Infrastructure Security Agency (CISA) requires US federal agencies to maintain a responsible disclosure policy.⁹⁷ On 12 May 2021, President Biden signed an Executive Order which included a range of measures to improve the transparency of software security, including industry guidance on vulnerability disclosure programs and consideration of a software labelling program.⁹⁸ The UK National Cyber Security Centre (NCSC) has released guidance to support businesses to develop their own responsible disclosure policy.⁹⁹

“We need to move to a world...where all companies providing internet services and devices adhere to a vulnerability disclosure policy”

Julian King
European Commissioner for Security Union.¹⁰⁰

93 European Union Agency for Network and Information Security 2018, *Economics of vulnerability disclosure*, available at <https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure>.

94 Ibid.

95 Ibid.

96 Australian Cyber Security Centre 2020, *Australian Government Information Security Manual – Guidelines for Software Development*, available at <https://www.cyber.gov.au/sites/default/files/2020-08/18.%20ISM%20-%20Guidelines%20for%20Software%20Development%20%28August%202020%29.pdf>.

97 Congressional Research Service 2020, *Cybersecurity: Recent Policy and Guidance on Federal Vulnerability Disclosure Programs*, available at <https://fas.org/sgp/crs/misc/IN11497.pdf>.

98 President Biden 2021, *Executive Order on Improving the Nation's Cybersecurity*, available at <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>.

99 National Cyber Security Centre 2020, *Vulnerability Disclosure Toolkit*, available at https://www.ncsc.gov.uk/files/NCSC_Vulnerability_Toolkit.pdf.

100 Computer Weekly 2017, *Euro commissioner calls for more collaboration on cyber security*, available at <https://www.computerweekly.com/news/450427879/Euro-commissioner-calls-for-more-collaboration-on-cyber-security>.

Adoption of responsible disclosure policies among Australian businesses remains low. Our research has identified that only 5 per cent of ASX 200 companies currently maintain a responsible disclosure policy. There is evidence to suggest that this may be lower than other technology leaders internationally including the US, UK and Germany,¹⁰¹ however there are differences between countries that make a direct comparison difficult.

Without formal procedures for responsible disclosure, security researchers may face increased risks of legal action, difficulties in contacting someone with authority to fix the problem, or businesses and software developers may be slow to respond to genuine problems. This is demonstrated by a 2011 incident where a legal action was reportedly brought against an Australian security researcher who identified a significant security vulnerability in a superannuation firm's systems.¹⁰² We are seeking your feedback about whether a stronger approach to responsible disclosure would benefit Australia and what role the Australian Government should play.

Option 0 – Status quo

Responsible disclosure policies are increasingly being adopted by businesses and governments in international markets. It is possible that Australian businesses will respond to this trend and also increase uptake of these policies. However, a slower rate of adoption domestically may impact the capability of Australian businesses to engage security researchers in the international market to support vulnerability detection.

Option 1 – Voluntary approaches to increasing responsible disclosure

Government could release guidance or tool-kits for industry on the process of developing and implementing responsible disclosure policies. We welcome your feedback about the kind of voluntary guidance that would be most useful, noting that various guides are already available.¹⁰³ Another option would be to include responsible disclosure as a component of the voluntary governance standard considered earlier in this paper ([Chapter 4](#)).

Option 2 – Regulatory approaches to increasing responsible disclosure

Government could consider driving adoption of responsible disclosure policies through existing regulatory frameworks. Responsible disclosure policies are already part of the product standard we are considering for smart devices ([Chapter 6](#)) and are recommended for businesses and government agencies required to comply with the Information Security Manual. Responsible disclosure could be incorporated into a potential cyber security standard for personal information (see [Chapter 5](#)).

In 2020, a committee established by the US Congress recommended legislating a requirement that final goods assemblers of software, hardware and firmware are liable for damages from incidents that exploit known and unpatched vulnerabilities.¹⁰⁴ We discuss

¹⁰¹ HackerOne 2020, *4th Annual Hacker Powered Security Report*, available at <https://www.hackerone.com/blog/introducing-4th-annual-hacker-powered-security-report>.

¹⁰² IT News 2011, *Legal threats for unauthorised security tests on the rise*, available at <https://www.itnews.com.au/news/legal-threats-for-unauthorised-security-tests-on-the-rise-277169>.

¹⁰³ See for example, Google's Starting a vulnerability disclosure program at <https://developers.google.com/android/play-protect/starting-a-vdp> or the European Union's Google Practice Guide on Vulnerability Disclosure at <https://www.enisa.europa.eu/publications/vulnerability-disclosure>.

¹⁰⁴ US Cyberspace Solarium Commission, *Final Report*, available at http://fd.org/wp-content/uploads/2020/03/CSC-Final-Report.pdf?bcsi_scan_25ee14e37a8217d2=xVMRM37MwwOSxVDL8/U4KPIT7W40AAAAo3jXbQ=&bcsi_scan_filename=CSC-Final-Report.pdf.

liability based approaches to cyber security in [Chapter 10](#).

Incorporating vulnerability disclosure into existing regulatory frameworks would increase adoption of good practices but would create a relatively low level of regulatory burden. Regulatory burden could be limited by offering software developers the flexibility to determine

the most appropriate responsible disclosure policies to adopt.

Government support for businesses to voluntarily adopt responsible disclosure policies would be consistent with the best practice principles (see [Appendix B](#)), and could be considered first, before giving further consideration to mandatory standards.

Summary of policy options

Option	Benefits	Costs	Net Impact
Option 0 – Status quo	Nil.	Nil.	– Software vulnerabilities will continue to be exploited before patches can be implemented.
	Zero	Zero	Status-quo
Option 1 – Voluntary approaches	– Businesses will be empowered to adopt best practices.	– Low administrative costs for industry and government.	– Seeking your feedback. More software vulnerabilities may be identified depending on uptake, but overall benefits expected to be modest.
	Low	Very Low	Positive
Option 2 – Regulatory approaches	– More consistent uptake of best practices.	– We expect costs would be low, but your feedback is required.	– Seeking your feedback.
	Low-medium	Unclear	Unclear

Seeking your views

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



9. Health checks for small businesses

One of the biggest challenges in cyber security is understanding supply chain risk. Supply chain risk can occur either because you are directly connected to the IT systems of another organisation, are a provider of a service to another organisation, or because a disruption to another organisation would interrupt the supply of goods and services that you need to keep your business running.

In Chapter 2, we outlined that one of the core problems we are seeking to address is *information asymmetries*, where sellers are in a better position to understand the cyber security of their digital products and services than buyers. Reducing information asymmetries would help businesses better understand their supply chain risk and improve Australia's overall cyber security.

We are already taking action on supply chain security. The Australian Government has recently released updated guidelines on managing cyber security supply chain risk for all businesses,¹⁰⁵ and is currently developing the *Critical Technology Supply Chain Principles* to assist organisations – including governments and businesses of all sizes – to make informed decisions regarding the security of their critical technology supply chains and the transparency of their own products. While we think a voluntary approach is appropriate for

most businesses, some responsible entities for critical infrastructure already have legislated requirements to manage supply chain risk.

One area where Government might be able to provide additional support is supply chain risk management for small businesses. During consultation on the Cyber Security Strategy, small businesses told us that they face a consistent set of challenges – limited time, limited money and limited cyber security expertise. This means that small businesses don't have as much opportunity to understand and implement existing guidance from the Australian Cyber Security Centre. As a result, small businesses are less likely to implement basic, but important, cyber security measures. This also means that many large businesses often don't have appropriate knowledge about the cyber security of important small business suppliers and customers.

This section considers a cyber security health check program to provide greater support to small businesses.

¹⁰⁵ ACSC 2021, *Cyber Supply Chain Risk Management*, available at <https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management>.

Case study: Cyber Security Strategy support for small and medium businesses

Australia's Cyber Security Strategy 2020 includes a range of initiatives to support small and medium businesses. This includes:

- \$26.0 million to expand the Australian Cyber Security Centre's services for SMEs.
- \$8.3 million for the *Connect and Protect* program, which provides SMEs with tailored cyber security advice and assistance from trusted sources.
- \$4.9 million for a public awareness campaign for households and small businesses.
- \$12.3 million to extend the Australian Cyber Security Centre's helpdesk to SMEs and families.
- \$6.1 million to support victims of cybercrime (including SMEs).
- Release of a cyber security self-assessment tool for small businesses.

Option 0 – Status quo

If no action is taken then small businesses will need to access existing government programs and cyber security guidance from the Australian Cyber Security Centre. Large businesses would need to invest time and money in understanding and managing cyber security risk to small businesses in their supply chain, and instead may choose to invest these resources in other priorities.

Option 1 – Cyber health checks for small businesses

One simple mechanism to improve cyber security for small businesses would be to introduce a voluntary cyber security health check program. On completion of the health check, the small business would be awarded a trust mark which they could use in marketing their business (see example in Figure 4). We anticipate that a health check would be most relevant in situations where a business' customers are concerned about cyber security, for example where sensitive data is involved or to address supply chain risk.



Figure 4: Example health check trust mark

Requirements for the health check program could be aligned with existing guidance provided by the Australian Cyber Security Centre. For example, choosing a secure cloud service provider, turning on free-to-use security settings like multi-factor authentication, training staff using free resources and ensuring data is backed up regularly. The health check could build on the recent release of a cyber security self-assessment tool for small businesses.¹⁰⁶

Businesses applying for the health check would self-assess their own compliance, with a basic level of due diligence provided by Government or a third party. This avoids the costs of a certification scheme and makes it clear that a health check is not a guarantee of complete security. A health check could expire after 12 months to ensure that small businesses don't adopt a 'set and forget' approach to their cyber security.

¹⁰⁶ Available from <https://www.business.gov.au/news/is-your-business-cyber-secure>.

Case study: UK cyber essentials

The UK Government runs a cyber security program called Cyber Essentials which helps businesses show their customers that they have achieved a basic level of cyber security through the use of a trust mark (see below). Businesses who earn the trust mark can use it to market their business as cyber secure. Cyber Essentials focuses on five simple cyber security controls: firewalls, secure device settings, appropriate administrator privileges, antivirus software and patching.

Most participants in the program self-assess their own cyber security, but expert assistance is available to make sure participants don't encounter technical barriers. An evaluation completed by the UK Government in 2020 found that the program has a positive impact on a wide range of factors, including improving business understanding of risk, identifying incidents more quickly and increasing business confidence in their cyber security capabilities.¹⁰⁷

Participating in the program is a requirement for some businesses providing services to the UK Government, which creates direct benefits for participating businesses.



Figure 5. Cyber Essentials trust mark¹⁰⁸

Benefits

Any small business who completed a health check would benefit from being able to provide additional assurance to their customers and suppliers about their cyber security. We are seeking your feedback about whether these commercial benefits are likely to be significant.

We know from other similar schemes that businesses who review their security tend to improve their cyber security knowledge and risk management practices, which is a benefit in its own right.¹⁰⁹

Large businesses could benefit from additional supply chain assurance from small business suppliers and customers. This could be particularly relevant for businesses like insurers, banks and accountants. These kinds of organisations might choose to encourage uptake of a health check program because of these flow-on benefits.

The size of these benefits could be tested in a pilot program.

Costs

We estimate that the costs of this policy would be low for both Government and industry.

A program design with very low direct costs to participants could be achievable if existing resources, guidance and support are used to support delivery of the program. Small businesses would need to invest their time to participate in the program and in any cyber security improvements, but this would be voluntary.

There would be some administrative costs to government, but these could be reduced by leveraging existing program delivery infrastructure.

¹⁰⁷ National Cyber Security Centre 2020, *Review of the Cyber Essentials influence on cyber security attitudes and behaviours in UK organisations*, available from <https://www.ncsc.gov.uk/information/setting-baseline-ce-prior-to-iasme>.

¹⁰⁸ Source: <https://iasme.co.uk/cyber-essentials/>

¹⁰⁹ For example, participant feedback on the UK Cyber Essentials Program and the Australian Taxation Office's Digital Services Program Operational Framework.

Implementation issues and risks

We believe that the success of a health check program would rest on the strength of incentives for small businesses to participate. In the UK, use of the Cyber Essentials trust mark has been encouraged by requiring its use in Government procurement (see case study). The Australian Government’s procurement rules already encourage strong cyber security,¹¹⁰ and we think there would be challenges to implementing additional requirements that only apply to small businesses.

This means that Australia may need to look to other incentives to undertake a cyber health check. As mentioned above, this could include working with organisations such as insurers, banks, accountants and peak groups to promote the program. We are seeking your feedback about whether this is a viable approach and what other incentives we should examine.

Note that there are other government programs providing cyber security assurance (such as the Consumer Data Right Data Safety Licence and consideration of a privacy certification scheme through the Privacy Act Review). These kinds of schemes are generally targeted towards larger businesses and have more stringent requirements. To our knowledge there are no other voluntary programs targeted at small businesses.

To ensure the trust mark does not provide a false sense of security, the program should clearly articulate to suppliers and consumers that the trust mark is not a guarantee of complete security.

On balance, a cyber health check program could have real benefits, but only if feedback indicates that there are realistic ways to encourage time-constrained small businesses to participate

Summary of policy options

Option	Benefits	Costs	Net Impact
Option 0 – Status quo	Nil.	Nil.	– Australia continues to face the challenge of supply chain risk management, but existing resources are available to assist industry.
	Low	Low	Status-quo
Option 1 – Cyber health checks for small businesses	<ul style="list-style-type: none"> – Participating small businesses are more secure. – Increased supply chain visibility for large businesses. – Commercial benefits for small businesses. 	<ul style="list-style-type: none"> – Administration costs for government. – Very low costs to participating businesses, depending on program design. 	– Seeking your feedback. Benefits may outweigh the costs if there is sufficient uptake. Modest level of benefits expected.
	Low	Very low	Positive

¹¹⁰ Department of Finance 2020, *Commonwealth Procurement Rules*, available at <https://www.finance.gov.au/government/procurement/commonwealth-procurement-rules>.

Seeking your views

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

Part 3 – Protecting consumers

Clear legal remedies for consumers after a cyber security incident occurs





10. Clear legal remedies for consumers

Currently, there are limited legal options for consumers to seek remedies or compensation for cyber security incidents. Existing laws, such as the Tort of Negligence and the Australian Consumer Law (ACL), have played a prominent role in legal action for physical goods. However, to our knowledge they have not been used to compensate consumers for cyber security incidents.

Earlier in this discussion paper, we discussed the need to increase transparency and disclosure, and explored options for providing consumers with information to make better purchasing decisions. Building on this principle, we believe that stronger rights of recourse for cyber security could provide appropriate compensation after an incident and incentivise technology companies to maintain acceptable levels of cyber security.

Recourse through the Australian Consumer Law (ACL)

The ACL is designed to regulate the conduct of businesses and to protect the rights of consumers in Australia. It applies to all businesses that engage in trade and commerce in Australia and is enforced by state and federal courts and state tribunals.

The ACL sets out general protections that apply to a wide variety of consumer products including digital goods and services (detailed in [Chapter 3](#)). The ACL's protections against misleading and deceptive conduct prohibit businesses from making false representations, including in relation to cyber security. However, this does not mean that a business needs to take any particular steps to prevent cyber security incidents – only that they cannot make misleading or deceptive representations about the cyber security of their products.

Consumer guarantees

The consumer guarantees help ensure that goods (including digital goods) are of acceptable quality and fit for purpose, and that services (including digital services) are provided with due care and skill. These provisions may extend to ensuring a digital good or service has an appropriate level of cyber security, although there have not been any significant court or tribunal cases to test this.

There are a number of challenges in applying consumer guarantees to cyber security:

- *Determining that the transaction is for a 'good' or 'service'* – under the ACL, the consumer needs to establish that the transaction is for a 'good' or 'service'. Digital goods and services usually consist of multiple components such as hardware, software and technology services. Some interpretations of current ACL provisions suggest that these components may not all fall within the scope of the ACL.¹¹¹ In 2015, the UK's *Consumer Rights Act 2015* introduced new consumer rights and remedies in respect of 'digital content' in addition to 'goods' and 'services' to address a similar issue.
 - *Identifying the responsible business* – most digital goods and services are made by multiple businesses. It can be difficult for a consumer to tell which business is responsible for a cyber security failure, which might make it more difficult to hold businesses to account.
 - *Determining what went wrong* – significant technical expertise may be required to establish that there has been a breach of the consumer guarantees because a good was not 'fit for purpose' or a service provided with 'all due care and skill'.
 - *Access to justice* – a consumer would need to have the resources to undertake action in a court or tribunal against potentially large companies based overseas, which is a significant barrier. There is no ability for regulators to take action to enforce consumer guarantees. This is an issue that extends beyond cyber security.

Planned reforms to consumer guarantees

Commonwealth, state and territory ministers responsible for Australia's consumer law have requested the development of a regulatory impact assessment of specific options to improve compliance with the ACL consumer guarantees.¹¹² Importantly, the regulatory impact statement will examine whether a civil prohibition should be introduced for failing to provide a consumer guarantee remedy. This would provide the Australian Competition and Consumer Commission (ACCC) with more options to directly enforce consumer guarantees in certain circumstances. This would help address some of the barriers described above (including identifying the responsible business, determining what went wrong and improving access to justice).

Treasury is leading this work on behalf of all states and territories and will undertake a consultation process in the coming months.

Separately, Treasury will also consult state and territory officials on exploring whether the ACL's application to digital products should be clarified to ensure there are no unintended gaps in the operation of the law. This could include consideration of existing product recall powers to treat physical recalls and software updates equally.

Recourse through the Privacy Act

A direct right of action for privacy breaches is currently being explored as part of the Privacy Act Review. This would mean that in certain circumstances victims of cyber security incidents involving personal information could take businesses who have not taken reasonable steps to protect this personal information (which may include through implementing adequate cyber security practices) to court and seek damages.

¹¹¹ Valve Corporation v ACCC [2017] FCAFC 224.

¹¹² Meeting of Ministers for Consumer Affairs, *Communique*, 30 August 2019, available at <https://consumerlaw.gov.au/consumer-affairs-forum/communiques/meeting-11-0>.

Individuals can already lodge a complaint with the Office of the Australian Information Commissioner (OAIC) if they believe their personal information has been mishandled.¹¹³ However, under the Privacy Act, individuals currently lack the ability to litigate a claim for breach of their privacy. In 2019, the ACCC published its findings from the Digital Platforms Inquiry and recommended that individuals should be given a direct right to bring actions and class actions in court to seek compensation for an interference with their privacy under the Privacy Act.¹¹⁴ The Government has indicated that it supports this recommendation in principle, subject to consultation and design of specific measures.

A direct right of action could give individuals greater control over their personal information and provide an additional incentive for entities covered by the Privacy Act to comply with their obligations under the Act.¹¹⁵ It could also increase the opportunity for the courts to provide greater clarity and certainty regarding cyber security requirements, and to set standards in relation to penalties and compensation for privacy breaches.¹¹⁶

However, a direct right of action could also suffer from similar limitations as consumer guarantees under the ACL because consumers would require significant resources and expert knowledge to prove that the steps taken by a businesses to protect their personal information were not reasonable. This limitation could be partially addressed through class actions or permitting OAIC to bring cases on behalf of individual or groups of consumers. The Government is also considering whether the small business exception from the Privacy Act should be retained, and how any changes would interact with a direct right of action.

The Attorney-General's Department is leading ongoing consultation on this matter. Further information is available at: <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>.

Seeking your views

We are seeking feedback on how current government initiatives can be strengthened to better protect consumers from cyber security threats and whether additional action is required.

- 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?
- 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?

113 See OAIC 2021, *Privacy Complaints*, available at <https://www.oaic.gov.au/privacy/privacy-complaints/>.

114 ACCC 2019, *Digital Platforms Inquiry Final Report*, June 2019, available at <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>.

115 Attorney-General's Department 2020, *Privacy Act Review Issues Paper*, available at <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>.

116 Attorney-General's Department 2020, *Privacy Act Review Issues Paper*, available at <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>.



Other issues

We are interested in your feedback on any other issue you believe we should consider to strengthen Australia's approach to cyber security regulation and incentives.

Seeking your views

- 28** What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights consumers?



Next steps

Make a written submission

The Government is seeking your views about the best way to uplift the cyber security of Australian businesses. We invite interested stakeholders to make a written submission via the Home Affairs website. Written submissions will close on 27 August 2021.

We will also be holding virtual public open forums to hear views from you directly. To register for a consultation session, please visit the Home Affairs website.

What we will do with your feedback

Your feedback will be used to refine our voluntary and regulatory cyber security policy options and will allow us to fully understand the costs and benefits of these different options. The regulatory burden of any new reforms will be carefully considered alongside the option of no new regulation.

What happens next?

In order to further refine these policy options and recommendations, we will continue to have ongoing conversations directly with industry and the Cyber Security Industry Advisory Committee. We may also seek additional views or advice from you on specific issues before providing recommendations to Government for consideration.

If you have any questions, please contact techpolicy@homeaffairs.gov.au.



Appendix A:

List of discussion questions

You may wish to answer some or all of these questions in your written submission.

Chapter 2: Why should government take action?

- 1 What are the factors preventing the adoption of cyber security best practice in Australia?
- 2 Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?

Chapter 3: The current regulatory framework

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

Chapter 4: Governance standards for large businesses

- 5 What is the best approach to strengthening corporate governance of cyber security risk? Why?
- 6 What cyber security support, if any, should be provided to directors of small and medium companies?
- 7 Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

Chapter 5: Minimum standards for 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?
- 9 What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?
- 10 What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes?

Chapter 6: Standards for smart devices

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

- 12** Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt for 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?
- 13** *[For online marketplaces]* Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?
- 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?
- 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?

Chapter 7: Labelling for smart devices

- 16** What is the best approach to encouraging consumers to purchase secure smart devices? Why?
- 17** Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?
- 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?
- 19** Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?
- 20** Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?
- 21** Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?

Chapter 8: Responsible disclosure policies

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

Chapter 9: Health checks for small businesses

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

Chapter 10: Clear legal remedies for consumers

- 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?
- 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?

Chapter 11: Other issues

- 28** What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights consumers?



Appendix B:

Best practice principles for effective policy and regulation

These principles are drawn from a large pre-existing body of knowledge on government decision-making and regulatory design, particularly previous work by the Productivity Commission, Treasury's Resilience Framework and the Office of Best Practice Regulation.

Best practice principles:

- A clear problem has been identified.
- Proposed action is proportionate to the problem.
- Benefits outweigh the costs.
- Implementation risks are identified and mitigated. Unintended consequences, such as market distortions, are considered.
- Policies with low regulatory burden are considered first.
- Impacts on specific groups, such as small businesses, have been identified.
- International standards are applied where relevant to reduce regulatory burden.
- There are clear roles and responsibilities for implementation.
- Policies are technologically neutral and are responsive to changes in technology.
- The policy is financially sustainable.
- The policy is practical to implement.
- If enforcement is required, there are clear monitoring and enforcement mechanisms.
- Policies are appropriately sequenced to reduce regulatory burden.
- The impact of the policy can be measured.



Annex A:

Understanding the cyber security of smart devices in Australia

Executive summary

The Department of Industry, Science, Energy and Resources (DISER) and the Department of Home Affairs, undertook research to understand how manufacturers manage cyber security risks from Internet of Things (IoT) devices. This research was undertaken approximately six months after the release of the Australian Government's *Code of Practice: Securing the Internet of Things for Consumers (Code of Practice)*, which is a set of 13 voluntary cyber security practices.¹¹⁷ This research provides insights into the impact of the Code of Practice, how industry cyber security practices are changing over time, and ongoing opportunities for stronger cyber security to inform the policy options presented in this discussion paper.

Consumer IoT devices, also referred to as smart devices, are products that are given extra functionality to connect to the internet, such as smart TVs and home assistants. It is estimated there will be 371 million smart devices in Australia by 2024, with the average Australian household owning around 36 connected devices by 2024.¹¹⁸ While these devices

enhance users' convenience, comfort and efficiency in day-to-day life, many of these devices have cyber security vulnerabilities.¹¹⁹

Throughout this project, DISER engaged 70 IoT firms (companies that manufacturer and/or sell IoT devices for purchase in Australia) and completed 13 in-depth qualitative interviews. During our interviews, many firms said the "high level" principles of the Code of Practice can be challenging to implement at the engineering and manufacturing phases of product development. Many firms interviewed indicated a preference for technical and internationally-aligned standards that can be implemented by all levels of the supply chain.

Most firms interviewed said they are strongly committed to cyber security and believe they comply with the Code of Practice, however not all had implemented all principles in the Code of Practice. For example, most firms interviewed had not yet implemented a vulnerability disclosure policy (a key principle of the Code of Practice).

We heard that operators of app stores and smart home ecosystems play important roles in influencing cyber security practices as both

¹¹⁷ Australian Government 2020, *Code of Practice: Securing the Internet of Things for Consumers*, available at <https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf>.

¹¹⁸ Telsyte 2020, *IOT@HOME gathers pace with home-bound Australians*, available at <https://www.telsyte.com.au/announcements/2020/10/20/iot-home-gathers-pace-with-home-bound-australians>.

¹¹⁹ The University of New South Wales and the Australian Communications Consumer Action Network 2017, *Inside job: Security and privacy threats for smart-home IoT devices*, available at https://accan.org.au/files/Grants/UNSW-ACCAN_InsideJob_web.pdf.

set standards for products to be listed on their store or to integrate with their systems. Interviewed firms said that ecosystems tend to drive higher cyber security standards and therefore create a barrier for insecure devices to integrate with their systems. Retailers, too, have the potential to influence cyber security in the products they sell.

Most firms interviewed told us that maintaining their reputation as a trusted brand was a strong driver underpinning their approach to cyber security. For many firms, working with well-established and reputable suppliers and partners was also important. Some firms interviewed delegated responsibility for cyber security to these third parties, with various levels of assurances.

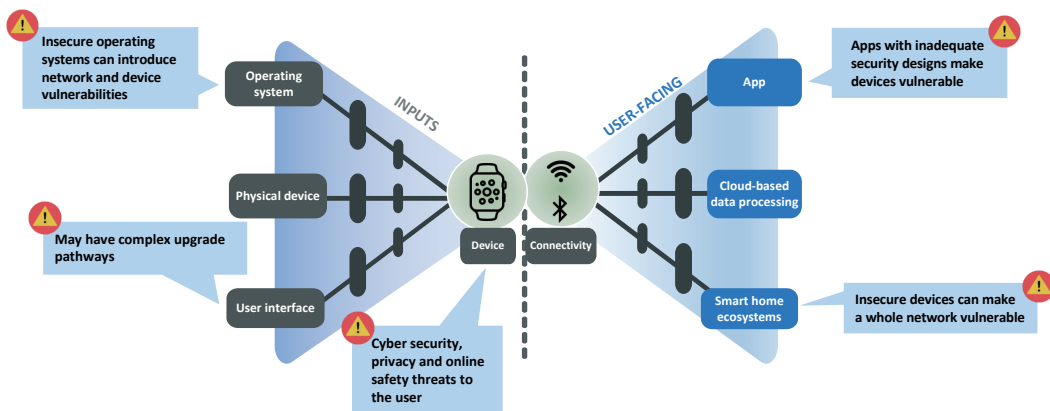
The policy options outlined in this discussion paper (Chapters 6 and 7) directly respond to the findings of this research, particularly feedback that international standards would help industry implement stronger cyber security practices, and that there is an opportunity for consumers to make more informed purchasing decisions.

How smart devices work, and what makes them vulnerable

Three important features of smart devices are:




- the **physical device** itself, an object with a sensor or multiple sensors that are bundled together
- the **operating system**, which is software that runs the basic functions of the device
- the **user interface**, which allows the user to interact with the device.

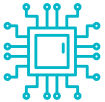




The smart device has some **connectivity**, which allows the device to connect to other systems and networks. Through this connectivity, smart devices can collect and store device data through **cloud-based data processing**, and connect to **smart home ecosystems** such as Google Home and Alexa.



Qualitative research with a sample of the Australian IoT market

In-depth qualitative interviews with a sample (13) of Australia's IoT firms. The sample comprised mostly large multinational companies who manufactured a range of smart products.

HQ location	Business size	Industries
		
Australia – 6 Asia – 4 Europe – 2 USA – 1	Small – 4 Medium – 1 Large – 8	70% of firms were from the home automation, consumer electronics and white goods industries. The remainder manufactured wearables and industrial IoT.

 <p>3 out of the 13 firms manufacture components of an IoT device</p>	 <p>11 out of the 13 firms manufacture the final product</p>	 <p>7 out of the 13 firms sell their IoT products wholesale</p>	 <p>10 out of the 13 firms sell to retailers</p>	 <p>3 out of the 13 firms sell directly to users</p>
---	--	---	--	--

The sample represents approximately 5 per cent of the Australian smart device market (based on open source research conducted throughout this project). Though it is indicative, the sample is not representative of the Australian smart device market. Noting the sample size for this research, there may be other firms in the market who are have different business models, approaches to security, and views on the Code of Practice than those who were interviewed.

Key interview findings

Internationally aligned standards are more useful than principles

- Firms prefer technical standards: Many firms we interviewed saw the principles of the Code of Practice as too high level and said they prefer technical standards that are translatable to their engineering and manufacturing teams.
- Consistent standards: Most firms we interviewed told us that it is important to align domestic standards with international standards. Many firms said they implement the most stringent standards available (generally European standards) to ensure they meet the standards in most domestic markets.
- Actual cyber security practices lag firms' intentions: Many firms interviewed said they were strongly committed to cyber security, but most have not yet implemented a vulnerability disclosure policy (a key part of the Code of Practice).
- Firms trust their suppliers and delegate cyber security responsibilities to these suppliers, often with limited assurance: Most firms interviewed believe their suppliers comply with the necessary standards and regulations, including cyber security standards. However, many of the interviewed firms were not able to describe established processes for checking this compliance.

All parts of the supply chain have a role to play

- Firms do not feel significant push from consumers: Many of the firms interviewed told us that consumers are largely unconcerned or uninformed about cyber security and often prioritise usability over security. Some firms saw cyber security as a shared responsibility with consumers.

- Smart home ecosystems drive strong cyber security practices: Firms we interviewed told us that smart home ecosystems – such as Amazon's Alexa and Google Home – drive strong cyber security practices, and often have higher standards than app stores. Devices that do not meet these standards cannot integrate with these ecosystems.
- App stores play an important role in influencing cyber security practices: Operators of app stores set standards for products to be listed on their store. Firms told us they play an important role in influencing cyber security practices.
- Retailers have the opportunity to drive cyber security standards: Firms we interviewed told us that retailers often push product standards (e.g. electrical safety standards) but not all retailers set cyber security standards for products. Retailers have the potential to play a significant role in influencing product cyber security expectations.

Trust drives investment in cyber security

- Reputation is the primary driver for implementing strong cyber security: Many of the firms interviewed – particularly large, multinational companies – told us that maintaining their reputation as a trusted brand drove their approach to cyber security.
- Some firms do not identify with the term "IoT": Many IoT firms produce only a small line of IoT products in addition to their traditional product range. Interviewed firms were more likely to identify as manufacturers of "smart" products than "IoT" devices.

