CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

CSCRC SUBMISSION:

Strengthening Australia's cyber security regulations and incentives

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: Strengthening Australia's cyber security regulations and incentives

The Cyber Security Cooperative Research Centre (CSCRC) is pleased to make this submission to the Department of Home Affairs regarding the *Strengthening Australia's cyber security regulations and incentives* discussion paper. The CSCRC commends the Federal Government for its ongoing commitment to ensuring Australia remains a safe and prosperous digital nation, which will only be achieved via consultation and co-design processes such as this.

About the CSCRC

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's cyber security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem. The CSCRC has two research programs: Critical Infrastructure Security and Cyber Security as a Service.

We look forward to answering any queries regarding this submission and welcome the opportunity to participate in future discussions on this very important topic.

Yours Sincerely,

Rachael Falk
CEO, Cyber Security Cooperative Research Centre
[redacted]

Introduction:

The CSCRC welcomes the progressive initiatives proposed by the Federal Government in the *Strengthening Australia's cyber security regulations and incentives* discussion paper, which aims to position Australia as a leading digital economy by 2030. These programs and reforms are timely and relevant, given the escalating level of cyber security threats since the release of *Australia's Cyber Security Strategy 2020* in August of last year. In 2021 there has been a string of high-profile cyber incidents, including the zero-day SolarWinds cyber espionage campaign; a ransomware attack on the 'jugular of the infrastructure in the United States',[1] Colonial Pipelines, which provides fuel to 45 per cent of the East Coast; and a significant ransomware hack on JBS Foods, the world's largest meat supplier, which had repercussions around the world, including in Australia. And on 19 July 2021, in an unprecedented display of diplomatic solidarity, the US, its Five Eyes allies, the European Union, Japan and NATO joined together[2] to attribute the March 2021 Microsoft Exchange Server cyber espionage operations to malicious cyber actors working at the behest of the Chinese Government's Ministry of State Security (MSS).

These attacks have had grave financial impacts on economies around the globe, Australia included. McAfee's recent report, *The Hidden Costs of Cybercrime*, notes the current epidemic of cybercrime is producing global losses totalling more than US$1 trillion,[3] up more than 50 per cent from 2018 figures. Hence, there is a pressing need to bolster the cyber security of Australian organisations through a collaborative, multistakeholder design process and through the development of new policies to tackle key action items.

Central to this must be a 'top down' approach, recognising that senior leaders and boards of all organisations – large and small – have a key role to play in driving cyber security uplift. Hence, there is a need for a greater understanding of cyber security, cyber risk and cyber threats among these leaders. Not only will this ensure that cyber security is a matter of significant priority for organisations right across the economy – it also means they will be better equipped to prepare staff and systems against cyber threats.

[1] Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed | Reuters
[2] The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China | The White House
[3] New McAfee Report Estimates Global Cybercrime Losses to Exceed $1 Trillion| McAfee Press Release

The CSCRC's submission responds to the following:

Chapter 2: Why should government take action?

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

There are multiple factors preventing the widespread adoption of cyber security best practice in Australia. First, factors vary widely according to size of organisation, with Australian small-to-medium sized enterprises (SMEs) having the lowest levels of cyber maturity. This is problematic, given SMEs are the lifeblood of the Australian economy, comprising more than 90 per cent of our nation's businesses, accounting for 33 per cent of GDP and employing more than 40 per cent of the workforce. Yet, according to the *Small Business Survey Report*[4] launched by the Australian Cyber Security Centre's (ACSC) last year, 50 per cent of businesses have an IT security spend of less than AUD $500 annually. There are three key factors that impede SMEs as it comes to adopting better cyber security practices, including:

1) prohibitive costs to purchase sufficient and suitable cyber security products, services and solutions along with a lack of budget for dedicated staff maintaining responsibility for cyber security spend and implementation;
2) time constraints within small organisations;
3) lack of awareness regarding cyber security threats along with a prevailing perspective that small business is immune to cyber threats given opportunity costs.

On the first, cost continues to be perhaps the most significant barrier to SMEs achieving sufficient levels of cyber security hygiene and posture. Existing models and certification schemes, including the ACSC's Essential Eight assessment, are targeted to medium-to-large enterprise with the requisite resources and budget. However, for small business, the cost remains prohibitive – expensive to undertake, implement and maintain. Furthermore, for small businesses, cyber security presents a noisy vendor environment, which can seem confusing and complex. Even if there is a willingness to implement a particular standard, this confusion can present a barrier for small businesses in actual implementation.

A lack of awareness and visibility concerning cyber security threats remains a key impediment. The Australian Small Business and Family Enterprise Ombudsman's 2018 *Small Business Cyber Security Best Practice Guide*[5] noted 33 per cent of businesses with 100 employees or less are not proactive when it comes to responding to and mitigating against cyber security breaches. Further, almost 90 per cent of SMEs rely on antivirus software as their sole cyber security protection.

There is an additional factor at play – a dearth of cyber security professionals, with the skills shortage also presenting a barrier to the adoption of cyber security best practice. Considering the skills gap there is a need for cyber security professional accreditation. Cyber security accreditation

[4] Announcing the ACSC Small Business Survey Report | Cyber.gov.au
[5] PowerPoint Presentation (asbfeo.gov.au)

functions like a 'quality seal', signalling a third-party validated measure of competency and expertise to employers. Government and industry action in this capacity should be immediate and active, with a focus on implementing agreed accreditation standards for Australian cyber security professionals. On this, the CSCRC advocates that government consider adopting the UK's NCSC Certification for Cyber Security/Information Assurance (IA) Professionals. This model could form the basis for an Australian cyber security accreditation regime, given its effective and holistic approach, along with its pronounced focus on facilitating expanded opportunities for non-technical cyber security experts into the workforce.

A final element impeding the uptake of stronger cyber security practices across the Australian economy is the lack of strong incentives for Australian businesses which encourage investment and uptake in cyber security. On this front, to lessen the burden on business to achieving cybersecurity uplift, the CSCRC submits that various incentivisation schemes should be considered for SMEs that can assist with cyber uplift. Such measures could include tax breaks and instant asset write offs, which would have a two-pronged effect and make economic sense, simultaneously easing the impost on SMEs while also hardening the systems of the widest swathe of the Australian economy.

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

The CSCRC submits that yes, a significant negative externality requiring government action is the need to mitigate supply chain risk. This is particularly relevant in relation to when and where producers of technology products and services pass cyber security risks on to third party suppliers and ultimately to consumers. Survey research produced by the CSCRC and Data61 found that despite widespread concerns about the cyber security risks associated with home Internet of Things (IoT) devices and products, 46 per cent of Australian consumers and 17 per cent of business consumer participants made the incorrect assumption that cyber security is built into all IoT devices sold in Australia. Further, there is purchasing demand for it – almost 90 per cent of business consumers indicated that cyber security should be specifically considered in the manufacturing of IoT devices.

IoT manufacturers have, thus far, indicated reluctance to absorb costs associated with cyber security uplift of products, instead letting responsibility flow down to end users. Hence, there is also an information asymmetry which directly impacts consumers, who lack the technical awareness to understand the inherent cyber security risks, thereby creating larger threat vectors for cyber security vulnerabilities across our economy. This is not preferable, and there is a need for better cyber security standards at the point of manufacture. Such changes will only come at the impetus of government through the establishment of baseline cyber security standards or regulations for smart consumer devices. Although such measures could apply to other areas or digital services, the sheer ubiquity of IoT devices in the forthcoming digital future – it is estimated there will be more than 41

billion IoT devices[6] connected to the internet by 2025 – and their interconnectivity brings increasing cyber threats and rising cyber threat vectors. The CSCRC urges the Federal Government to consider appropriate measures and mechanisms to reduce supply chain risks across the smart home device market.

[6] The Growth in Connected IoT Devices is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast | Business Wire

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?**

Although Australia has an extensive ecosystem of laws and regulations which can and do pertain to cyber security, complexity and lack of harmonisation presents an impediment. Current legislative and regulatory regimes are both sector-specific and cross-sectoral, yet as they do not follow a comprehensive framework, there are overlapping requirements causing unnecessary complexity and confusion. Presently there are multiple standards which, for boards of critical infrastructure entities, could lead to confusion as to what 'best practice' could be. Clarity in this regard is especially prudent given proposed reforms in the CI/SoNS legislation currently before Federal Parliament.

For example, for critical infrastructure energy providers, Australian Energy Market Operator (AEMO) has set required minimum standards. For financial services critical infrastructure entities regulated by the Australian Prudential Regulation Authority (APRA), there is CPS234 [Prudential Standard CPS 234 Information Security], which the CSCRC submits sets a high bar and could be viewed as a 'gold standard' in cyber security regulation. While CPS234 is not directly applicable to other sectors, efforts should be made to identify any existing 'gold standard' regulatory regimes across other sectors and, if such regulation exists, to highlight them as best practice.

Alongside streamlining and harmonising existing laws and regulations, guidance must be provided for boards and management as to their obligations regarding cyber security governance, otherwise they could become unnecessarily distracted as to which governance and operation standards to adopt. In addition, given CI/SoNS is currently before the Federal Parliament, clarity needs to be provided concerning which regulators will have oversight over particular sectors, what their enforcement powers will be, and what they will be enforcing to ensure harmonisation with existing regulation and legislation. Furthermore, greater clarity is required in relation as to who or what would have oversight over the functions of these regulators to ensure compliance with the CI/SoNS regime.

Further, for Australian organisations not already captured by existing legislation and regulation pertaining to cyber security and who have a lower level of cyber maturity, the complexity and challenges entailed in understanding obligations and technical requirements and successfully implementing them remain impediments to achieving economy-wide cyber security uplift. The provision of clear and ongoing guidance about organisations' compliance requirements and how these can be successfully met is advisable.

In addition, proposed reforms to the *Security of Critical Infrastructure Act 2018* (SOCI Act) which will capture a much wider swathe of Australian critical infrastructure entities – expanding from four sectors to 11 – are still undergoing a co-design process together with relevant industry stakeholders. It is essential new measures contained in the Bill be developed with harmonisation as a primary consideration. This will support significant uptake from industry and help achieve economy-wide cyber security uplift.

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?**

Data is a valuable target for cyber criminals. Therefore, there is a need to increase understanding and, where appropriate, support management and boards about the acute importance of cyber security and continued cyber security maturity. Australian organisations and their boards must pay as much attention to their online assets and managing their valuable data with the same level of care and attention they pay to their real-world assets, because now both are inextricably linked. Boards must satisfy themselves that data assets are stored and protected appropriately, as the organisation is the legal custodian of that data. These should include independent external assurances, such as a cyber security audit, with findings reported back to the board, to give them a sense of whether they are effectively managing their cyber risk. It is the responsibility of executives, business leaders and boards to be aware of the risks, ensure appropriate measures are in place and to foster a cyber security culture from the top. If cyber security matters to a chair and a board it will have a trickle-down effect.

Further, Australian directors increasingly bear personal exposure to cyber risk liability. This is currently being played out in the Federal Courts, with the Australian Securities and Investments Commission (ASIC) and RI Advice Group case potentially setting a new legal precedent in regard to cyber security liability. ASIC alleges the company had deficient cyber security controls and, despite knowing of them, failed to remedy them. As a result, sensitive client information allegedly was compromised. The case is significant given ASIC, as opposed to the Office of the Australian Information Commissioner (OAIC), is bringing the action. It is a signpost for all organisations that the regulator is prepared to take tough enforcement measures in relation to cyber security responsibilities. Further, while ASIC has chosen to rely on a financial-sector specific part of the Corporations Act to begin these proceedings, it is not a stretch to consider a general directors' duties case could be brought. This would focus on the "degree of care and diligence"– mandated of directors under Section 180 (1) of the *Corporations Act 2001* – when it comes to overall management of cyber security risk and obligations to customers, shareholders and the market.

Given this, the CSCRC recommends rather than voluntary or mandatory standards for larger organisations, and submits the Federal Government consider introducing these as 'best practice' guidelines.

Such guidelines would build off the duties and provisions in Section 180, which remain necessarily broad and fit for purpose, providing clarity as to how the provisions should be addressed through a cyber security lens.

Such an approach would provide appropriate parameters and clarity to management and boards as to their Section 180 duties as they apply to cyber security, ultimately encouraging cyber security uplift. Further, such an approach would signal to both shareholders and consumers that boards of organisations engaging with best practice guidelines were striving towards better cyber security posture, demonstrating they are *aware* of the risks, have *considered* them, and have taken *reasonable* action.

Given the rapidly evolving nature of cyber security risk, guidelines of this sort should be considered a 'living document' and reviewed regularly to ensure they remain fit for purpose. Importantly, they would build on the legal concept of 'reasonableness' and ensure that management and boards consider this lens when understanding and following such guidelines.

This would have a two-pronged effect, improving cyber security awareness among executives and board members of large organisations, which would likely have a trickle-down effect to organisational governance more broadly across the economy. Further, it would draw a line in the sand for boards and leadership teams to handle their data and systems with utmost care, take reasonable steps to protect it at all times and, when issues arise, respond quickly.

It is entirely appropriate and necessary that all directors are familiar with the relevant legislation and adapt cyber security best practices across their organisations to effectively manage cyber risk – as failure to do so could be an expensive mistake. Hence, clarity of directors' duties needs to be provided on an ongoing basis. This is especially relevant for directors of small and medium companies, whose organisations may lack established cyber security baselines and/or have less mature cyber security governance postures, budgets and awareness. Such organisations will require assistance to shift their governance structures to accommodate mandatory governance standards for larger business, which will have a trickle-down effect to smaller organisations.

Importantly, if government adopts the voluntary 'best practice' guidelines for management and directors there will be a need to bring these guidelines to life and assist board with what 'good' looks like with respect to the guidelines and cyber security risk. To this end, there is a role for government to play in providing clear guidance on cyber security standards to ensure the boards of small to medium enterprises are adequately informed. This should be provided on an ongoing basis given the fast-moving pace of cyber security threats and challenges and also given that if an organisation holds personally identifiable information (PII) or sensitive data, there is a need to understand directors' obligations, regardless of the size of their business.

To ensure greater industry buy-in, government might consider opportunities to co-design best practice guidelines together with organisations such as the Australian Institute of Company Directors (AICD), along with the Business Council of Australian (BCA) and the Council of Small

Business Australian (COSBOA), which have strong and effective linkages into Australian business. Furthermore, the AICD is well placed to administer tailored training programs for directors of all levels, driving improved understanding by providing pragmatic and non-technical advice to directors to assist with their awareness and ability to implement proposed guidelines.

Importantly, any training or changes as a result of a company implementing voluntary best practice guidelines could be potentially used in any regulatory investigation or in any s180 litigation as evidence of the culture and approach of the board in management around cyber security risk. So, while these guidelines would be voluntary in nature, if adopted and followed, they would be significant in terms of demonstrating that the board and management had regard to the guidelines and took *reasonable* steps to understand and manage the risk.

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

The CSCRC submits that yes, additional education and awareness raising initiatives for senior business leaders is necessary, particularly if best practice governance standards for larger businesses are to be triggered. Despite the rapid escalation in cyber security risks in recent years, cyber security continues to fly under the radar of boards and executives across many industries, with a recent study[7] finding 94 per cent of Asia-Pacific CEOs are not in regular conversation with chief security officers (CSOs) responsible for managing cyber risk.

The CSCRC recommends any awareness raising initiatives be co-designed with industry, to ensure educational training is fit-for-purpose and will be sufficiently taken-up by industry leaders. Additionally, any campaigns developed should leverage the expertise of relevant Australian organisations, such as the AICD, which offers the *Board's Role in Cyber*[8] course for company directors concerning the management of cyber security risk. Further the BCA could also assist with educating Australian businesses across various sectors about cyber security risk, contributing to an uplift in cyber security awareness.

Furthermore, as previously noted, there is a key role for organisations like the AICD, BCA and COSBOA to play in raising awareness and taking a lead as it comes to delivery of education. Because without proper education, it is difficult to raise meaningful awareness.

[7] Making Security Priorities Business Priorities | LogRhythm
[8] Course Calendar (companydirectors.com.au)

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 as a standard for smart devices? If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate?

The number of smart devices continues to grow and diversify as new 5G networks roll out, bandwidth increases, small energy generation and storage units to power devices diversify and computational power increases. However, along with greater connectivity comes greater risk to consumers looking to take advantage of IoT devices within their homes and businesses. Research undertaken by the CSCRC in collaboration with Data61 involving Australian consumers and Australian business consumers about their perceptions regarding cyber security considerations of IoT devices highlights the majority of participants incorrectly assumed that cyber security is in-built into all IoT devices sold in Australia, with many having strong concerns about the cyber security risks associated with their home IoT devices. Further, 96 per cent of business consumer participants indicated they would be more likely to purchase an IoT device if it had a cyber security rating system attached to it, with those indicating high cyber security awareness articulating willingness to pay more for IoT devices built with assurances of low cyber security risk.

Noting the Federal Government has recognised the voluntary *Code of Practice: Security the Internet of Things for Consumers* (Code of Practice) released last year has had limited effect – as was also found in the UK – and that device manufacturers have signalled their preference for alignment with international best practice standards, there may be merit in introducing mandatory standards for IoT devices. This would trigger greater cyber security uplift across this market. It would, however, require clear and ongoing communication from government, which would provide industry with the necessary awareness and visibility of preferred standards. This would be in line with global best practice seen across the EU, the UK and Singapore, and given that the Australian manufacturing market of IoT devices remains relatively negligible in comparison to more significant IoT manufacturing markets,[9] would help ensure Australia remains at the forefront of global best practice in cyber security standards of IoT devices.

Given Australia's Code of Practice was developed in alignment with the UK's Code of Practice and the European Telecommunication Standards Institute (ETSI) baseline standard on smart devices (ESTI EN 303 645), it is appropriate and relatively easy for Australia to adopt the latter, as there are pre-existing synergies. The CSCRC recommends that at this time, only the top three requirements be mandated for all IoT devices, including smart phones, through a phased approach, in alignment

[9] 2021 Top 500 Industrial IoT Companies | IoT ONE Digital Transformation Advisors

with the approach demonstrated by the UK. Such mandatory requirements would significantly and positively affect the market, creating cyber security uplift and also, fulfilling expectations by Australian consumers that cyber security protections are built-in to smart devices. Further, a phased approach would ease the burden on manufacturers. Lastly, an internationally harmonised approach is suitable and prudent, and would reduce regulatory and standards overlap, streamlining requirements and imposts for manufacturers.

Chapter 7: Labelling for smart devices

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

&

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

The CSCRC notes that given demonstrated appetite by Australian consumers for IoT devices with in-built cyber security protections, as well as need to secure this rapidly proliferating space, the best approach to encourage consumers to purchase secure smart devices is through the design and implementation of a simple, voluntary cyber security rating system for IoT products sold in Australia. A simple easy-to-identify rating system would benefit IoT device manufacturers, retailers and consumers. A survey conducted by the CSCRC and Data61 in 2020 found that cyber security featured in the purchasing patterns of IoT devices in 69 per cent of survey participants, but less than half the participants knew how to look for cyber security features when buying an IoT device. Therefore, an easy-to-understand rating system would likely improve the take-up of more cyber secure IoT devices and nudge the market and IoT manufacturers towards more 'secure by design' principles. The CSCRC recommends this be a digital labelling system, given how quickly physical labels for smart devices become obsolete. A digital system would also potentially allow device manufacturers to update ratings and expiration dates in real time, given escalating and changing cyber security threats and vulnerabilities.

At present, a voluntary rating system is preferable to a mandatory regime, given it would generate greater industry buy-in with less onerous imposts while also producing a significant positive net benefit as it comes to cyber security uplift of smart devices. Further, this approach is in line with global best practice – as seen in Singapore[10] and with the May 2021 Executive Order on Improving the Nation's Cybersecurity[11] signed by the US White House, which includes a cyber security labelling scheme for smart devices. It would also provide scope to move to a mandatory rating system in the future while generating greater cyber security awareness in the interim.

Alongside the voluntary cyber security rating system, IoT device manufacturers and retailers should be required to include easy-to-read consumer information and cyber security feature details on their products. Australians surveyed in research conducted by Data61 on behalf of the CSCRC disclosed preferences for more cyber security related information concerning IoT devices. Further, privacy statements often do not apply to devices despite the inherent privacy risks such devices carry for consumers and citizens, which places consumers at risk of theft of financial data and other sensitive personal information.

[10] About the Cybersecurity Labelling Scheme (csa.gov.sg)
[11] Executive Order on Improving the Nation's Cybersecurity | CISA

While a labelling system would be practical and effective, it should be accompanied by an ongoing cyber security educational and awareness campaign about IoT devices and appropriate cyber security measures to mitigate threats and protect personal data. Research undertaken by the CSCRC and Data61 indicated there is a dearth of consumer awareness concerning cyber security in Australia, with almost half of survey participants making the erroneous assumption cyber security was built in to all IoT devices available in the Australian market. Given this, Australian consumers need greater and ongoing education about cyber security risks pertaining to their IoT devices as well as appropriate cyber security measures and mechanisms that can be implemented by individuals to counter or neutralise threats.

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

The CSCRC supports the development and design of a voluntary cyber security health check program targeted to Australian SMEs, which would improve Australia's cyber security posture among small business and supply chains more generally. The CSCRC is currently leading a 'hands on' pilot project focused on uplifting cyber security across Australia's SME sector, launched in Adelaide in February 2021. The pilot has been designed to address the cyber security lag SMEs often experience, making them a soft target for cyber criminals. The CSCRC recognises the cost and time pressures SMEs face in bolstering their cyber security and the need for simple, straightforward and cost-effective solutions. Anecdotal preliminary evidence from the pilot indicates although there is sufficient guidance in the Australian market targeted to SMEs about how to bolster their cyber security posture, *implementation* remains difficult given existing constraints.

There is much work to be done to achieve comprehensive, whole of economy cyber security uplift: the Australian Cyber Security Centre (ACSC) provides ongoing advice to all government agencies to implement its Essential Eight baseline[12] strategies to mitigate cyber security risks. As it stands, under the *Protective Security Policy Framework* (PSPF), which is administered by the Attorney-General's Department, only the first four of these mitigation strategies are mandatory for Non-Corporate Commonwealth entities (NCCEs).[13]

The CSCRC notes that a voluntary cyber health check is the preferred mode given the wide-ranging level of cyber maturity among Australian SMEs and as a low-cost option. However, for any small business entity procuring with government, the health check should be a requirement. This would incentivise uplift across a critical segment of Australia's economy and help bolster our national security in the face of growing cyber security threats. This should be considered the starting point, with a view to growing this requirement for any SME procuring with any of the 11 sectors encapsulated within the forthcoming CI/SoNS legislation given its pronounced focus on bolstered cyber security mechanisms.

[12] ASD Essential Eight cybersecurity controls not essential: Canberra | ZDNet
[13] Protective Security Policy Framework

However, in order to ensure significant uptake from SMEs, any such initiative should be accompanied by an ongoing public awareness campaign about what the health check does and does not do, the need for the health check, its market benefits and advantages, as well as the development of potential incentives to encourage SMEs to participate, given it will likely be considered as an onerous activity by many time-poor small businesses. Further, any such program should be subject to annual review, to ensure it remains fit-for-purpose considering the fast-moving nature of cyber security threats. Additionally, a health check program must be thoughtfully designed, with meaningful questions to ensure useful data is extracted. Such data would be a powerful tool for analysis to indicate key cyber security strengths and weaknesses across the Australian economy. This will have a corollary effect of informing the effectiveness of government policy. As with any health check, it is vital that SMEs have accessible resources once they have received the results of the health check otherwise this process risks becoming simply a paper exercise to assess risk with limited focus on tangible cyber security outcomes.

The CSCRC has observed in its interactions with business there is appetite for uplift but this is an area where clear and ongoing public messaging is required. Public awareness campaigns could be co-designed by government and industry and effectively rolled out to the public through viable public-private partnership models, with incentives on offer from industry. Government might consider looking to the BCA, as well as other well-known and cyber mature industry partners, such as leading Australian financial institutions and telecommunication providers, who could offer bundles and packages to participating small businesses to drive uptake. Additional partners might include local government councils (LGAs) who have oversight of their regional jurisdictions and engage extensively with local small business through well established business and marketing models. Government might also consider the establishment of various incentivisation programs to encourage business uptake, which could include measures such as tax breaks and instant asset write offs.

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 of consumers?

The CSCRC notes that further work should be done to develop effective policies concerning 'cyber harm', defined as 'the damage that arises as a direct result of an attack conducted wholly or partially via digital infrastructures, and the information, devices and software applications that these infrastructures are composed of".[14] These harms can manifest as physical or digital; psychological; economic; reputational and/social and societal. However, despite their very real effects, courts so far have struggled to measure cyber harms. In the United States, scholars have concluded that US "courts have been reaching wildly inconsistent conclusions on the issue of harm, with most courts dismissing data-breach lawsuits for failure to allege harm. A sound and principled approach to this is yet to emerge". However, they argue that courts can draw on legal precedent to recognise data-breach harms:

> *…there are ample conceptual foundations in the law to address risk and anxiety and thus to recognise data-breach harms. In some areas, the law has been developing gingerly in the direction of recognising concepts helpful to recognise data-breach harms; in other areas of the law, such concepts are widely accepted yet remain sequestered from similar kinds of harm in other contexts.*

Australian courts, thus far, have also struggled to recognise cyber harms, as in Australia there is no constitutional right to privacy although there is some existing case law. Currently there is no tort that recognises harm arising as a result of a privacy breach, although *The Privacy Act 1988* and state privacy legislation provide guidelines for the collection, correction, use and disclosure of personal information. The Federal Government might consider two key avenues for policy development concerning cyber harms: in 2014 the Australian Law Reform Commission (ALRC) released a report *Serious Invasions of Privacy in the Digital Era*[15] which made a number of recommendations, including a new tort in a new Commonwealth act along with a number of related recommendations. In addition, the OAIC Notifiable Data Breach Scheme (NDB), established in 2018, helps ensure the protection of personal information and applies to any organisation or agency covered by *The Privacy Act 1988*. Under the NDB, the Information Commissioner has a number of enforcement powers, which, although they have not been used widely thus far, they have been applied and, more importantly, recognise harm. For example, on 30 June 2020, the Commissioner made a determination in the case of ST and Chief Executive Officer of Services Australia (Privacy). The decision states:

> *I have the discretion under s 52(1)(b)(iii) to award compensation for any loss or damage suffered by reason of the interference with privacy. Subsection 52(1AB) states that loss or*

[14] Agrafiotis, Ioannis (2018). "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate". *Journal of cybersecurity (Oxford)* (2057-2085), 4 (1).
[15] Serious Invasions of Privacy in the Digital Era (ALRC Report 123) | ALRC

> *damage can include injury to the complainant's feelings or humiliation suffered by the complainant.*

and goes on to say:

> *I accept the evidence provided by the complainant's consultant psychiatrist stating that the disclosure caused her 'considerable distress'. I accept the evidence provided in the complainant's friend's statutory declaration that the complainant became more 'hypervigilant, fearful and anxious, and she would talk to me about her fears and how restrictive she feels in her daily life.' I accept this on the basis that the declarant's observations were that the complainant became more 'anxious' in the emotional sense, rather than a psychological disorder, as the declarant does not profess to be a mental health professional.*

In light of this, this CSCRC notes that while the law has progressed in relation to cyber harms, there is still more to be done. Legislation has failed to keep pace with technological developments and laws should be applied in the cyber world just as they are in the real world. Cyber harms are real and have tangible effects – such negative impacts should be recognised in law. A new Commonwealth tort that deals with privacy breaches in today's interconnected world would help provide clarity in what remains a legal grey area.