

The Australian Industry Group
Submission to Home Affairs'
Discussion Paper on Strengthening
Australia's Cyber Security
Regulations and Incentives



Contents

1. Introduction	4
2. Why should government take action?	8
3. The current regulatory framework	13
4. Governance standards for large businesses	24
5. Minimum standards for personal information.....	28
6. Standards for smart devices	32
7. Labelling for smart devices	36
8. Responsible disclosure policies	40
9. Health checks for small businesses	41
10. Clear legal remedies for consumers and other issues	42

About Australian Industry Group

The Australian Industry Group (Ai Group®) is a peak national employer organisation representing traditional, innovative and emerging industry sectors. We have been acting on behalf of businesses across Australia for nearly 150 years.

Together with partner organisations we represent the interests of more than 60,000 businesses employing more than 1 million staff. Our members are small and large businesses in sectors including manufacturing, construction, engineering, transport & logistics, labour hire, mining services, the defence industry, civil airlines and ICT.

Our vision is for thriving industries and a prosperous community. We offer our membership high quality services, strong advocacy and an effective voice at all levels of government underpinned by our respected position of policy leadership and political non-partisanship.

1. Introduction

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission on the Discussion Paper on strengthening Australia's cyber security regulations and incentives by the Department of Home Affairs (Home Affairs).

Ai Group's members represent businesses of all sizes and many sectors across Australia. As shown with COVID-19, many of these businesses are essential and contribute to our economy. While in many ways diverse, businesses have a common and collective interest to be cyber secure. Strong cyber secure and resilient businesses are central to customer trust. This includes protecting data privacy, competitiveness, the strength of our economy and the reliability of our infrastructure.

Ai Group has been supportive of the Government's release of its revised 2020 Cyber Security Strategy last year, reinforced in the 2020-21 Federal Budget with a \$1.7 billion commitment over ten years to invest in strengthening Australia's security through initiatives designed to improve cyber security.

In our 2019 submission to Home Affairs' 2020 Cyber Security Strategy Discussion Paper (2019 submission), we noted that cyber security threats continue to grow and evolve as a risk management issue for many organisations and their boardrooms, with news about data breaches and cyber security attacks becoming more mainstream.¹ If left unchecked, these can diminish corporate trust and reputation, business and consumer confidence, as well as disrupting business operations and provision of services. And in light of growing public awareness and scrutiny about data privacy and rights, it is important organisations ensure they are adequately meeting public expectations and level of trust. These threats are further compounded as organisations become more digitalised and connected through the internet.

These are certainly ongoing concerns for many. With more people working from home in light of the COVID-19 pandemic, there are new risks. The Government's announcement in June last year about malicious cyber activity against Australian organisations was a timely reminder that businesses and the community need to be vigilant during this time, and that cyber security is a shared responsibility.

This is especially the case when businesses also become victims. The Government has stated that cyber security incidents cost Australian businesses up to \$29 billion each year, with almost one in three Australian adults impacted by cybercrime. Recent reports released by the ACSC and ACCC highlight the impact of cyber security incidents. According to the ACCC, Australians lost over \$850 million to scams in 2020.² The ACSC indicates that it received almost 60,000 reports a year, or one report every 10 minutes – and bearing in mind those are only reported incidents, noting that cybercrime within Australia is underreported.³ These various reports also highlight the importance of proper coordination between various government agencies to assist businesses and individuals that are victims of cyber security related incidents.

It is also essential that any reforms that may arise as a result of this review do not result in excessive or overlapping regulation and that any additional obligations placed upon business recognise the importance of ensuring industry is not excessively burdened as the economy seeks to lift itself from the damaging impacts of the pandemic. It would also be a perverse outcome if reforms are proposed that do not address the underlying problem and root cause that could lead to unintended consequences.

Given the rapidly evolving state of cyber threats and attacks, it is essential that our nation is sufficiently resourced and supported through industry and government collaboration to ensure national security, and to protect businesses and the community against global cyber crime and related threats. Indeed, Ai Group works closely with Government and its agencies on improving Australia's cyber security.

¹ Ai Group submission to Home Affairs (November 2019), https://cdn.aigroup.com.au/Submissions/Technology/2020_Aust_Govt_Cyber_Security_Strategy_Discussion_Paper_1Nov_2019.pdf.

² ACCC, "Targeting scams: Report of the ACCC on scams activity 2020" (June 2021).

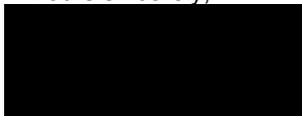
³ ACSC, "Annual Cyber Treat Report, July 2019 to June 2020" (September 2020).

In this context, we welcome our continued inclusion in close consultation with Home Affairs, along with relevant members covering a wide range of sectors and other stakeholders.

For the purposes of this submission, we respond to the specific questions that have been raised in the Discussion Paper, including recommendations for Government which build on the work of the 2020 Cyber Security Strategy (a summary of these recommendations is also included below). Where relevant, we also reiterate relevant points that we have previously raised in submissions. Given that several proposed issues and solutions have just been raised in this Discussion Paper, some of our views will be preliminary and there may be updated comments once further detail around proposals have been developed in the consultation process.

Should you be interested in discussing our submission further, please do not hesitate to contact me or our adviser Charles Hoang [REDACTED]

Yours sincerely,

A black rectangular redaction box covering the signature of Louise McGrath.

Louise McGrath
Head of Industry Development and Policy

Summary of recommendations

Below is a summary of our recommendations made in this submission in response to questions raised in the Discussion Paper.

Chapter 2: Why should government take action?

1. Government should properly assess the underlying problems and root causes for cyber security incidents, in addition to inhibitors to business investment in cyber security best practices.
2. Government should explore the current trends in business investment in cyber security and cyber security incidents through sources such as the ABS, ACCC, ACSC and OAIC.
3. Government should explore business behaviours and commercial drivers to invest by leveraging on activities that drive business uplift (including in cyber security) e.g. commercial contracts, export/trade activities, supply chain expectations, and Government driven activities in procurement and tender processes and business development initiatives such as the Entrepreneurs' Programme.
4. Government should give proper consideration to non-regulatory options to address inhibitors against businesses from properly investing in cyber security and respond to cyber security incidents.

Chapter 3: The current regulatory framework

5. Government should explore non-regulatory options to improve coordination and collaboration on cyber security activities between governments, regulators and industry.
6. Government should have regard to relevant cyber security matters arising from the critical infrastructure security reforms.
7. Government should review the following issues highlighted by the NDB Scheme, including through Government assistance:
 - Address the source of malicious or criminal attacks that lead to data breaches.
 - Publish more frequent OAIC NDB Scheme insights reports (e.g. annually) that may help to better inform policymakers with respect to privacy and cyber security policy.
 - Fund businesses with transition support to meet regulatory obligations associated with cyber security including NDB Scheme.
 - Develop policy options to assist businesses to mitigate data breaches from occurring in the first instance, including awareness and effective responses. This could entail further collaboration between industry and governments to co-design workable and practical remedies to increase cyber security capability, such as technological solutions and education and training programs.
 - Proper coordination between Government agencies to assist business victims of data breaches and cyber security incidents.
 - Ensure the ACSC is sufficiently resourced to meet the cyber security demands of industry and the community.
 - Undertake a public health approach through specific awareness campaigns targeted at industries that most often appear in the NDB Scheme reports.
8. For significant policy reforms especially associated with cyber security, we strongly encourage the Government to improve upon its consultation processes by building more time to properly consult and work with key stakeholders to co-design workable and practicable solutions to achieve mutual outcomes.

Chapter 4: Governance standards for large businesses

9. To help better inform on options to strengthen corporate governance of cyber security risk, Government should properly assess the underlying problems and root causes for cyber security incidents, and properly understand business inhibitors to investment in cyber security best practices.
10. To help support SMEs, Government could undertake the following:
 - Address general business issues around cyber security which should also benefit SMEs.

- Explore ways to alleviate business pain points associated with Government activities that require cyber security adherence and uplift.
- Harmonise cyber security standards requirements across the various inter- and intra-governmental procurement policies.

11. Government and industry should work together to develop a well-designed cyber security uplift program to support businesses.

Chapter 5: Minimum standards for personal information

12. In absence of substantiated evidence to the contrary, we do not consider that an adequate case has been made to introduce a new cyber security code under the Privacy Act.

13. Home Affairs should coordinate with the AGD on its review of the Privacy Act.

14. Any options under consideration will require further detail to be developed and should be properly consulted with stakeholders. It should also take into account considerations including (but not limited to) the importance of: a principles-based, technology neutral and non-prescriptive approach; a risk-based and proportionate approach; consistency with existing international standards and requirements as a baseline (wherever possible); and cost-benefits assessment.

Chapter 6: Standards for smart devices

15. Government should review key activities relating to standards for smart devices (as opposed to adopting Option 1 (Mandatory standard for smart devices) in the first instance). This includes allowing more time to properly review the voluntary *Code of Practice: Securing the Internet of Things for Consumers*, and understanding the barriers and options to improve its uptake.

Chapter 7: Labelling for smart devices

16. Government should undertake a proper contextual analysis of consumer issues and expectations to assess the materiality of consumer concerns and expectations as it relates to a proposed labelling scheme.

17. Before further consideration of a cyber security labelling scheme, the Government should take into account international lessons.

18. Government should develop other options to encourage consumers to purchase secure smart devices (as opposed to adopting in the first instance a cyber security labelling scheme under Option 1 or 2).

19. Should Government wish to proceed with cyber security labelling schemes, it should undertake a feasibility study of implementing such schemes, including (but not limited to) with respect to standards, assessment (including cost-benefits), certification, enforcement and complex global supply chains.

Chapter 8: Responsible disclosure policies

20. In absence of substantiated evidence to the contrary, we do not consider that an adequate case has been made to introduce a mandatory regime for responsible disclosure policy.

Chapter 9: Health checks for small businesses

See recommendations under Chapter 4.

Chapters 10 and 11: Clear legal remedies for consumers and other issues

21. In absence of substantiated evidence to the contrary, we do not consider that an adequate case has been made for further cyber security reforms associated with consumer protections.

2. Why should government take action?

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

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

2.1 Properly understanding the underlying problem and root causes

Before responding to Questions 1 and 2 in Chapter 2 of the Discussion Paper, we would like to provide comments regarding assumptions, and underlying problems and root causes that need to be properly understood.

The Discussion Paper suggests various factors that could come into play for why government should take action and why businesses are not always investing in cyber security. It also suggests that there are two categories of key market failures that may be preventing more widespread adoption of effective cyber risk management by business; namely, negative externalities and information failures. It also notes other factors including skilled workforce issues.

We agree that it is important to develop a better understanding of the factors or root causes that may inhibit investment in cyber security best practice. More significantly, however, it is also important to understand the factors that lead to cyber security incidents in the first place. Some of these incidents may not be within the control of businesses and may require other responses from external bodies such as Government.

However, we would be cautious against automatically assuming that a general reason for certain businesses not sufficiently investing in cyber security practices are due to intentionally behaving nefariously. For instance, the paper suggests technology companies may prioritise commercial interests over interests of their customers when it comes to cyber security. Another example in the paper suggests that due to the market power of major technology platforms and software companies, this may lead to these companies not being incentivised to offer secure products.

It is in businesses' commercial interests to protect the cyber security of their customers – this should not be perceived as a negative incentive. Moreover, each organisation will have its own requirements to assess risks, which will likely reflect their business considerations including shareholder and customer expectations. Therefore, controls that are in place for an organisation should depend on their risk management considerations.

We are sure that many businesses aim to do the right thing, but are vilified through reactive heavy-handed policy reforms if they become a victim of a cyber security incident, or are tarred with the same brush for the cyber security failures of others. At the centre of these issues is the role of state actors and their direct or criminal agents with high levels of capability and intent that have the capacity to undermine a nation state, let alone a business enterprise. It would be a particularly perverse outcome if a company that undertook reasonable cyber security measures were to be vilified or penalised for a cyber security breach.

In absence of substantiated evidence to the contrary, it would create a false dichotomy to generally suggest there are competing priorities between commercial and customer interests that lead to decisions that weaken cyber security.

Similarly, perceived power imbalances of digital platforms were also suggested as a basis for certain recommendations in the ACCC's Digital Platforms Inquiry Final Report. While well-intentioned, we were concerned about a general lack of evidence-based identification, analysis and assessment of

underlying root causes for purported issues and associated recommendations made in that inquiry.⁴

As an additional general comment that will likely also apply to other questions raised in the Discussion Paper, it will be critical that rigorous investigation be required for any recommendations that may arise from this review. The 2020 Cyber Security Strategy and work of the Industry Advisory Panel have played important roles in opening the conversation, and this Discussion Paper provides an opportunity of progressing the next phase of ideas for a deeper discussion. To progress these questions further, any recommendations should be developed through proper consultation with key stakeholders, analysis and assessment of issues, underlying root causes, and options to address these issues. A robust and considered cost-benefit assessment for any recommendations will also be required. In absence of these considerations, it is unclear whether any potential recommendations will provide material benefit to consumers and businesses in the long term, which may result in unintended consequences.

Recommendation:

- 1. Government should properly assess the underlying problems and root causes for cyber security incidents, in addition to inhibitors to business investment in cyber security best practices.**

2.2 Suggested factors

Notwithstanding our concerns above, we would like to suggest possible reasons why there may be inhibitors to investment in cyber security best practice for certain organisations in answer to Question 1 of the Discussion Paper.

In our 2019 submission, we touched upon potential reasons that may inhibit business investment in cyber security. We also suggested ways in which Government and industry could play a role in addressing such challenges.

In partnership with industry experts, Ai Group runs cyber awareness events for businesses from time to time. Based on the anecdotal feedback over the last several years, there appears to be a range of reasons for why there may be perceived barriers against proper cyber security investment which can be categorised into several areas: costs; priorities; resources and capability; and awareness and education.

Some businesses have told us that the cost to invest and implement cyber security measures is expensive compared to the risk of an attack. For example, for medium to larger size businesses, the cost of insurance against ransomware attacks or rebuilding a system containing critical data may be disproportionately more expensive or too difficult compared to the option of paying for a ransom.

For smaller businesses, the resources and capability to manage cyber security are likely to be limited – often little more than the use of basic cyber security technology, allocation of responsibility to an employee with general IT skills or an outsourced IT service provider.

The problem may be further exacerbated by a lack of awareness about good cyber security hygiene. An example was a local defence subcontractor who was infiltrated by a hacker several years ago, which made global news. According to reports, this local company lost a significant number of commercially sensitive documents for defence-related projects including the Joint Strike Fighter program.⁵ This incident had three particularly alarming features. Firstly, the company was made more vulnerable by a combination of several poor cyber hygiene practices, including use of very basic default passwords and old unpatched software. Secondly, the breach began in July 2016, was not discovered until November 2016, and only publicly reported in October 2017 (almost one year on). Thirdly, and of most concern, the company in question was a small engineering firm of about 50 employees, with just

⁴ Ai Group submission to Treasury (September 2019),

https://cdn.aigroup.com.au/Submissions/Technology/AiGroup_submission_Digital_Platforms_Inquiry.pdf.

⁵ ZDNet article, “Secret F-35, P-8, C-130 data stolen in Australian defence contractor hack” (11 October 2017).

one IT staff member, which could describe a great many Australian businesses. They may have thought “my business is too small to attract the attention of hackers”, which is a common response that we hear from smaller businesses.

Cyber capability churn in new software and firmware also creates a situation where enterprise systems have to be constantly updated to continue operation and new vulnerabilities are introduced as a consequence. This will be even more important with the rise of digital technology application use and limited support for obsolete products, leading to a potential increase in enterprise vulnerabilities.

Notwithstanding the above, we have seen improvements in business investment in cyber security. Of businesses previously surveyed by Ai Group, 79% indicated that they invested in cyber security measures in 2018.⁶ While our survey did not explore other drivers for cyber security investment, the higher proportion of businesses proactively investing in cyber security compared to our previous survey suggested a dramatic shift in business attitudes. This may possibly be due to increasing awareness about cyber management hygiene and incidents, and compliance with new privacy and data breach legislations such as the Notifiable Data Breaches Scheme and European Union General Data Protection Regulation (EU GDPR).

Separately, the ABS asked businesses about the importance of cyber security technology in 2017-18.⁷ The ABS data was less optimistic than Ai Group’s findings.⁸ A high proportion of businesses (46%) did not see any value at all, closely aligned with micro and small businesses (52% and 42%, respectively), compared to medium (23%) and large (8%) businesses. The accommodation and food services sector valued cyber security the least (no importance at 59%). Conversely, large businesses valued cyber security technology the most (major value at 52%), as well as the financial and insurance services sector (29%).⁹

Despite the differences between Ai Group and ABS data, there was still a proportion of businesses that did not invest or value the importance of cyber security technology or other measure. This suggests that either more work could be done to improve cyber security posture, or that some businesses feel they already have adequate levels of protection.

Arguably, the above statistics are based on past data and cyber security investment and awareness may have increased since that time. For instance, as more businesses have accelerated investment in digital technologies as an inadvertent response to the pandemic, there could have been an uplift in businesses’ cyber security capability.

In this regard, it will be important to continually review recent trends around business investment in cyber security, as well as cyber security incidents. Public sources such as the ABS, ACCC, ACSC and OAIC may be useful avenues to provide that information, as well as industry sources.

Complementing this, there may be an opportunity to better understand business behaviours and commercial drivers by leveraging on activities that may drive business uplift (including in cyber security) such as through requirements in commercial contracts, export/trade activities, and supply chain expectations. Government driven activities in procurement and tendering, and public funded business development initiatives such as the Entrepreneurs’ Programme may also provide some useful intelligence to policymakers.

⁶ Ai Group report, “The Fourth Industrial Revolution: Australian businesses in transition” (August 2019), https://cdn.aigroup.com.au/Reports/2019/AiGroup_Fourth_Industrial_Revolution_Report.pdf.

⁷ ABS, 8167.0 – Characteristics of Australian Business, 2017-18.

⁸ Ibid. Note: Differences in results between Ai Group and ABS survey data may reflect differences in sampling and data definitions. The ABS sample for *Business Use of IT* includes micro, sole trader and non-employed businesses. Ai Group survey samples exclude these very small and non-employed businesses.

⁹ Ibid.

Recommendations:

- 2. Government should explore the current trends in business investment in cyber security and cyber security incidents through sources such as the ABS, ACCC, ACSC and OAIC.**
- 3. Government should explore business behaviours and commercial drivers to invest by leveraging on activities that drive business uplift (including in cyber security) e.g. commercial contracts, export/trade activities, supply chain expectations, and Government driven activities in procurement and tender processes and business development initiatives such as the Entrepreneurs' Programme.**

2.3 Government support

Setting aside for the moment our concerns regarding assumptions made in the Discussion Paper with respect to negative externalities and information asymmetries, there are opportunities for Government to take action in the form of assistance to organisations to improve their cyber security in answer to Question 2 of the Discussion Paper.

In particular, a range of ways that Government can assist relate to both addressing inhibitors against businesses from properly investing in cyber security, and responses to cyber security incidents. While introducing mandatory regulation and legislation in diverse forms have been proposed as solutions by others in various forums, we suggest that there are non-regulatory measures that could be as, if not more, effective. These could especially target root causes than the symptoms, including where businesses become victims of cyber security incidents. Some of these were raised in our 2019 submission.

For example:¹⁰

- Businesses and individuals need to be better informed about good cyber security hygiene on an ongoing basis. This is especially important to manage high volume, low sophistication malicious activities that are continuously evolving. Raising cyber awareness through continuous education and training will be key to helping consumers understand how to protect their data. This is an area where support from Government and industry can play an important role. Ai Group continues to make continued efforts to improve business awareness about the laws and mitigating cyber security incidents. We always welcome the opportunity to continue working closely with Government and industry to elevate business awareness with useful information.
- It is positive that more organisations including Government departments and bodies have incorporated cyber security as part of their vernacular. However, further improvement is required to Government's coordination and engagement with industry and the community on cyber security matters. For instance, the ACSC's industry and community engagement activities should be commended and should be allocated with sufficient resources to ensure they are able to properly undertake their work.
- AustCyber's latest report on the state of the Australian cyber security industry includes a discussion about the cyber security skills growth challenge, noting that "while the skills pipeline has grown rapidly, maintaining momentum is critical".¹¹ We encourage Government to explore this further. For instance, there is an opportunity for Government to take leadership in developing a market for cyber security professionals by building capability within Government to tackle cyber threats. This will likely require employing skilled professionals. In the medium to long term, this could create another pathway for cyber security professionals to work in the private sector.

And while there may be valid comparisons between cyber security and safety for example in promoting good safety and cyber security hygiene within organisations, there are also important distinct differences that need to be appreciated. For example, if a cyber security incident occurs, a different

¹⁰ Further depth on each of the issues covered here can be found in our 2019 submission to Home Affairs.

¹¹ AustCyber, Australia's Cyber Security Sector Competitiveness Plan, 2020 Update (November 2020).

approach may be required, especially if the incident did not originate from within the organisation. In contrast to safety issues, cyber security incidents may be caused by external malicious criminal behaviour or foreign state actors. In those instances, it is important that law enforcement and other agencies are given the adequate resources to respond to such incidents as they would to non-cyber related crimes and attacks. As previously commented in our 2019 submission, given the rapidly evolving state of cyber threats and attacks, it is essential that our law enforcement bodies are sufficiently resourced, not only for protecting our national security, but also to protect businesses and the community against global cyber crime and other malicious actors.

Additionally, standards play an important role that can assist businesses. These are discussed later in this submission.

Recommendation:

- 4. Government should give proper consideration to non-regulatory options to address inhibitors against businesses from properly investing in cyber security and responding to cyber security incidents.**

3. The current regulatory framework

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

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

Questions 3 and 4 in Chapter 3 of the Discussion Paper are closely related so these have been discussed together in this section.

The Discussion Paper briefly discusses various existing forms of legislation and regulation associated with cyber security in terms of sector-specific, cross-sectoral and international related requirements. It also suggests that, due to existing Australian laws not originally intended to address cyber security, this has led to limitations in effectively addressing cyber security threats.

We agree that it would be prudent to properly consider each piece of legislation relevant to cyber security, including reviewing their strengths and limitations, and how they can be improved upon. We also support a holistic approach to properly understand how these legislations apply in the broader context associated with cyber security, which will help to avoid unnecessary duplication and conflict with various Government initiatives.

In this section, we provide a non-exhaustive list of examples of relevant pieces of legislation or regulation that are relevant to this discussion. We also discuss later in this submission on legislation associated with personal information (including the Privacy Act) in section 5 and Australian Consumer Law in section 10. However, before discussing particular relevant legislative and regulatory instruments, it is important to first consider the role of regulation.

3.1 General comment about regulation

In our 2019 submission, we discussed the need for better collaboration to respond to cyber security issues and understanding the role of regulation in this context. We consider that it is worth reiterating these points as they remain pertinent to this discussion.

It is critical that there is proper collaboration between Government and industry to tackle modern cyber security threats. Collaboration enables sharing of information about threats. It is therefore important that collaboration is encouraged in a safe environment where businesses can share threat information without being punished. This requires a light-handed approach by Government that encourages – rather than penalises – an environment of open collaboration. A collaborative environment can also be conducive to developing innovative solutions to counter cyber security and make us globally competitive.

As one member previously commented in relation to constraints to information sharing:

Understanding constraints and an open discussion on which are critical or negotiable would be of significant assistance in assuring effective delivery of cyber controls. Increased sharing of information, whilst taking into account risk and exposure of that information, will assist in a more effective and consolidated approach to cyber protection.

With respect to threat identification and management, traditional forms of regulation have been criticised for being inflexible and slow to respond to rapidly evolving threats and pace of technological change. Governments tempted to over-use these regulatory sticks need to consider a different approach if it wishes to achieve proper collaboration to tackle modern cyber security threats.

In practice, there may already exist activity in this area. However, we suggest there may be value in improving upon this, including having this done more consistently and integrated across all levels and

jurisdictions of governments and their agencies with industry.

For instance, further exploration could be given to a national “one-stop shop” or single whole-of-government point on cyber security to enable coordination on matters relating to regulation, guidance, reporting and compliance. This could also assist in collating the cyber security reporting that represents sector specific requirements, which would help reduce complexity and improve business, regulator and government performance.

As another example, in our submission to Home Affairs on the critical infrastructure reforms, member feedback suggested improvements could be made to the Critical Infrastructure Resilience Strategy and Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN) in the following areas that are relevant to cyber security:¹²

- Better alignment between Government departments, including DFAT, Home Affairs, Treasury and other Government agencies to drive improvements to more resilient infrastructure and national security protections.
- Collaboration between State and Federal Government departments and agencies. They all have an important role to play and removes duplication for participants.
- Jurisdictions being included in the TISN as the primary responders, which connects the Federal Government with industry in a much more meaningful and outcomes driven manner.
- Introducing other sectors to the TISN to create a more cross-functional and cross-sectoral representation of industry.
- Operationalising of segments or subgroups and functionally common informal networks in the TISN could enable greater agility and flexibility within the sectors.
- Prioritising flexibility within the TISN framework.
- Supporting the ongoing work plan of the Resilience Expert Advisory Group (REAG) to continue mapping exercises in the State jurisdictions, facilitating ongoing learnings, and the collection of much deeper and richer data, while continually building on the ecosystem approach.
- Improving the TISN to make it more relevant, given its large size. The ASD/ACSC’s forums are of very high value in terms of cyber security, but could be more focussed on cyber security and embedded in the TISN.

Regulation can also either make or break the growth of an industry at its early stages of development or going through a period of transition – in this case the Fourth Industrial Revolution. This also presents an even greater opportunity to provide an accelerated pathway to recovery from this pandemic. In this context, there are opportunities to build a cyber security industry as well as a *cyber secure* industry. The extent to which businesses are regulated can act as an investment barrier and diminish our attractiveness relative to other jurisdictions.

While regulation has a role in addressing reasonable public concerns such as around security, safety, privacy and environmental issues, there are also often alternative approaches to the regulatory stick. Regulatory barriers should only be introduced where there are clear net community benefits.

Depending on the identified policy issue, regulation may be an option, as well as non-regulatory measures. The issues need to be understood and developed further before an appropriate policy response can be considered.

¹² Ai Group submission to Home Affairs (September 2020), https://cdn.aigroup.com.au/Submissions/Technology/Dept_Home_Affairs_Critical_Infrastructure_Security_Reforms_Sept2020.pdf.

Unfortunately, we have been alarmed by a trend of heavy-handed interventions that seek to eliminate some forms of risk rather than manage them, while ignoring the risks and costs to innovation and the economy.

New or variations of sources of cyber related risk will continually arise, external to those currently identified. Legislation and regulation will likely not mitigate such risks. Further consideration should be given to more effective options. For example, it may be worth exploring further on whether an adaptive, principles-based resilience and security maturity model could assist in maintaining adaptive, responsive and agile capabilities.

Recommendation:

- 5. Government should explore non-regulatory options to improve coordination and collaboration on cyber security activities between governments, regulators and industry.**

3.2 Critical Infrastructure Security Reforms

The Discussion Paper notes that its work will build on the Government's critical infrastructure security reforms, which include cyber security considerations. It also discusses how these reforms are an example of sector specific legislation and suggests that these do not cover all businesses.

Overall, we support measures to improve the security and resilience of our critical infrastructure, with non-regulatory approaches as the default response before contemplating heavier forms of regulation. However, there remain outstanding concerns that need to be resolved with respect to these reforms. Once these are properly resolved, there will be relevant cyber security considerations with these reforms that would be worth considering in the context of this Discussion Paper.

For instance, while the critical infrastructure security reforms do explicitly target 11 critical infrastructure sectors that have been identified to be subject to the Security Legislation Amendment (Critical Infrastructure) Bill 2020, it has a potentially wider scope that may encompass many companies (directly or indirectly). For example, there remains a potential concern as to how the reforms might apply to companies that have diversified portfolios and operate, service or supply assets to a range of sectors identified under this Bill, including (but not limited to) suppliers, manufacturers and "data storage or processing" sector. There is also a potentially higher regulatory burden created for SMEs and those not currently subject to critical infrastructure security legislation. And there is also a need to understand the extent of entity responsibility based on what is within the entity's control (including scope of critical assets and supply chains), as well as related matters such as the scope of responsibility of an entity that may flow down the supply chain.¹³

More generally, it is fair to say that many engaged sectors and businesses are seeking to better understand the scope of the Bill and its impact on their particular businesses. The challenge with these reforms is providing meaningful comments on the impact (including regulatory costs) on a Bill that requires further detail. As one member previously commented, it is impossible to estimate costs of such measures without the detail.

There are a range of matters that remain outstanding with this Bill. For instance, the scope of the Bill will largely be contingent on clarifying its various aspects that may include (but not limited to) properly defining targeted entities and sectors, sector specific requirements, entity responsibilities and obligations, critical supply chains, critical assets, and a range of other matters that have been raised by stakeholders. Clarifying these should assist in providing more regulatory certainty for stakeholders that may be affected, and in better understanding the regulatory impact of the Bill such as potential costs. It should also help to minimise the risk of duplicating existing requirements and assist relevant

¹³ These are examples of matters that we raised (amongst others) in our submissions to the PJCIS in February and July 2021 concerning the uncertainty around the scope of these reforms. For further details, see our submissions to the PJCIS (Submissions No. 41 and 41.1): https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/SOCI/Submissions.

Government agencies (including regulatory bodies) in understanding their roles should such a Bill be implemented.

Amongst various suggestions and recommendations made in our previous submission to Home Affairs, we proposed a possible solution where a thorough gap analysis and assessment could be undertaken of the proposed obligations against existing obligations across the various sectors. This should assist sectors covered in this Bill, as well as for those that operate across sectors. Such a gap analysis may also include: assessment of the level of maturity of practices; access to required standards and competencies to ensure vulnerabilities are identified, understood and risk controls put in place; readiness to be regulated; expected baseline competencies; and access to supported competencies training. Once these are clarified for the various sectors, further consideration could be given to businesses that operate across sectors. If a gap analysis and assessment of requirements for each specific sector were to be undertaken, further consultation will be required with relevant stakeholders.

Recommendation:

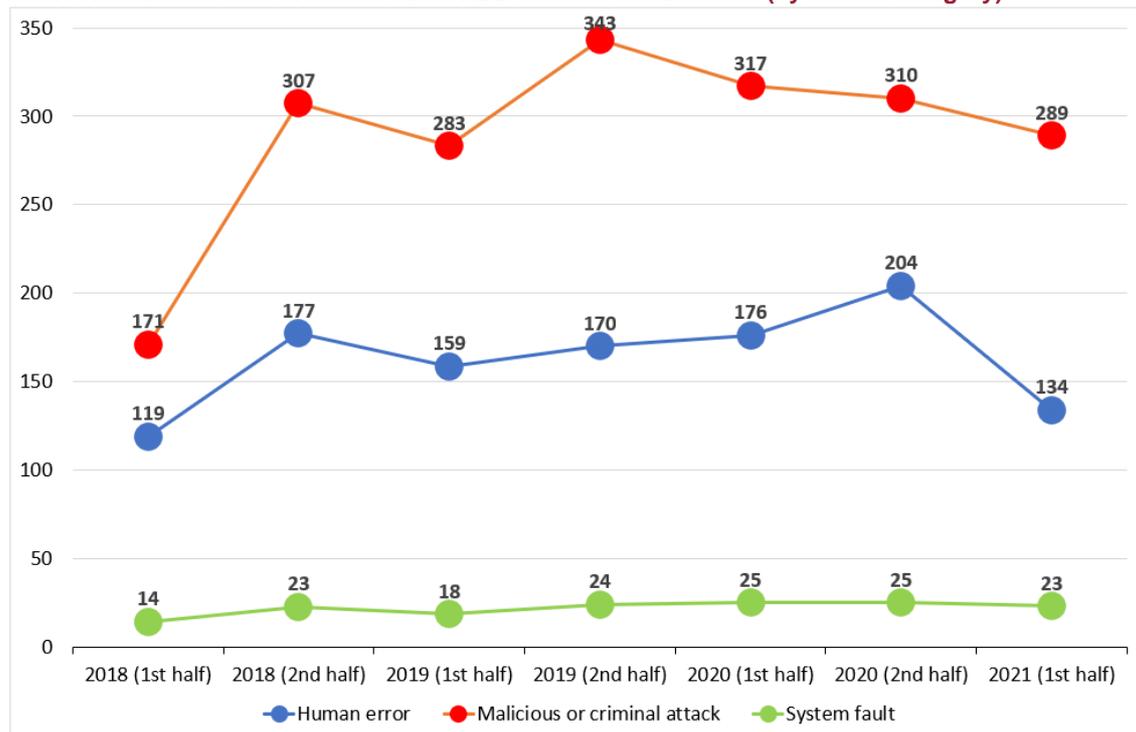
- 6. Government should have regard to relevant cyber security matters arising from the critical infrastructure security reforms.**

3.3 Notifiable Data Breaches Scheme

With respect to the Notifiable Data Breaches (NDB) Scheme under the *Privacy Act 1998* (Cth), we provided observations in our 2019 submission regarding the types of breaches reported in the various OAIC NDB Statistics Reports. Below we provide updated views regarding the Scheme. In short, while the Scheme may have been a useful source for analysing reasons for data breaches, more can be done to assist businesses in mitigating them from occurring in the first place.

Chart 1 below shows information on the number of data breaches reported to the OAIC since the NDB Scheme commenced.

Chart 1: Notifiable data breaches since NDB Scheme commenced (by breach category)



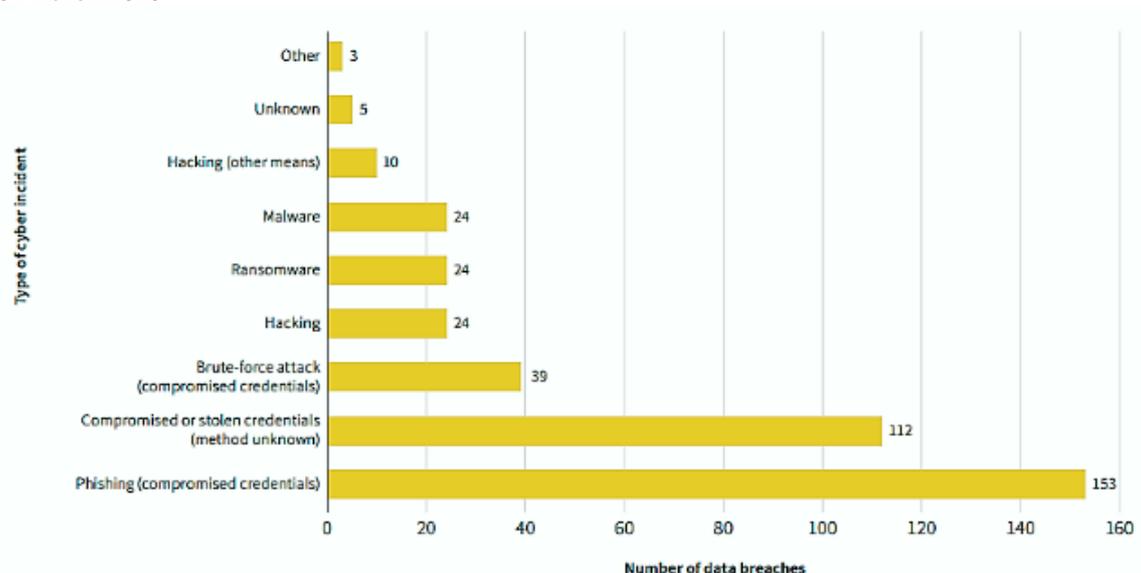
Source: OAIC

Since the NDB Scheme commenced in February 2018, it would be fair to say that there has been a consistent pattern of data breaches largely arising from malicious or criminal attacks, followed by human error. The OAIC's latest report for the January-June 2021 period notes that the majority of data breaches in the malicious or criminal attack category involved cyber security incidents (66%).¹⁴ Overall, 43% of all data breaches resulted from cyber security incidents.

By the end of June 2021, there were over 3,310 data breaches reported to the OAIC since the NDB Scheme commenced.¹⁵ Over this period, malicious or criminal attacks greatly contributed to these data breaches (61%), followed by human error (34%). System faults (5%) were rarely a factor.

Delving deeper into the data, the OAIC provided a breakdown of the types of cyber security incidents that gave rise to data breaches from the period of 1 April 2018 to 31 March 2019 (see Chart 2).¹⁶ For the same period, the OAIC also categorised the types of human errors and system faults that resulted in data breaches (see Chart 3).¹⁷

Chart 2: Notifiable data breaches caused by cyber security incidents, 1 April 2018 – 31 March 2019



Source: OAIC, Insights Report, 2019

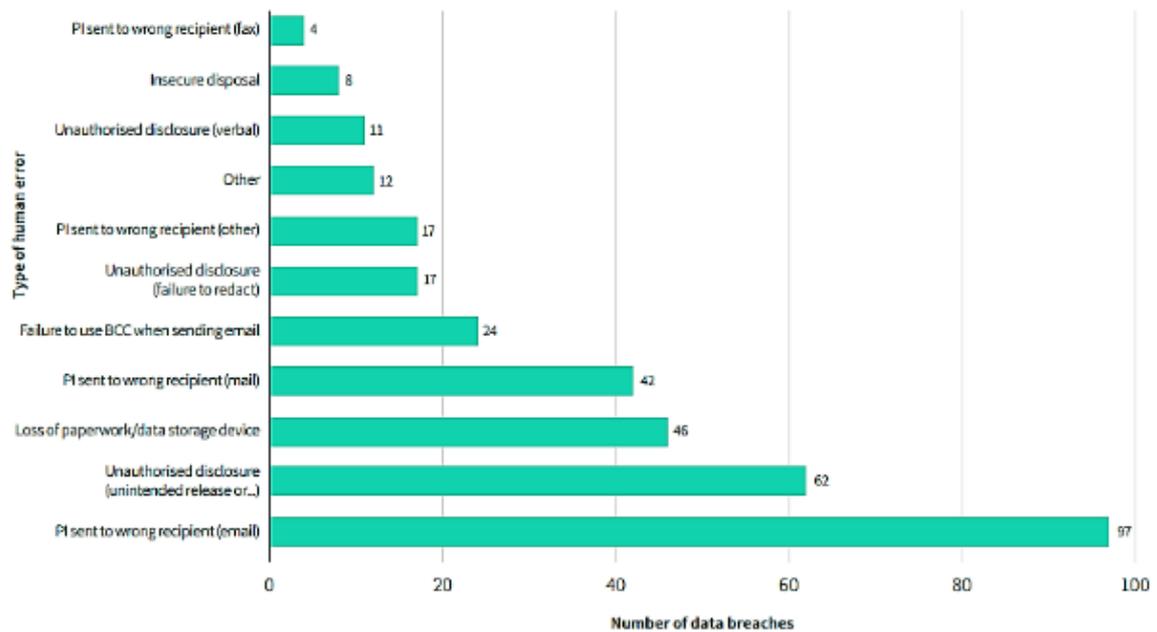
¹⁴ OAIC, Notifiable Data Breaches Statistics Report (1 January 2021 – 30 June 2021).

¹⁵ OAIC, Notifiable Data Breaches Statistics Reports (January 2018 – March 2018, 1 April – 30 June 2018, 1 July – 30 September 2018, 1 October – 31 December 2018, 1 January 2019 – 31 March 2019, 1 April 2019 – 30 June 2019, 1 July 2019 – 31 December 2019, 1 January 2020 – 30 June 2020, 1 July 2020 – 31 December 2020, 1 January 2021 – 30 June 2021).

¹⁶ OAIC, “Notifiable Data Breaches Scheme 12-month Insights Report” (Report, May 2019), p. 10.

¹⁷ Ibid, p. 12.

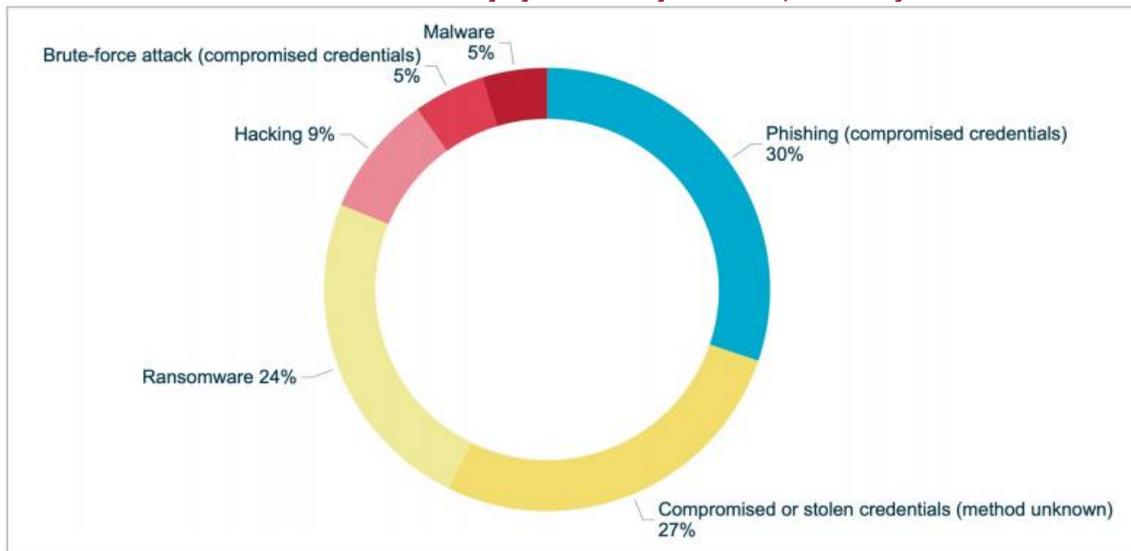
Chart 3: Notifiable data breaches caused by human error and system faults, 1 April 2018 – 31 March 2019



Source: OAIC, Insights Report, 2019

For completeness, the OAIC's latest report for the January-June 2021 period includes the most recent breakdown of the types of cyber security incidents (see Chart 4) and types of human errors that resulted in data breaches (see Chart 5).¹⁸

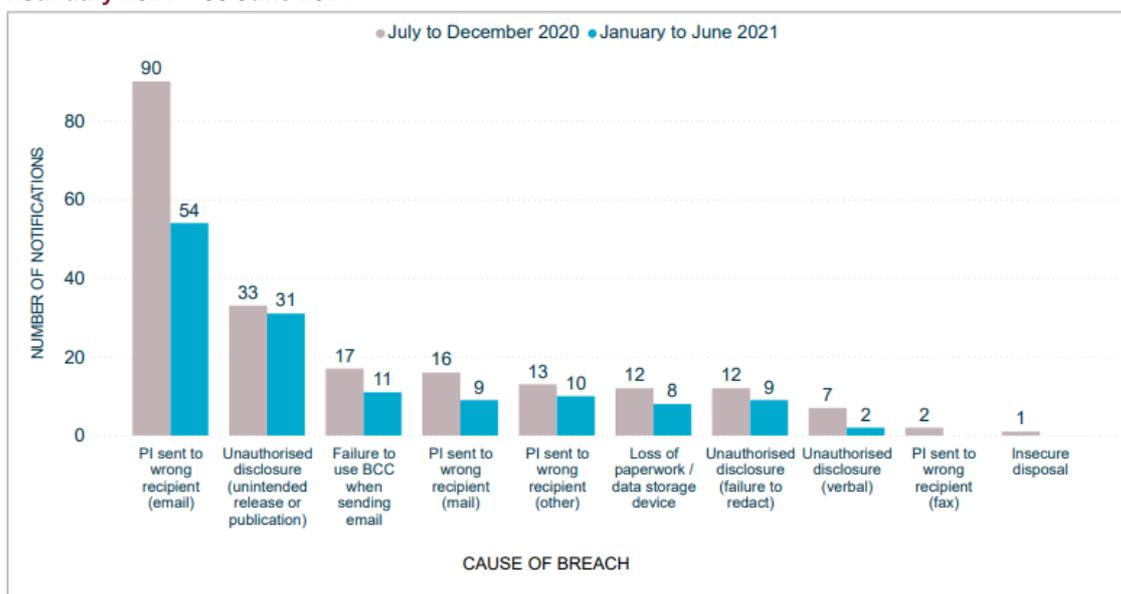
Chart 4: Notifiable data breaches caused by cyber security incidents, 1 January 2021 – 30 June 2021



Source: OAIC

¹⁸ OAIC, Notifiable Data Breaches Statistics Report (1 January 2021 – 30 June 2021), pp. 17, 19.

Chart 5: Notifiable data breaches caused by human error, 1 July 2020 – 31 December 2020 & 1 January 2021 – 30 June 2021



Source: OAIC

To some extent, these causes for data breaches point to the need for cyber security hygiene within organisations, as well as more general improvements in internal management of personal data to minimise human errors. According to a previous Telstra report, human errors were “often caused by inadequate business processes and employees not understanding their organisation’s security policies”.¹⁹

While improved business processes and human factor design of systems will help to reduce this component, a critical factor will require security awareness and practice of personnel. This needs to start at community and school levels to ensure that people entering the workforce are cyber security literate.

On the other hand, the higher proportion of data breaches arising from malicious or criminal attacks highlights an area where Government could provide support to address the source of these attacks.

As an aside, there may also be value if Government could support the OAIC to produce annual insights reports on the NDB, as it had initially done so 12 months into the commencement of the NDB. In addition to the ACSC’s annual cyber security threat reports, these OAIC’s insights reports may help to better inform policymakers with respect to privacy and cyber security policy.

Of the breaches reported to the OAIC since the NDB Scheme commenced, industries that have consistently appeared as top five sectors include: health service providers (21%); finance (14%); and professional services (legal, accounting and management) (8%).²⁰ Chart 6 provides a half-yearly breakdown of data breaches reported for these sectors.²¹ Given how much personal data are handled in these respective industries, this should be no surprise. Of greater concern is that these sectors provide service to other industries so others are not immune.

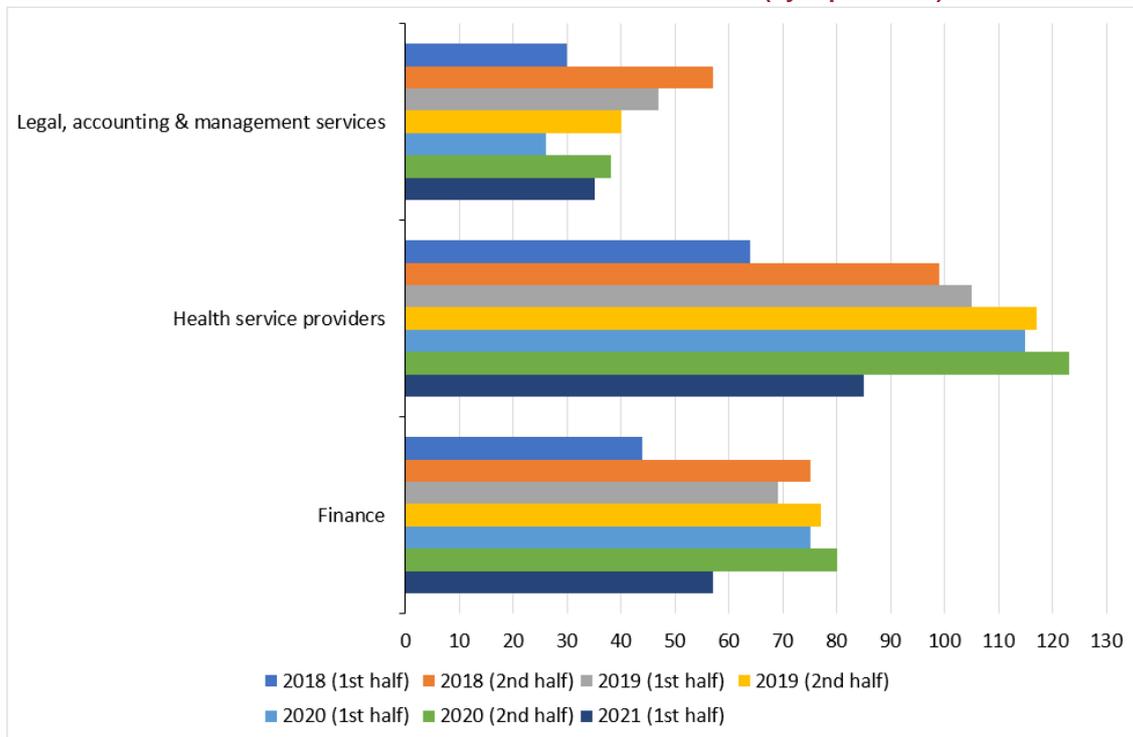
¹⁹ Telstra, “Breach expectation: the new mindset for cyber security success” (Article on Telstra website, April 2019).

²⁰ The education sector has also regularly appeared as a top five sector in the OAIC NDB Statistics Reports.

However, in the latest OAIC report, it was not in the top five.

²¹ OAIC, Notifiable Data Breaches Quarterly Statistics Reports (January 2018 – March 2018, 1 April – 30 June 2018, 1 July – 30 September 2018, 1 October – 31 December 2018, 1 January 2019 – 31 March 2019, 1 April 2019 – 30 June 2019, 1 July 2019 – 31 December 2019, 1 January 2020 – 30 June 2020, 1 July 2020 – 31 December 2020, 1 January 2021 – 30 June 2021).

Chart 6: Notifiable data breaches since NDB Scheme commenced (by top sectors)



Source: OAIC

The fact that there is a steady rate of data breaches being reported from a diverse range of industries highlight the need for additional government support.

As discussed above, the latest NDB Scheme analysis shows that a high proportion of data breaches are due to human error. Therefore, it is not only about having cyber security technology to mitigate data breaches.

We have received anecdotal feedback from businesses, especially SMEs, about the costs arising from new legislation such as the NDB Scheme. Other data and privacy legislations such as the EU GDPR and Consumer Data Right (CDR, which continues to be developed for specific sectors), as well as the controversial *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth), also present an additional regulatory burden and challenge for a range of businesses. Government support for businesses to meet these obligations may be required.

The NDB Scheme was introduced with an intention to reduce data breaches. While well-intentioned, the Scheme may only promote a compliance culture, as opposed to addressing the root cause e.g. a proper proactive leadership and risk management culture, and tackling the sources of malicious attacks. There are still questions as to how integrity and privacy measures and Government responses can be put in place to mitigate data breaches from occurring in the first instance.

In this regard, a policy or regulatory response is only effective if it properly identifies and targets the problem (especially underlying root cause) that it is trying to address. Automatically reaching for penalties may not be the most effective solution, and potentially creates a compliance-only mindset.

In other forms of regulation such as safety, business and governments have evolved over decades from pure compliance and concerns about over-regulation to a culture of risk management – this was partly driven by customer and supply chain expectations as they became more informed about safety.

However, while there may be similarities to safety in terms of promoting good security posture as noted earlier, there are distinct differences that may require a different approach in responding to cyber security incidents. The various reports from the ACCC, ACSC and OAIC highlight that businesses and

individuals are victims of cyber security related incidents. It is therefore important that there is proper coordination between Government agencies to assist these victims.

Rather than automatically reaching out for new regulatory instruments, further collaboration will be needed between industry and governments to co-design workable and practical remedies to increase cyber security capability, such as technological solutions and education and training programs.

Bodies such as the ACSC should be commended for working closely with organisations affected by cyber security incidents. However, as the ACSC has noted, this is help after the fact.²² The ACSC will also require sufficient resources to ensure that they can meet the demands from industry and the community.

Given that a large proportion of data breaches under the NDB Scheme have been triggered by malicious or criminal attacks and human error, it is important to tackle these causes and prevent breaches from occurring in the first place. For instance, while the OAIC suggested that awareness of the NDB Scheme appeared to be high, there remains a potential gap in awareness about mitigating data breaches, as well as responding to them effectively if they do arise.²³

As noted earlier, industries that consistently appear in the NDB Scheme reporting include health service providers, finance and professional services (legal, accounting and management). This suggests a targeted approach to cyber security awareness raising is worth considering – sometimes referred to as a “public health” approach where those most vulnerable are targeted with appropriate messaging. In this case, a specific awareness campaign could be developed that targets the industries that most often appear on the NDB Scheme reporting.

Recommendation:

7. Government should review the following issues highlighted by the NDB Scheme, including through Government assistance:

- **Address the source of malicious or criminal attacks that lead to data breaches.**
- **Publish more frequent OAIC NDB Scheme insights reports (e.g. annually) that may help to better inform policymakers with respect to privacy and cyber security policy.**
- **Fund businesses with transition support to meet regulatory obligations associated with cyber security including NDB Scheme.**
- **Develop policy options to assist businesses to mitigate data breaches from occurring in the first instance, including awareness and effective responses. This could entail further collaboration between industry and governments to co-design workable and practical remedies to increase cyber security capability, such as technological solutions and education and training programs.**
- **Proper coordination between Government agencies to assist business victims of data breaches and cyber security incidents.**
- **Ensure the ACSC is sufficiently resourced to meet the cyber security demands of industry and the community.**
- **Undertake a public health approach through specific awareness campaigns targeted at industries that most often appear in the NDB Scheme reports.**

3.4 TOLA Act

As raised in our 2019 submission, the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (TOLA Act) – while aimed at national security – raised public concerns about cyber security. The TOLA Act was rushed through Australian Parliament in 2018

²² OAIC, “Notifiable Data Breaches Scheme 12-month Insights Report” (Report, May 2019), p. 19.

²³ Ibid.

without full consideration of the impact that this could create for a broad range of stakeholders. Legitimate concerns about the legislation were raised from a broad range of stakeholders including industry, civil society, and technical and privacy experts. However, the Government response largely ignored the issues raised by passing the TOLA Bill without reflecting stakeholder concerns.

As a consequence, the TOLA Act potentially risks substantial damage (both real and perceived) to the security, credibility and reputation of Australia's connected systems and products and the businesses and people who use them. Such measures not only add potential costs to international business, but risk curtailing innovation and limiting the benefits of digitalisation to businesses and their customers. For instance, this may have created other unintended consequences, including Australia's image overseas in relation to trust in Australian products.²⁴ This has led to an outcome where businesses could be facing a heavier degree of regulatory burden and uncertainty compared to their competitors operating in overseas jurisdictions, with smaller businesses likely to be relatively worse off.

Most importantly, we are concerned that the TOLA Act could lead to the weakening of existing cyber security of businesses and its customers. As mentioned earlier, cyber security threats remain a growing and evolving risk management issue for many businesses. The introduction of the TOLA Act created an additional layer of risk, which may include impacting on the ability of Government and business to access international security and encryption products, making Australian businesses, Government agencies and the broader community vulnerable to cyber attacks and data breaches.

In this regard, we endorsed the Independent National Security Legislation Monitor's (INSLM) recommendations to its review of the TOLA Act, especially in relation to improved independent oversight, clarification of definitions, and improved transparency and accountability.²⁵ To date, issues with the TOLA Act remain outstanding.

In this example, industry has a mutual objective with Government to: protect Australians from crimes such as terrorism; enforce the law; and enable the intelligence, interception and enforcement agencies to effectively do so in a rapidly evolving digital environment. Protecting the security of communications and information between businesses and their customers is of fundamental importance. However, proper collaboration requires proper consultation by Government to ensure that the potentially broad impacts of the legislation are tested by exposure to a cross-section of industry and the broader community. Unfortunately, this did not occur in the development of the Act.

There are significant lessons that should be learnt from the negative industry and public experience with the TOLA Act, and avoid repeating them again.

Since that time, we note that there have been improvements in Government engagement with industry and Home Affairs should be commended in this regard. For instance, returning to the critical infrastructure security reforms, we have welcomed the consultative approach that Home Affairs has undertaken in holding virtual town halls and workshops.

That being said, however, the Bill for these reforms have not addressed various areas of uncertainty and it was premature to have this Bill tabled into Australian Parliament in December last year. We acknowledge that Home Affairs has been consulting through workshops concurrently to this Bill on sector specific rules with the electricity and gas sectors being the first sectors. This has now been followed by the data storage and processing, and water sectors. However, other identified sectors in the Bill are yet to be considered. Home Affairs has also this year consulted on generic governance rules, and critical asset definitions and rules. These concurrent consultations have been undertaken in

²⁴ For further details, see: Joint submission by Communications Alliance, Ai Group, AIIA, AMTA, DIGI and ITPA to PJCIS on "Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018" (Submission No. 23, July 2019), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Submissions; ASPI, "Perceptions survey: Industry views on the economic implications of the Assistance and Access Bill 2018" (December 2018), p. 3.

²⁵ For further details, see: Ai Group submission to the PJCIS on (Submission No. 23.1, July 2020), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Submissions.

anticipation of legislation being passed through Parliament.

Our preference would have been for these consultations, especially on sector specific requirements, to have occurred prior to the Bill having been tabled into Parliament. This may have assisted stakeholders to gain a better understanding of the specific requirements that may or may not apply to their specific sectors and businesses. Understandably, there have been many relevant and important questions and ideas raised by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and stakeholders during the PJCIS's public hearing about the Bill – this may be due to issues and options not having been properly worked through before it was tabled into Parliament.

Given these parallel consultations, there may also be confusion for all parties (including policy makers and stakeholders) regarding the order of reforms. For instance, should changes arise from the PJCIS's review, this could impact on Home Affairs' consultation and stakeholders may need to be consulted again. In our submission to Home Affairs on its Draft Critical Infrastructure Asset Definition Rules consultation in May 2021, we suggested that there should be time allowed for the PJCIS's review to be completed before other related consultations arising from the Bill commence.

Recommendation:

- 8. For significant policy reforms especially associated with cyber security, we strongly encourage the Government to improve upon its consultation processes by building more time to properly consult and work with key stakeholders to co-design workable and practicable solutions to achieve mutual outcomes.**

4. Governance standards for large businesses

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

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

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

Chapter 4 of the Discussion Paper discusses feedback provided to Government and a Government desire for large businesses to improve their management of cyber security related risk. The Paper therefore seeks ways to encourage stronger cyber security risk management within large businesses, noting smaller businesses are much less likely to have these processes in place or employ dedicated cyber security teams. It also puts forward three policy options, namely: maintaining the status quo (Option 0); setting voluntary governance standards for larger businesses (Option 1); and setting mandatory governance standards for larger businesses (Option 2).

4.1 Properly understanding the underlying problem and root causes

In the first instance, in order to respond to Question 5 of the Discussion Paper (similar to the other questions raised), it is important to first properly understand the underlying problems and root cause that the governance standards are aiming to address.

We would be generally opposed to Option 2, noting our comments above regarding the role of regulation and preference towards non-regulatory measures. For instance, we have discussed issues of creating a compliance mindset in cyber security, which is generally synonymous with introducing mandatory obligations. An example provided was the NDB Scheme. A compliance-based approach would not be conducive to instilling a culture which supports good cyber security practices and mitigating breaches from occurring in the first place. Instead, it shifts a regulatory burden on businesses without giving them the proper assistance to address an underlying problem (assuming that is within their control). A mandatory approach also treats the victim (in this case the business) as the malicious actor by attaching penalties for non-compliance, where a proportionate regulatory response should be to target the originator of the incident (e.g. malicious or criminal attacker).

With respect to Options 0 and 1, these may or may not be optimal solutions. If there are areas identified that can be improved upon that is not currently being addressed by Government or industry, Option 0 may not be a viable solution.

Similarly, Option 1 may not be the preferred approach if there are a range of non-mandatory solutions available that is not limited to governance standards, but would still require further support that is not covered in Option 0. For example, there may be benefit in: increasing industry awareness of existing standards and other industry best practices; connecting to existing obligations or harmonising them across sectors; and improving cyber security capability uplift through increased and targeted awareness campaigns, education and training, and sufficiently resourcing Government agencies to support businesses.

Recommendation:

- 9. To help better inform on options to strengthen corporate governance of cyber security risk, Government should properly assess the underlying problems and root causes for cyber security incidents, and properly understand business inhibitors to investment in cyber security best practices.**

4.2 Properly understanding the SME and supply chain security

In responding to Question 6 of the Discussion Paper, the Paper initially suggests that the three options proposed are only targeting large companies. However, SMEs may be automatically captured through their engagement with larger companies through supply chains, or depending on how large companies are defined. The link between SMEs and supply chains are acknowledged in Chapter 10 of the Discussion Paper.

Supply chain security

If the objective is to promote cyber security and resilience, it is imperative that a secure organisational ecosystem is not limited to within an organisation's own boundaries but extend to its supply chain or partner network. However, it is also important that proper consideration is given to what is within an organisation's reasonable control. We raised a similar issue in the critical infrastructure security reforms, and suggested that there should be flexibility for those along the supply chain to have their own processes in place to determine their critical assets and a best endeavours approach could be considered.

In our 2019 submission we briefly touched upon supply chain security in terms of trust. For example, the Charter of Trust initiative brings together several major global companies who have signed up to a range of principles for establishing trust around cyber security with their customers and partners.²⁶ Consideration could be given as to whether a similar charter could be developed in Australia.

Another way to build trust, especially in the supply chain, is through a chain of custody (CoC) approach, which some companies currently use. If CoC is too difficult to establish, then alternative approaches could be explored such as developing a trusted supplier list.

We also discussed standards more generally, which may equally apply to supply chain security. Standards are discussed in more detail in section 6 of this submission.

SME support

For smaller businesses, we discussed earlier about their resources and capability limitations to manage cyber security. We also highlighted that smaller businesses are likely to be relatively worse off compared to larger businesses when new regulatory obligations are introduced. And the cost impact of cyber security incidents on business victims are relatively more significant for smaller businesses. In short, many of these issues apply to businesses of all shapes and sizes, but the relative impact will be felt even more significantly for smaller businesses.

We also briefly discussed in section 2 about opportunities to better understand business behaviours and commercial drivers to invest in cyber security by leveraging on activities that generally drive business uplift. This exercise could equally help to provide a better understanding of SMEs' needs and drivers, and provide them with the appropriate support.

In section 2, we also suggested factors that might inhibit businesses to invest in cyber security and ways in which Government can provide support to industry. Section 3 also touched upon ideas such as funding businesses with transition support to meet their regulatory obligations associated with cyber security including NDB Scheme. SMEs would naturally benefit if Government provides support for all businesses.

Building further on these ideas, it would be valuable to explore ways to alleviate business pain points associated with Government activities (e.g. regulatory reforms, procurement activities). For example, elaborating further on funding businesses to meet new compliance requirements, this could include providing cyber security uplift such as education and training, compliance assessment, cyber security assessment, and cyber security investment. Such a cyber security support scheme could offer a range of security services and capabilities that can be accessed by businesses at a subsidised cost (i.e.

²⁶ The Charter of Trust can be accessed here: <https://new.siemens.com/global/en/company/topic-areas/cybersecurity.html>.

either no or minimal cost).

We have also heard anecdotally of specific problems for businesses having to comply with multiple cyber security standards if they are (or want to be) involved in various government procurement projects. This problem appears to be prevalent across various government levels and jurisdictions. For businesses (from SMEs to large) wishing to tender for various government projects, meeting multiple cyber security standards can become a very costly exercise and inadvertently an even greater barrier for SMEs in being given full and fair access to government procurement. Therefore, it would be greatly beneficial if the various cyber security standards requirements across the various government agencies and jurisdictions could be harmonised. We discuss standards harmonisation further in section 6 of this submission.

Recommendation:

10. To help support SMEs, Government could undertake the following:

- **Address general business issues around cyber security which should also benefit SMEs.**
- **Explore ways to alleviate business pain points associated with Government activities that require cyber security adherence and uplift.**
- **Harmonise cyber security standards requirements across the various inter- and intra-governmental procurement policies.**

4.3 Education and awareness for senior business leaders

With respect to Question 7, the value of education and awareness as part of a package of providing cyber security uplift including for senior business leaders should not be underestimated. As with any continuous learning required in many modern professions, senior leaders are expected to manage the latest threats and risks to ensure their business remain competitive, sustainable and resilient. As cyber security is a continually evolving issue for many businesses, it is important that their businesses including leaders and employees are adequately equipped through regular awareness and training.

For example, the World Economic Forum published a white paper that explored a range of considerations for Boards to take action on cyber security and resilience including principles and tools, which may be informative to this discussion. On training and awareness, questions that the paper raises include:²⁷

- *Do new board members receive cyber resilience general orientation? (This should include a general training of the subject matter in order to have a foundational understanding of the subject matter and their oversight responsibilities over the subject matter.)*
- *Are regular updates on general cyber resilience given? (The board should receive periodic training, e.g. annually, on cyber resilience and when significant threats or risks are identified that are industry specific in order for the members to have a good command of the subject matter. This regular/annual update may be accomplished by leveraging the enterprise's current awareness programme.)*
- *Is cyber resilience awareness incorporated at all levels and operational elements across the enterprise? How are resources allocated to make this possible?*
- *Is there an evaluation of cybersecurity culture and awareness among employees and are resulting action plans communicated to the board?*

Ai Group has run a series of awareness and training activities with support from industry experts

²⁷ World Economic Forum, "Advancing Cyber Resilience: Principles and Tools for Boards" (White Paper, January 2017).

around cyber security over the last several years. We would welcome working with Government and industry to ensure businesses receive the most benefit from a well-designed cyber security uplift program.

Recommendation:

- 11. Government and industry should work together to develop a well-designed cyber security uplift program to support businesses.**

5. Minimum standards for personal information

Question 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?

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

Question 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 5 of the Discussion Paper notes that feedback suggested certain best practice cyber security controls be adopted and one way to encourage their uptake could be through technical standards. The Paper also discusses Australia's slowness and barriers to adopt cyber security standards. However, the chapter and questions are focused on privacy (particularly personal information) and its association with cyber security standards and codes.²⁸ It presents two options for consideration, namely: maintaining the status quo (Option 0); and creating an enforceable cyber security code for personal information (Option 1).

In this section, we specifically respond to Question 8 in the Discussion Paper.

Continuing from section 3 of this submission where we discussed the role of regulation and relevant legislative and regulatory instruments related to cyber security, it is important to first understand the effectiveness of the current privacy legislation and other related regimes in order to respond to Question 8 of the Discussion Paper.

5.1 Effectiveness of current privacy requirements

As noted in the Discussion Paper, the Attorney-General's Department (AGD) is currently undertaking a review of the Privacy Act. This follows from the Australian Government's consultation on the Final Report of the ACCC's Digital Platforms Inquiry, which included a range of recommendations associated with reforms to the Privacy Act.

Overall, industry recognises the importance of protecting customer information and data, and supports a data and privacy regime which can benefit both customers and businesses through outcomes such as improved transparency and customer experience.

Our extensive submission to the AGD covered a range of questions raised in its Issues Paper.²⁹ However, for the purposes of this submission, we focus particularly on our discussion about cyber security and the effectiveness of the Privacy Act in general.

On the specific subject of cyber security as it relates to the Privacy Act, we have discussed in section 3 about the NDB Scheme, especially in terms of its impact and effectiveness, and where Government could assist in providing cyber security support.

With respect to the effectiveness of the Privacy Act, we note that a general criticism about regulation is that it is too slow and inflexible to adapt and respond to technological change. Cyber security could

²⁸ It is important to note that a privacy breach, regardless of its magnitude, is one of several consequences that could arise from poor security practice, inappropriate technology use, or a new or unexpected capability of a malicious actor.

²⁹ Ai Group submission to AGD (November 2020), <https://www.ag.gov.au/sites/default/files/2020-12/ai-group.PDF>.

be considered an example of this. Thoughtful strategy and credible policy responses from governments and regulators are important to plan for and respond to economic and technological change in ways that will meet community expectations.

A principles-based approach to privacy regulation, as currently reflected in the Privacy Act, is flexible enough to enable future proofing and therefore technology neutrality in a rapidly changing environment. This strikes the appropriate balance between protecting the privacy of individuals and regulating businesses.

As the former Privacy Commissioner, Karen Curtis, stated:³⁰

By encouraging organisations to recognise the business advantages of good personal information handling practices and regulating their behaviour accordingly, government regulators can minimise regulatory intervention and red tape. This has been a common theme of our regulatory approach where a legislative framework is balanced by an emphasis on business privacy awareness and self-regulation. The idea is to inculcate the values and objectives of privacy law in business rather than just the superficial rules. When this happens organisations will be better equipped to deal with technological change because they will understand the ideas behind the laws – the principles – and will not become as confused by detailed technology-specific regulations.

In reference to the former Commissioner's remarks, the ALRC concluded:³¹

In this way, principles-based regulation aims to minimise the need for enforcement by 'encouraging organisations to understand the values behind the law and change their behaviour accordingly; not because they might get caught out by a regulator, but because they understand why the law is there and what its objectives are'.

In contrast, an alternative to principles-based regulation (i.e. prescriptive regulation) runs the risk of stifling innovation and making Australia less competitive compared to its more advanced peers. Regulation should be drafted to allow it to be nimble and flexible rather than overly prescriptive and heavy handed in the first instance. Therefore, we would be concerned if there were to be broader reform of the privacy regime that shifted from the current flexible principles-based regulatory approach.

Therefore in relation to this Discussion Paper, we would be cautious against introducing a new regulatory mechanism such as a cyber security code that would be another addition to existing regulatory requirements.

In absence of substantiated evidence to the contrary, we do not consider that an adequate case has been made to introduce an additional regime in addition to the existing arrangements.

5.2 Multiple approaches to personal information

Amongst the range of issues discussed regarding personal information in the AGD's review, we raised the issue of multiple approaches to personal information and the additional complexity if the definition were to be changed. An additional cyber security code proposed in the Discussion Paper will likely create additional complexity to an already overcrowded landscape of regulation and topic that is subject to current reform.

Further, as the Privacy Act is currently under review by the AGD, we suggest that it would be premature and risk duplicating work in this area to introduce additional reforms from Home Affairs. However, we would strongly encourage Home Affairs and the AGD to coordinate together on these matters as part of that review.

As noted in our submission to the AGD, questions remain on how changing the definition of personal information will fit with other multiple forms of regulation in this area, including the CDR and industry specific regulations. Making changes to the definition of personal information will likely create additional complexity and uncertainty.

³⁰ ALRC, "For Your Information: Australian Privacy Law and Practice" (Report 108, August 2008), p. 237.

³¹ Ibid.

We have also raised this issue during Treasury's inquiry into the future direction for the CDR.³² Using the banking sector as an example, with the introduction of the CDR, there now exists the Australian Privacy Principles (APPs) regime under the Privacy Act and the CDR Privacy Safeguards regime under the *Competition and Consumer Act 2010* (Cth). This effectively creates a dual privacy regime, with regulatory oversight of the CDR Privacy Safeguards by the ACCC and OAIC. Such an outcome creates complexity and compliance costs for businesses that have to comply with both regimes, and also for small businesses that may not currently be subject to the Privacy Act and therefore not familiar with privacy regulatory regimes.³³

To help clarify these new requirements, the OAIC consulted with stakeholders about its CDR Privacy Safeguard Guidelines. The Government allocated \$90 million in its 2018-19 Budget and 2018-19 MYEFO over five years for the OAIC and other relevant agencies to ensure that they can properly administer the new regime.³⁴ Subsequent funding for the CDR rollout has included an additional \$28.6 million in 2020-21 in the 2020-21 Budget, and \$111.3 million over the next two years in the 2021-22 Budget.

However, more can be done to support industry. Proper cost-benefit assessments need to be undertaken including compliance cost impacts on industry. With respect to multiple privacy and data regimes, there may be no additional benefit of protecting the privacy and security of consumers through the CDR, while creating an additional compliance burden on businesses. Government should consider ways to alleviate such regulatory burdens.

Alternative approaches do not appear to have been properly considered before the Final Report's recommendation was made. For example, instead of immediately resorting to changing the legal definition for personal information, a solution could be for the OAIC to provide additional guidance around the existing definition on a case-by-case basis. Such an approach would be a more proportionate response to address issues of legal uncertainty, without creating an unnecessary regulatory burden for businesses.

5.3 EU GDPR

In addition to the Australian privacy and data regulatory regimes, the Discussion Paper briefly mentions the EU GDPR and suggests that a 2020 UK review found a large proportion of organisations with improved cyber security to some extent as a result of its introduction.

In the Final Report for the Digital Platforms Inquiry, the ACCC made several recommendations to adopt privacy reforms similar to the EU GDPR. The AGD's Issues Paper subsequently discussed these recommendations, including the contemporary definition of personal information which it considered may be achieved by aligning it with the definition of personal information in the EU GDPR. Our submission to the AGD provided specific comments regarding that issue, as well as a range of other recommendations that referred to the EU GDPR.

However, for the purposes of this submission, we would like to offer a general comment regarding the EU GDPR and highlight issues that may arise in considering the GDPR that Home Affairs should be cognisant of:

- Some businesses may be subject to and compliant with the GDPR; if the privacy regime is changed to align with the GDPR, there may be an assumption that the regulatory burden would be minimal for businesses. But not all businesses, including smaller businesses, are subject to the GDPR and will likely see a greater regulatory burden and create a competitive disadvantage.
- For businesses compliant with the GDPR, there is a false economy if an ACCC recommendation

³² Ai Group submission to Treasury (June 2020), Link:

https://cdn.aigroup.com.au/Submissions/Technology/Treasury_CDR_Inquiry_5Jun_2020.pdf.

³³ OAIC, "OAIC commences consultation on draft CDR Privacy Safeguard Guidelines" (Media release, 17 October 2019).

³⁴ Treasury, "Consumer Data Right Overview" (Booklet, September 2019), p. 6.

varies from the GDPR. This issue was discussed further in our submission to the AGD in the context of consent requirements.

- The GDPR operates in a very different legal framework than Australia's Privacy Act and relies on different administrative and enforcement structures. For these reasons, it cannot simply be implemented into Australia.
- Given the GDPR is relatively new, the Centre for Information Policy Leadership identified unresolved issues and challenges with the GDPR one year after it commenced operation, "where organisations feel the Regulation has not lived up to its objectives and has presented practical difficulties, despite their dedication to implementing the new requirements".³⁵ The International Association of Privacy Professionals also found more work was still required for companies to comply with the GDPR.³⁶
- The potential impact of any GDPR type reforms to Australian businesses must also be carefully assessed. We should learn from the successes and failures of the GDPR and consider the real impact the GDPR has had on individuals and businesses in Europe and elsewhere. We should not simply align to the GDPR where its scope and potential impact is unclear or untested, or where requirements are overly cumbersome with limited positive impact on privacy protection.

5.4 Relevant standards

With respect to standards relevant to privacy, there already exists standards (especially international) and initiatives to support industry standards that may address or respond to the issues raised in this Discussion Paper. For instance, Standards Australia's AI Standards Roadmap includes references to such standards.³⁷ Also, international standards such as ISO 27000 series and from the NIST provide more than adequate guidance. Alignment with such international standards, complemented by other best practice guidance such as the Australian Information Security Manual could significantly help to reduce the need for mandatory regulations.

Noting our caution regarding a proposed new cyber security code under the Privacy Act, we consider that any options proposed by Government will require further detail to be developed and should be properly consulted with stakeholders. It should also take into account considerations including (but not limited to) the importance of: a principles-based, technology neutral and non-prescriptive approach; a risk-based and proportionate approach; consistency with existing international standards and requirements as a baseline (wherever possible); and cost-benefits assessment.

Standards are discussed further in section 6 of this submission.

Recommendations:

- 12. In absence of substantiated evidence to the contrary, we do not consider that an adequate case has been made to introduce a new cyber security code under the Privacy Act.**
- 13. Home Affairs should coordinate with the AGD on its review of the Privacy Act.**
- 14. Any options under consideration will require further detail to be developed and should be properly consulted with stakeholders. It should also take into account considerations including (but not limited to) the importance of: a principles-based, technology neutral and non-prescriptive approach; a risk-based and proportionate approach; consistency with existing international standards and requirements as a baseline (wherever possible); and cost-benefits assessment.**

³⁵ Centre for Information Policy Leadership, "GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges" (May 2019).

³⁶ International Association of Privacy Professionals, "GDPR compliance: Hits and misses" (May 2019).

³⁷ Standards Australia, "Artificial Intelligence Standards Roadmap: Making Australia's Voice Heard" (March 2020).

6. Standards for smart devices

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

Question 12: Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt for as a standard for smart devices?

- a. If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate?
- b. If not, what standard should be considered?

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

Question 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?

Question 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 6 of the Discussion Paper discusses about the vulnerability of smart devices and suggests these are partly due to information asymmetries and negative externalities. It discusses about Government action around this area including its voluntary *Code of Practice: Securing the Internet of Things for Consumers* (IoT Security Code of Practice) and complementary ACSC advice, its research on industry responses to the IoT Security Code of Practice, and international activities around mandatory standards or labelling. Finally, it discusses options to implement cyber security standards for smart devices in Australia, namely: maintaining the status quo (Option 0); and setting a mandatory standard for smart devices (Option 1).

In this section, we specifically respond to Question 11 in the Discussion Paper.

6.1 Understanding Australian and international context

Firstly, we note that the Government's IoT Security Code of Practice has only been in operation since September 2020 and it may still be premature to properly assess its effectiveness. For example, the problems noted in the Discussion Paper could be due to a lack of industry engagement and awareness, which could be resolved through increased collaboration with industry. Nevertheless, the Paper presents an opportunity to explore further on matters associated with standards more generally.

While we supported Home Affairs' intent for the IoT Security Code of Practice to operate as a voluntary mechanism,³⁸ we previously noted that it was important to consider its appropriateness in the Australian context. This was especially given that the Code of Practice was modelled on a UK approach.

Further, we support a security-by-design approach underpinned by principles, with the ultimate objective to protect Australia's cyber security. In this context, governments should reinvigorate and promote best practice regulation initiatives, by taking into account existing business practices and study global best practices in regulation and business support that encourage – rather than inhibit – innovation and productivity.

³⁸ UK Government, *Code of Practice for Consumer IoT Security* (October 2018).

For instance:

- In Home Affairs' consideration of an IoT Security Code of Practice, it was not clear whether consideration was given to the effectiveness of existing industry and internal business practices in Australia. For example, one manufacturing member tested their IoT system against a global reference, the Open Web Application Security Project (OWASP), which includes top ten things to avoid relating to security in IoT systems.³⁹
- The specific products and services targeted in the IoT Security Code of Practice may be supplied to the Australian consumer market from regions overseas, which might differ from the UK market. It is important to consider the relevant best practices that have been adopted from originating countries that supply products and services to the Australian market. Input from other government agencies already engaged internationally on promoting cyber security development may be of valuable assistance. These include AustCyber and the Ambassador for Cyber Affairs and Critical Technology.
- There is an opportunity to promote relevant existing cyber security standards and explain how they apply to products, services and supply chains. For instance, there are international forums such as ISO/IEC and NIST that have developed standards applicable to security-by-design, which appear to be missing from Home Affairs' considerations. These include:
 - ISO/IEC:
 - ISO/IEC 27000 series of standards
 - ISO 31000:2018 *Risk Management*
 - ISO/IEC 27701:2019 *Security Techniques*
 - NIST:
 - NISTIR 8228 *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* (Jun 2019)
 - Draft NISTIR 8267 *Security Review of Consumer Home Internet of Things (IoT) Products* (Oct 2019)
 - NISTIR 8259 *Foundational Cybersecurity Activities for IoT Device Manufacturers* (May 2020)
 - NIST SP 800-53 Revision 5 *Security and Privacy Controls for Information Systems and Organizations* (Sep 2020)

In addition to the above standards, we note that the top three principles of the Government's IoT Security Code of Practice are similar to the top three requirements of ETSI EN 303 645 i.e.: no duplicated default or weak passwords; implement a vulnerability disclosure policy; and keep software securely updated. We also note that Government is consulting on whether these ETSI requirements should be mandated, with an understanding that this is similar to the UK Government's approach. On its face, this could be regarded as a lower regulatory cost approach that could be a preferred option. However, we would be cautious about introducing a mandatory approach, without properly understanding the context and issues. Further work will be required to better understand this option, as well as other considerations.

For example, businesses and individuals still need to be better informed about good cyber security hygiene. Businesses are also consumers. Raising cyber awareness through education and training will be key to helping consumers understand how to protect their data. This is an area where support from Government and industry can play an important role. We also raise other questions in relation to proposed cyber security labelling of smart devices in the next section, which could similarly apply to standards.

We have previously raised the topic of cyber security certification, which is another concept that has been considered overseas. For example, the EU Cybersecurity Act came into force in June 2019,

³⁹ The objective of OWASP is "to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies".

which “establishes an EU certification framework for ICT digital products, services and processes. The European cybersecurity certification framework enables the creation of tailored and risk-based EU certification schemes”.⁴⁰ The Commission considered that certification is a way to increase trust by enabling transparency about the security of products and services. On its face, this appears to be an attractive proposition. However, there will be issues that need to be addressed in relation to its implementation, such as being: meaningful to consumers; economically viable for providers of products and services; fit-for-purpose; internationally recognised; and harmonised with other approaches. Although a different piece of law, we noted earlier that the EU GDPR is an example where it was introduced and there were unresolved issues and challenges with its own implementation: “organisations feel the Regulation has not lived up to its objectives and has presented practical difficulties, despite their dedication to implementing the new requirements”.⁴¹ As the EU cyber security certification scheme is relatively new, caution should be taken if Australia were to consider either to adopt this or implement a similar approach – the scope and potential impact of the new scheme on individuals and businesses in Europe and elsewhere is still unclear and untested.

Another issue that we have alluded to earlier was in relation to a need to harmonise multiple cyber security standards associated with various government procurement requirements. Ai Group was involved in a partnership with the NSW Government, Standards Australia, AustCyber and other key industry stakeholders to harmonise cyber security standards across several key sectors.⁴² There is an opportunity for the scope of this work to be expanded to other sectors and jurisdictions. We would strongly encourage Home Affairs’ support for such initiatives.

6.2 General comment about standards

Standards are fundamental to promoting digitalisation because they can enable an ecosystem for technological innovation, competition, international trade and interoperability. Standards, when called up by regulation, offer a mechanism to quickly respond to changing markets. Australia’s regulatory and standards framework needs to be sufficiently flexible to accommodate rapid changes in technologies that lead to new types of business models and competition, while also protecting consumers’ interests.

Much global standards work seeks to address broad systems approaches to significant challenges, including cyber security, as well as other related topics such as smart factories, smart grids, smart cities, IoT and Industry 4.0. These challenges require a new level of coordination and effort, and development of new ways to exchange knowledge between the public and private sectors, academia, standards and conformity institutions.

More generally, it is important that international standards are referred to as the baseline wherever possible. This will make it easier for Australian businesses to export their goods and services, as well as avoid the risk of creating domestic cyber security standards that creates a global competitive disadvantage for Australian businesses and barrier to investment in Australia. International agreements and requirements, and Australia’s regional market (import and export) may also influence the choice of standards.

More generally, Australia should strive for a more judicious and effective mix of standards and regulation in lifting public safety, consumer confidence and business performance. There is considerable potential for the more effective use of consensus-developed standards in addressing a range of economic and social opportunities and challenges. In some cases, standards can work alongside formal regulatory approaches (such as when standards are called up in regulatory instruments) and at other times as a lower-cost substitute for formal regulation.

There has been a trend for Government to move away from the use of Australian standards. While international consistency and efficiency have clear value, international standards development processes may be unduly influenced by particular interests without adequate opportunities for Australian input reflecting domestic expertise, local conditions and needs.

⁴⁰ European Commission, “The EU cybersecurity certification framework” (Policy, July 2019).

⁴¹ Centre for Information Policy Leadership, “GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges” (May 2019).

⁴² Standards Australia, “Cyber security taskforce releases priority recommendations” (Media Release, January 2021).

Of concern, there has been a disturbing tendency for Australian Government agencies to forego the well-regarded model of the transparent, consensus approach to the development of standards in favour of rules and regulations developed by the agencies themselves, including with respect to product energy efficiency. Government agencies typically do not have the technical expertise, the practical experience or the proficiency in effective and structured consultation with industry and others in the community. The result is often sub-standard, and Government should be more willing to back and expedite the use of the more transparent consensus driven standards development model.

Notwithstanding the above, it should be noted that Australia has strong representation at ISO/IEC JTC1 on Information Technology, and its relevant sub-committees on cyber governance and security, with local active committees comprising of industry and community representatives.

The Australian Government should continue to help fund Australian involvement in international standards development and it should ensure that an Australian filter (consistent with the WTO Technical Barriers to Trade provisions in Annexure 3) is applied before the adoption of international standards in Australia. This can be facilitated through a suitable forum such as Standards Australia to consider international standards discussions that impact on a wide range of sectors.

It is vital that Australian industry and consumers have support and access to all international fora involved in standards development (particularly ISO and the IEC IEC) to ensure our national interests are preserved. This will allow for effective contribution to standards development at an ideal stage in which products and services are still under development. Australia is generally known to play a strong role in standards development. Accelerating technological change makes this role even more important to facilitate fast adoption of new technology and realisation of its benefits.

Therefore, there are a range of activities that we strongly encourage Home Affairs to consider before contemplating Option 1 in the Discussion Paper.

Recommendation:

- 15. Government should review key activities relating to standards for smart devices (as opposed to adopting Option 1 (Mandatory standard for smart devices) in the first instance). This includes allowing more time to properly review the voluntary *Code of Practice: Securing the Internet of Things for Consumers*, and understanding the barriers and options to improve its uptake.**

7. Labelling for smart devices

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

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

Question 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?

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

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

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

Chapter 7 of the Discussion Paper suggests that there is a lack of tools for consumers to easily understand the cyber security of smart devices, many smart devices have poor cyber security, and cyber security labelling schemes could be adopted and successful in Australia, citing other regulatory regimes. It proposes three options, namely: maintaining the status quo (Option 0); establishing a voluntary star rating labelling scheme (Option 1); and establishing a mandatory expiry date labelling scheme (Option 2).

Similar to other questions raised in the Discussion Paper, in order to properly respond to the questions raised in this chapter of the Discussion Paper, it is important to first understand the root cause and problems properly before considering whether labelling of smart devices would be a suitable option.

In this section, we specifically respond to Questions 16 and 17 in the Discussion Paper.

7.1 Proper consideration of consumer views and expectations

The labelling schemes discussed in the Discussion Paper appear to be based on the objective to help consumers make informed choices. If a labelling scheme were to be introduced on this basis, it must be designed in a way that consumers will actually be supported to use. Therefore, it is important for Home Affairs to be cautious against making assumptions about consumers' views and expectations. This was an issue that we have identified in discussions with various Government agencies.

For instance, despite best efforts and intentions in the ACCC's Digital Platforms Inquiry, the Inquiry demonstrated that identifying drivers of consumer behaviour is a complex process. It can be easy to unintentionally oversimplify or misrepresent consumer views. That is why it is so important to undertake thorough analysis of consumer behaviour.

In that Inquiry, the ACCC referenced consumer surveys to support some of its arguments on behalf of the consumer and recommendations relating to privacy and data regulation reform. Even so, we questioned whether the ACCC's issues and recommendations properly reflected consumers' views and expectations that are material in nature.

For instance, the ACCC's Digital Platforms Inquiry Final Report acknowledged the concept of the

“privacy paradox”.⁴³

In essence, the privacy paradox refers to a perceived discrepancy between the strong privacy concerns voiced by consumers who, paradoxically, do not appear to make choices that prioritise privacy.

One possible explanation for the privacy paradox is that consumers claim to care about their privacy in theory but, in practice, the value they derive from using a digital platform’s services outweighs the ‘price’ they pay in allowing the collection of their user data. A further explanation is that, while consumer attitudes are often expressed generically in surveys, actual behaviours are specific and contextual, and therefore, consumers’ generic views regarding privacy do not necessarily predict their context-specific online behaviours.

Despite this, the ACCC did not appear to give much weight to this concept on the basis that the privacy paradox rests on the premise of consumers making informed decisions in their transactions with digital platforms. The ACCC was of the view that consumers may be prevented from making informed choices.

Notwithstanding the ACCC’s views, we considered that the potential for a privacy paradox highlighted a need to conduct more rigorous consumer interviews and dialogue to accurately identify the drivers of consumer perceptions. Without accurate identification of drivers, there was risk that recommendations made would not address potential underlying issues.

Government’s interest in this area of reform relates to providing transparency and consumer value. However, the ACCC’s proposed reforms that were based on these aspirations may instead lead to impractical outcomes for consumers such as information and communication overload, and lack of consumer interest and value, not ensuring consumer useability, as well as creating unnecessary regulatory costs and red tape for businesses to implement. There were also practical questions about: whether the consumer would actually go searching for information as a result of increased information and communication; and whether consumers will ultimately be disadvantaged by not getting access to, for example discounts or specials, as a result of the ACCC’s proposed opt-in consent.

We can see similar issues arising in a cyber security labelling scheme discussion and caution against assumptions that could be improperly made about consumers’ concerns, expectations, and the level of information required by customers to contextualise any labelling in such a scheme.

Recommendation:

16. Government should undertake a proper contextual analysis of consumer issues and expectations to assess the materiality of consumer concerns and expectations as it relates to a proposed labelling scheme.

7.2 Overseas considerations

A consideration of overseas approaches to cyber security labelling schemes can be informative before contemplating such an adoption in Australia. For instance, the UK Government has explored the concept of a labelling scheme with the goal of helping consumers make informed purchasing decisions.⁴⁴

At the outset, we would question whether such a labelling scheme would in practice drive consumer decisions, especially if there is limited consumer awareness about cyber security. In fact, the UK Government paper notes that consumer surveys indicated poor user cyber security practices. Nevertheless, the paper offers several important findings:⁴⁵

⁴³ ACCC, Digital Platforms Inquiry (Final Report, 26 July 2019), p. 384.

⁴⁴ UK Houses of Parliament, Parliamentary Office of Science & Technology, “Cyber Security of Consumer Devices” (Postnote, No 593, February 2019).

⁴⁵ Ibid.

... more evidence is needed on how consumers would interpret and act on a cyber security label. Some industry stakeholders have reservations about a trust label as it is not clear who would carry out any certification and how cyber security can be measured. It is difficult to verify that a device is secure due to complex global supply chains ... and because devices produced by following best practice may still contain vulnerabilities. Vulnerabilities may be discovered once a device is on the market, after a label has been awarded. Some academics have suggested that labels should indicate when devices will no longer be supported, and that companies be obliged to address vulnerabilities discovered during this period.

Discussing further about vulnerabilities in device supply chains:⁴⁶

Companies involved in the production and distribution of connected devices include hardware manufacturers, cloud providers, and the developers of operating systems and third-party applications. Complex global supply chains provide many opportunities for vulnerabilities to be introduced, either inadvertently or deliberately. It can be challenging for manufacturers and retailers to validate the security claims of their products, and it may be difficult to establish responsibility for security. Furthermore, attackers may exploit this supply chain, for example, by implanting malware into a software update or third-party application. The Royal Academy of Engineering has highlighted the need for governments, industry and international institutions to collaborate on developing an international baseline for security standards.

In addition to the UK, there are other countries that are contemplating or trialling a cyber security labelling scheme, including in Singapore, US and several EU countries. It should be acknowledged that these overseas activities are still in their infancy of development and significantly larger markets compared to Australia. It is important to appreciate this context and it may be prudent to observe developments and lessons in these other countries.

With the consumer aimed to be at the centre of these initiatives, understanding consumer behaviours will assist policy makers to meet consumer needs. If not properly designed, such schemes could promise much but achieve little to assist consumers in practice. Of concern will be businesses subject to a labelling scheme facing uncertain regulatory costs to comply, while consumers see little benefit or interest.

Recommendation:

17. Before further consideration of a cyber security labelling scheme, the Government should take into account international lessons.

7.3 Australian considerations

In the Australian context, there are likely to be similar practical questions with regard to a cyber security labelling scheme. For instance:

- How will consumers in practice interpret and respond to a cyber security label (especially if we assume consumers generally have a limited understanding of good cyber security posture)?
- How will cyber security labelling of smart devices be useful to consumers if they engage with an intermediary or third party (e.g. product purchased and installed by a tradesperson on behalf of the consumer)?
- Who will be responsible for certification of labelling?
- Who will enforce certification and labelling compliance?
- Who will assess cyber security and to what standard (especially international)?
- How will cyber security be determined for a product that is comprised of complex global supply chains?
- How will subsequent vulnerabilities be handled after product labelling?
- What will be the impact of products expiring due to labelling (e.g. environmental impact on landfill waste)?

⁴⁶ Ibid.

-
- How will responsibility be apportioned for validating security between multiple parties in the supply chain?
 - What is the role of labelling with respect to malicious cyber security attacks that is beyond the control of the manufacturer?
 - Will there be a conflict between representations made in a labelling scheme that might be misleading or deceptive in the eyes of the consumer and consumer affairs regulator under Australian Consumer Law?
 - As smart devices are global in nature, how will such a labelling scheme be consistent with Australia's international trade obligations?

As can be seen, there are several interrelated issues including with respect to standards, certification, supply chains, consumer affairs and international trade. These issues will need to be properly worked through and consulted with industry before contemplating a labelling scheme. For example, the use of online resources could be a solution to assist the consumer. Nevertheless, any detailed considerations of solutions would require further investigation and consultation with industry.

Irrespective of a labelling scheme, as with standards, businesses and individuals still need to be better informed about good cyber security hygiene. Labelling should not be seen as a substitute for this and there could be a risk that consumers are given a false sense of security.

Recommendations:

- 18. Government should develop other options to encourage consumers to purchase secure smart devices (as opposed to adopting in the first instance a cyber security labelling scheme under Option 1 or 2).**
- 19. Should Government wish to proceed with cyber security labelling schemes, it should undertake a feasibility study of implementing such schemes, including (but not limited to) with respect to standards, assessment (including cost-benefits), certification, enforcement and complex global supply chains.**

8. Responsible disclosure policies

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

Chapter 8 of the Discussion Paper discusses the concept of responsible disclosure policies and suggests adoption is low among Australian businesses and may impact Australian business capability to engage with security researchers internationally to support vulnerability detection. It proposes three options, namely: maintaining the status quo (Option 0); voluntary approaches to increasing responsible disclosure (Option 1); and regulatory approaches to increasing responsible disclosure (Option 2).

The Discussion Paper notes that the Australian Government already encourages responsible disclosure through its ISM, and the ACSC also encourages the public to responsibly report security vulnerabilities directly with organisations. If attempts are impractical or unsuccessful, then these can be reported to the ACSC who can in turn pass on unverified vulnerabilities to other agencies where appropriate.

In principle, we support the concept of responsible disclosure policies, given the various purported benefits outlined in the Discussion Paper. However, we do not consider that a strong case has been made to support a mandatory approach to a responsible disclosure policy. In absence of substantiated evidence to support a heavier approach towards regulation on increasing responsible disclosure, we consider the existing mechanism to be sufficient (i.e. Option 0 to maintain the status quo).

If the objective were to assist in boosting security research in Australia, then there are other mechanisms that would be more appropriate than through regulation and should be investigated further. For example, public funding for collaboration R&D initiatives between industry and research on security.

Recommendation:

20. In absence of substantiated evidence to the contrary, we do not consider that an adequate case has been made to introduce a mandatory regime for responsible disclosure policy.

9. Health checks for small businesses

Question 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?

Question 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?

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

Chapter 9 of the Discussion Paper discusses providing additional support in supply chain risk management for small businesses, noting limited time, money and expertise to understand and implement cyber security. It therefore proposes options, namely: maintaining the status quo (Option 0); and introducing a voluntary cyber security health check program (Option 1).

Businesses of different sizes require cyber security support. However, SMEs (not only small) require relatively more support than larger businesses.

We support a health check program as one avenue to support SMEs. However, there is more that can be done to improve the cyber security uplift of businesses.

As a peak industry association, Ai Group's role is to help businesses and we would welcome working with Government and industry to ensure businesses (especially SMEs) receive the most benefit from a well-designed cyber security uplift program.

We discuss further on ways that Government could assist businesses in uplifting their cyber security in section 4 of this submission.

10. Clear legal remedies for consumers and other issues

Question 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?

Question 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?

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

Chapter 10 of the Discussion Paper suggests there are limited legal options for consumers to seek remedies or compensation for cyber security incidents, and consider stronger rights of recourse for cyber security be provided to appropriately compensate after an incident and incentivise technology companies to maintain acceptable levels of cyber security.

In addition to our comments about existing regulations and legislations related to cyber security in section 3 and on the effectiveness of the privacy regulations and legislations in section 5 of this submission, we would like to provide additional comments, specifically in response to Questions 26 and 27 in the Discussion Paper.

As stated in our 2019 submission, firstly industry clearly has commercial interests in ensuring that their business and customers' transactions are protected. Customer protections are certainly important. When implemented, it should govern the requirements in the design and implementation of security in products and services that meets an appropriate cyber security standard.

In addition to the Privacy Act, consumers are currently afforded with protections under the Australian Consumer Law and now the recently passed Online Safety Act.

Nevertheless, increasing consumer protections was proposed in the ACCC's Digital Platforms Inquiry and subsequently in the AGD's review of the Privacy Act. In particular, the ACCC recommended for a direct right of action for individuals and a statutory tort for serious invasions of privacy. It argued that consumers would become empowered and given greater control over their personal information by giving them another avenue for redress, and will incentivise APP entities to comply with the Privacy Act. It also suggested that a new cause of action relating to a statutory tort for serious invasions of privacy would lessen the bargaining power imbalance for consumers, address existing gaps in the privacy framework and increase the deterrence effect on businesses.

While it is important for consumers to have access to an avenue to seek redress for breaches of the Privacy Act, caution needs to be taken when considering creating any new forum or cause of action.

We consider that the forum with the appropriate expertise lies with the OAIC to assess breaches relating to privacy and act on an affected individual's behalf. If there are concerns that the OAIC has insufficient resources to undertake its responsibilities or expeditiously resolve matters, a more appropriate response would be to increase the OAIC's resources.

Creating another avenue and action for redress through the courts may create other problems, including shifting the administrative burden from the OAIC to the courts, duplicating the OAIC's function, and potentially opening up the floodgates to a litigious culture. Such an outcome would be an administratively inefficient use of public resources and would most likely harm many businesses.

There may also be a false economy created for the consumer in seeking legal action through the courts. There will be legal costs for consumers and businesses in using this avenue which need to be accounted for.

We discuss in further detail about issues with the above proposals in our submission to the AGD.⁴⁷ In short, the current avenues for enforcing the provisions of the Privacy Act are fit for purpose and do not currently require amendment.

The example above highlights that there are important considerations that Home Affairs should be cognisant of when considering reforms associated with consumer protections. Substantiated evidence will be required if there is a view that the current protections are inadequate, supported by proper consultation with relevant stakeholders to properly identify any problems and develop options to address any identified issues.

Recommendation:

- 21. In absence of substantiated evidence to the contrary, we do not consider that an adequate case has been made for further cyber security reforms associated with consumer protections.**

⁴⁷ Ai Group submission to AGD (November 2020), <https://www.ag.gov.au/sites/default/files/2020-12/ai-group.PDF>.