Australian Computer Society Inc. (ACT)

ARBN 160 325 931

National Secretariat

Tower One, 100 Barangaroo Avenue, Sydney NSW 2000
PO Box Q534, Queen Victoria Building, Sydney NSW 1230
T +61 2 9299 3666 | F +61 2 9299 3997
E info@acs.org.au | W www.acs.org.au

To the Cyber, Digital and Technology Policy Division,

Australian Department of Home Affairs

ACS response to Strengthening Australia's cyber security regulations and incentives – A call for views

5 August 2021

Dear Sir or Madam

Thank you for the opportunity to contribute to this critical discussion.

The Australian Computer Society (ACS) is the peak professional association for Australia's information and communications technology (ICT) sector, with over 48,000 members.

As you might expect, we have a keen interest in ensuring Australia continues to have the among the best cyber security in the world. We believe it is incumbent on both business and government to ensure everything possible is done to protect the Australian people and the Australian economy from increasingly aggressive and sophisticated adversaries.

To that end, we asked our Cyber Security Advisory Committee to prepare a response to the recent DHA Discussion Paper. The Cyber Security Advisory Committee is comprised of some of the most experienced and credentialled cyber security professionals working in Australia today, and their response to the paper follows.

Thank you so much again for your time and the opportunity to comment on this work, and we'd be delighted to discuss this response and its proposals with you further. If you'd like to discuss any part of this response or simply seek further clarification or input, please feel free to contact myself by email at troy.steer@acs.org.au or by phone on 0417 173 740.

Yours sincerely

Troy Steer

ACS Director of Corporate Affairs and Public Policy

ACS responses to questions in the Strengthening Australia's cyber security regulations and incentives discussion paper

Chapter 2: Why should government take action?	
1. What are the factors preventing the adoption of cyber security best practice in Australia?	The key issue is competing priorities and the inability to articulate a compelling argument for diverting investment from something else into cyber security. Part of the challenge is that cyber security doesn't become a compelling business problem until it becomes a business-critical problem. In addition, current regulation is primarily targeted at the largest Australian businesses or those in critical sectors, meaning that most businesses are not regulated for cyber security. With proper incentives, Government can increase the adoption of better practices across all organisations and industries. There is also a dichotomy between suppliers of technology and consumers of technology. Business consumers expect and should be able to rely on the systems being supplied to them as being "secure" in the same way they are able to rely on the other business tools being supplied to them as being "safe".
2. Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?	On the supplier side, unfortunately, regulation of software and services is going to be the only way to make cyber a compelling business problem before it becomes a business-critical problem. Ideally, commercial regulations should be similar to consumer protection regulation that prevents suppliers contracting out of reasonable obligations such as cyber security and requires them to step up to advertising that claims their software is "secure" or "safe". Additionally, on the consumer side, the root of many problems in getting cybersecurity addressed by businesses is the fundamental problem of quantifying the negative externalities. Without a clear articulation of the makeup of these losses, any attempt to shift costs onto businesses through regulation will be hampered by the rejection of the burden of regulation. Rather than seek to solve the fundamental problem, businesses will seek to find the least expensive way to comply. The information asymmetry between suppliers and consumers in this space is a significant problem. Suppliers hold all the power in the relationship, and the "take it or leave it" approach

	to EULAs (End User License Agreements) removes the consumers' ability to negotiate a solution, which in turn causes many to simply agree to the terms in the hopes that the non-negotiability of the agreement will act as a defence later, should it be required. In such situations, why would companies expend time and effort understanding the security implications of such agreements? To solve this problem, there must be some flexibility in the agreement between suppliers and consumers. Most importantly, there must be legal provisions preventing suppliers from passing all duty of care regarding the product's security to the customer. Manufacturers of systems must retain some accountability for the security of the products they offer in the market, and this needs to be backed by legal penalties. Conversely, there must be a clear delineation of those aspects that do fall to the consumer to remove the hazard associated with the abnegation of responsibility.

Chapter 3: The current regulatory framework	
3. What are the strengths and limitations of Australia's current regulatory framework for cyber security?	The current regulatory regime is targeted at the largest Australian businesses or those in critical sectors, meaning that most businesses are not regulated for cyber. Much of the current regulation is focused on preventing the accidental exposure, or exfiltration, of personal information from the clients of the targeted businesses. While important, this does not address the issues associated with the direct losses of a business, such as loss of intellectual property, loss of position in negotiations, damage to reputation, and a range of other losses that may be experienced, including illicit and unauthorised modifications to operational systems.
4. How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?	There needs to be a stronger legal framework forcing businesses to deal with the issue. Without a legal driver many businesses either avoid the issue as being too hard or they seek to take the minimum actions possible to offload risk to third parties. While offloading risks can be good business practice, it cannot be the main approach to cyber security. Regulation should be targeted correctly – it should encourage those businesses supplying systems (with the ability to effect cyber security) to improve cyber security and not be an unfair burden on those businesses consuming systems (with little ability to effect cyber security).

Chapter 4: Governance standards for large businesses	
5. What is the best approach to strengthening corporate governance of cyber security risk? Why?	The best and proven way to strengthen governance of large corporations is through increasing regulatory controls and legal requirements. For those companies that already take the threat seriously such controls should not materially alter their behaviour. For those companies that are not satisfactorily addressing the issue the fear of regulatory or legal issue may be the only way to entice management to act. The regulations required to achieve this need not be overly burdensome, but the responsibility for ensuring compliance should clearly lay with directors and senior management.
6. What cyber security support, if any, should be provided to directors of small and medium companies?	There is already a reasonable amount of support for directors in the form of courses, consultancies, and advice. More would help, but without a driver for the uptake of these resources they would sit idle.
7. Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?	Over the past few years, cybercrime has achieved quite a high profile within the business world. Most, if not all, business leaders know of the issue. The problem remains convincing those leaders to act and prepare their companies ahead of an attack.

Chapter 5: Minimum standards for personal information	
8. Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?	Including a cyber security code under the Privacy Act will neglect to cover portion of businesses that are exempted either as small businesses (i.e. <$2M) or through other exemptions. These represent a significant holding of personal and sensitive information and need to be covered by a suitable compliance regime. In addition, the definitions within the Privacy Act as to what constitutes information people would regard as private needs reviewing. By way of example, many IoT-style devices require access to a households Wi-Fi network to operate. Such information is often communicated to the service provider, who is under no obligation to keep this data confidential under the Privacy Act as it does not fall into the current definition of private information.

9. What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?	Adding technical controls to the Privacy Act creates the risk that businesses will take a check-box approach to complying with privacy, focusing on compliance at the expense of the general principles. Rather than adding specific codes, the definition of what needs to be kept private needs to be broadened, and the principles applied to all businesses, companies and entities holding private information.
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?	Given the interconnected nature of the world today, all companies must be covered equally, regardless of size or revenue. A small company not covered by the Act due to size or revenue may still hold significant amounts of personal information, which could have dire consequences if leaked. The Act needs to cover all sectors, both public and private. The concept of the type of data that needs to be protected needs to evolve. Sensitive data such as biometric information, passwords, network access keys, encryption keys, and much more need to be shared with various companies in the modern world. Citizens need to know that this data is covered by legal requirements to protect it.

Chapter 6: Standards for smart devices

11. What is the best approach to strengthening the cyber security of smart devices in Australia? Why?	One approach could be defining what is meant by “secure” and cracking down on suppliers that advertise their devices as “secure”. Another fundamental issue is the time-variable nature of any security rating. Many consumers will expect that the initial rating applies to the security of the device itself and lasts for the life of the device. In fact, the rating is more closely tied to the initial state and the manufacturer’s process for maintaining the device.
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**	Yes, ESTI EN 303 645 is an appropriate standard for Australia to adopt. Given the small market share we represent, attempting to introduce another standard would mostly likely result in lower compliance, or the withdrawal of products from the Australian market. All the requirements are appropriate, though a phased approach for their introduction should be considered to allow industry time to make the required changes. Most

standard of security appropriate? **b. If not, what standard should be considered?**	requirements could be enforced in phase one, with only those requiring hardware changes being given more time. In section 6 of ESTI EN 303 645 (“Data protection provisions for consumer IoT”) there is reference to the protection of “personal data”. The definition of data here is different to that in the Privacy Act 1998, and the aims of the regulation will not be met if the existing Act is used for the definition. The Privacy Act requires updating before it would be suitable, or a separate definition of “private data” would be required.
13. *[For online marketplaces]* Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?	If given time, say two to three years, most products available for sale will naturally retire or be brought into compliance, and there would be little need to remove products. Non-complying products would be difficult to sell, so market forces would mostly resolve this issue. Conversely, any products that do not meet the standards required for security should be removed from the market at the end of the grace period in order for the country improve its overall security posture. Cyber security is a serious problem and vendors should not be left the option of saying “no thank you” to security standards.
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?	When designed for security from the start, the overall impact to cost is quite manageable. There may be some increases in some areas, but this is moving the prices back to where they would have been if devices had been designed for security in the first place.
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?	Having a standard means Australia will not become the dumping ground for insecure products. Without a strong set of standards, we risk an ever-worsening security posture as cheaper, less secure solutions are sold in the local market. Eventually, as stocks of less secure devices run out, the secure devices will become the norm in all markets – but why would Australia wish to wait?

Chapter 7: Labelling for smart devices	
16. What is the best approach to encouraging consumers to purchase secure smart devices? Why?	Ongoing education, both about the risks and what the rating system truly means. Without this many will unwittingly purchase less secure devices, and those that do buy secure devices may not realise the steps required to ensure the devices remain secure.
17. Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?	Consumers have been taught to think in terms of "star" ratings where a device is given a rating prior to the purchasing decision, and that rating will last the life of the product. This is not true of cyber security ratings. The "secure rating" of a device will change frequently as vulnerabilities are found and fixed – or not. The rating system proposed only covers the initial design and the manufacture's ability to keep the product updated. If would have to be made clear to people that in some circumstances, such as where automatic patching is not available, they still hold a responsibility to maintain the rating through their actions.
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?	A voluntary scheme would only see uptake if it aligned with global schemes in other jurisdictions. Given the relatively small scale of the Australian market it is unlikely we would be able to effect global change in this space. Attempting to mandate such a system would see products removed from the Australian market. Consumers, however, would still be able to procure these devices from offshore. The net result would be bad for local manufacturers, suppliers and consumers.
19. Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?	An expiry date makes sense, provided manufacturers are obligated to ensure service, maintenance, and patching for devices through to the product's end of life. Most manufacturers already have a product life cycle that define the end of support dates. Having manufacturers state this clearly such that the consumer is aware of this date prior to purchase should be relatively easy to implement. It is possible there will be an adverse reaction from consumers, who typically assume devices will last forever, however this is manageable.

20. Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?	Devices such as mobile phones, tablets, smart watches are all custodians of data citizens would wish to keep private. These devices must be included in a scheme if it is to have any real hope of addressing the fundamental issues of security.
21. Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?	Devices should be labelled electronically and physically. The electronic labelling should be more than an RFID attached to the device, but should also be accessible from within the operating system of the device. This allows for easier automatic discovery when conducting audits and reviews. For many personal consumers and small businesses, it would be important to see the rating prior to purchase, which is before any electronic rating could be read. For many people these devices are "set and forget" and a physical visual reminder of the end-of-life date will be the only reminder seen. The real question is should the device stop functioning or provide some other visual warning sign once it reaches the end-of-life date?

Chapter 8: Responsible disclosure policies	
22. Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?	When it comes to a business disclosing that it has exposed personal information, a voluntary scheme will not work. Every business knows the negative press will outweigh the potential good will. Unless a system is mandatory, with penalties for noncompliance, most businesses will simply seek ways to justify non-disclosure.

Chapter 9: Health checks for small businesses	
23. Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?	Yes. However, it will need to be fit for purpose, meaning different for each sector. The problem with the current scheme is that those offering to conduct a Health Checks are pricing them beyond the means of many small businesses, especially in the current economic climate. The outcomes also have little meaning for the business owner, since they are expressed in terms of Essential 8 compliance

	rather than something meaningful, making it difficult to prioritise spending against other business-critical items investments. Rather than mandating the implementation of solutions it may be better to mandate the implementation of reviews. A framework outlining areas that must be considered and a requirement that annual business audits include evidence that the business has considered the issues and the directors have signed off on the treatments. This puts the responsibility for ensuring the issues are considered onto the directors of the company.
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?	The Government procurement process can be used to encourage small businesses by giving those SMEs with a Health Check an advantage over those without, in a similar manner to indigenous procurement. This should apply across all levels of government, from Commonwealth through to local. Alternatively, a useful approach might be the creation of a set of guided reviews to ensure small businesses know the questions to be asking of their suppliers. Right now, business who wish to do the right thing but do not have to skills in house have no simple framework for guidance. Those frameworks that do exist focus on implementation, not governance, and as a result tend to be too large and unwieldly for small businesses.
25. If there anything else we should consider in the design of a health check program?	There is a need to have a suitable pool of consultants able to meaningfully conduct the Health Check. This can be problematic in regional and rural areas. Conversely, such reviews could be conducted remotely, providing an opportunity for rural participation in the reviews – though the usual problem of finding the talent still applies.

Chapter 10: Clear legal remedies for consumers

26. What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?	No response provided.

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?	No response provided.

Chapter 11: Other issues

28. What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights consumers?	No response provided.