Response to Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper

Submitted by: Frank Zeichner, CEO, Internet of Things Alliance Australia
Email: frank.zeichner@iot.org.au
Phone: 0408 233 762
Date of submission: xxxxx

Introduction

IoT Alliance Australia (IoTAA) is the peak Australian IoT industry body with over 500 participating organisations and 1000 individual participants working across 12 workstreams. We address deployment and uses of Internet of Things (IoT) devices and services in Australia. Our mission is to accelerate the adoption of IoT in Australia to improve our competitive advantage and benefit society.

IoTAA welcomes this opportunity to convey our views on *strengthening Australia's cyber security regulations and incentives* (the Paper).

Our submission focusses on cyber security regulations and incentives addressing the security of IoT products and services, primarily Smart Devices covered in Chapter 7 (page 36 of the Paper)

To address the rapidly changing IoT smart device security threat landscape and to support Australian security innovation and leadership, we propose a consumer-informed, industry-led certification and labelling scheme that is supported by Government. This scheme would create highly visible and adaptable security credentials for IoT devices and services to build consumer confidence, reduce security risks and support and reward good IoT product practice and service providers.

This submission also contains responses to selected questions related to 'smart' devices proposed throughout the Paper.

The IoT devices (and services) security problem

The economic and societal benefit and impact of IoT is critical to Australia's productivity and competitiveness. IoTAA agrees that there is a significant risk and growing threat of cyber security incidents related to the rapid growth of Internet of Things (IoT) 'smart' devices and services. Addressing the associated security risks is critical to building the trust needed to realise the above IoT benefits.

Our members strongly support the IoTAA eight-point Australian IoT security strategy initiated in 2017[1], which seeks to address the security threats and position Australia as a leading 'IoT secure' nation.

Unfortunately, the fast-changing security threat landscape, combined with consumer lack of awareness and understanding of IoT security, has created circumstances where consumer experience and cost are sometimes prioritised over in-built 'security by design' features, leaving unknowing consumers without protection and exposing them and others to risk of cyber-attack.

Security experts say that approximately 60 per cent of the 30 billion plus IoT connected devices on the market are completely unsecure or can be hacked using straight forward brute force attacks.[2]

---

[1] https://www.iot.org.au/wp/wp-content/uploads/2019/11/IoTAA-Submission-to-Australias-2020-Cyber-Security-Strategy-1.pdf

[2] Roberts, G. 'Australian security cameras hacked, streamed on a Russian-based website', ABC News, 24 June 2020 - accessed at www.abc.net.au/news/2020-06-24/security-cameras-hacked-streamed-on-russianwebsite/12380606

While consumers and businesses are becoming more aware of the financial and non-financial costs of security breaches from IoT devices and services, they lack the ability to differentiate more secure devices from others.

Device vendors don't always make the right investments in cyber security because of weak commercial incentives. Such businesses find it difficult to differentiate their cyber security features resulting in cyber risks often being transferred to third parties such as customers and suppliers.

We need incentives to shift this paradigm to raise the visibility of IoT security credentials, reward secure IoT vendors and service providers, educate and motivate new suppliers to implement security by design and expose bad actors and practices.

Industry taking the lead

To significantly shift the current IoT security paradigm, IoTAA proposes a consumer-informed, market driven, industry-led certification and labelling scheme supported by Government.

This has been a key element of our eight-point security strategy since 2017 and the subject of wide industry consultation and design by IoTAA, and would provide an important foundation for encouraging industry to drive best practice in IoT security.

A certification and labelling scheme would provide consumers, business and governments with critical visibility and confidence of the independently verified security claims of the devices and solutions they are purchasing.

The features and benefits of this approach provide:

- **Visibility: to empower consumer choice and create a market to drive to better security**

  By labelling certified vendors' security claims, consumers and buyers can be informed and empowered to choose devices and services that are certified against good security practice guidelines and frameworks. This enables a market driven incentive that drives businesses to invest in security and certify their device security claims and helps consumers gain a greater understanding of cyber security threats.

  By contrast, an extension of product safety requirements of Australian Consumer Law (ACL) to mandate that products must be 'secure' as well as 'safe' does not enable a prospective purchaser to know that the manufacturer or another supplier has taken account of and ensured compliance with any such new ACL requirement.

- **Adaptability**: **to encourage higher security levels and market competition**

  Participation in the scheme by device vendors should encourage and give them flexibility to design-in and certify appropriate security levels. For example, some devices may need little security while others (e.g. those with safety risks) will require higher levels.

  Given the constantly changing security landscape and diversity of IoT devices, services, contexts and scenarios of deployment and use, a 'one size fits all' statutory requirement that a device or service be 'secure' is unlikely to provide appropriate incentives for suppliers to address vulnerabilities or provide appropriate instructions and support to address security vulnerabilities over time.

A new mandate under Australian Consumer Law that products must be 'secure' or comply with a certification scheme for a mandated minimum standard level of security, risks nurturing false consumer expectations that a product is inherently 'secure' and reduces business incentives for vendors to invest in higher level security.

- **Standards based**: **for global market recognition and goods flow and avoiding Australian-only costs and applicability**

  IoTAA recommends security implementation and claims in accordance with recognised international IoT device standards bodies and a baseline security level such as:

  - ETSI EN 303 645
  - Cyber Security for IoT: Baseline Requirements (which is similar to the UK (DCMS, October 2018) and the Australian IoT Device Voluntary Code of Conduct (DoHA, September 2020).

  Other standards bodies to observe in the IoT 'smart' device space are:

  - ENISA with the publication of Baseline Security Recommendations for IoT, and
  - NIST with the NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers.

- **Industry led**: **for faster introduction and lower costs**

  Due to the rapidly evolving nature of cyber-attacks, security capability, implementation and claims testing need to be adaptable. Industry is best placed to administer and adapt such a scheme. Costs would be largely borne by industry, although IoTAA sees a key role for Government departments, agencies and associated stakeholders such as Standards Australia and the Australian Cyber Security Centre to guide the adoption of such standards and procedures.

  The underpinnings of an Industry-led IoT Security trust mark have already been developed by IoTAA and offers an immediate pathway to implementation.

- **Supported by government**: **to rapidly create earlier market scale and incentives**

  There is a vital role for government to raise awareness and (to the greatest extent possible) promote the use of devices that carry the security label, both for its own internal use and by Australian businesses and consumers.

Moving forward

The IoTAA has presented a proposal for a labelling scheme that will achieve secure, resilient and trusted IoT-enabled solutions and services in Australia. We would welcome the opportunity to discuss any aspects of our submission in further detail and how the IoT industry may assist in achieving the Department's vision to strengthen Australia's cyber security regulations and incentives, specifically in the IoT 'smart' device and related services arena.

Answers to selected questions from 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?**	As the market expands, consumer experience and costs have been prioritised over in-built 'security by design' features, leaving unknowing consumers without protection and exposing them to significant risk of cyber-attack. Security experts believe about 60% of the 30 billion IoT connected devices on the market are totally unsecured or can be hacked using brute force attacks.[3] Device vendors don't always make the right investments in cyber security because of weak commercial incentives. Anecdotal evidence suggests that these organisations find it difficult to differentiate their products based on better cyber security. Cyber risks are often transferred to third parties such as customers and suppliers because there is limited business and legal incentive for suppliers to carry that risk. Most consumers are not empowered to readily make decisions regarding product security. Nor should they be expected to understand complex, dynamic and evolving information security threats and vulnerabilities or assess, address, mitigate and manage residual risks in deployment and use of most IoT devices and IoT device enabled services.
2.	**Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?**	The main issue is that consumers do not understand security risks. The principal issue is a coupling of (1) asymmetrical capabilities to assess, address, mitigate and manage security risks and (2) negative externalities. In essence, there is limited business incentive and legal incentive for suppliers to carry security risk associated with deployment and use of most IoT devices and IoT device enabled services. IoT device security is not widely understood, nor are security choices for IoT devices for consumers a leading concern.
Chapter 3: The current regulatory framework		
3.	**What are the strengths and limitations of Australia's current regulatory framework for cyber security?**	The Australian Government released the Voluntary [Code of Practice: Securing the Internet of Things for Consumers](#) (Code of Practice). This is a first step towards improving the security of smart devices in Australia. The Code of Practice contains 13 principles that signal Government expectations to manufacturers about the security of smart products. Early experience in Australia (and longer experience with the UK voluntary

---

[3] Roberts, G. 'Australian security cameras hacked, streamed on a Russian-based website', ABC News, 24 June 2020 - accessed at www.abc.net.au/news/2020-06-24/security-cameras-hacked-streamed-on-russianwebsite/12380606

		code of conduct) points to the scheme having little impact on compliance and visible improvement in security levels. This provides good guidance to willing and proactive vendors and service providers but requires incentives to drive broader adoption.
4.	**How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?**	Recent changes to regulation focus on large Australian businesses and those operating in critical sectors and we consider the efforts of government and industry in this regard have strengthened cyber security and resilience in those sectors. Attention now needs to turn to small-medium enterprises and consumers to improve coverage of good cyber security practices through a combination of education, incentives and possibly some changes to the regulatory environment. In determining the best approach to expand good cyber security practices into the SME and consumer sectors, attention should be paid to reducing negative externalities and providing appropriate incentives for both supplier and users of IoT devices and IoT device enabled services to assess, address, mitigate and manage security risks. We noted above how a certification and labelling scheme would provide consumers, business and governments with critical visibility and confidence that the devices and solutions they are purchasing and using independently meet vendor claims of security capabilities. We consider this approach would be more effective than increasing or expanding 'black letter' regulation. We also noted the risk that a 'one size fits all' mandating of product 'security' under Australian Consumer Law would not create appropriate incentives for heightened levels of security or targeted accountability of the entities best able to address security risks. If regulation is developed to accompany and/or enforce activities such as a security certification and labelling scheme, we consider it should focus on creating accountability for those entities best able to address security risks.
Chapter 4: Governance standards for large businesses		
5.	**What is the best approach to strengthening corporate governance of cyber security risk? Why?**	No response
6.	**What cyber security support, if any, should be provided to directors of small and medium companies?**	No response

7.	Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?	No response
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?	APP 11 of the Australian Privacy Principles (APPs) and community expectations as to good data privacy governance create business and legal incentives for APP entities to take such information security steps as are reasonable to protect personal information from misuse, interference or loss and from unauthorised access, modification or disclosure. These incentives are reinforced by the mandatory notifiable data breach scheme. However, the Office of the Australian Information Commissioner is not financially or technologically resourced to develop or oversee cyber security standards. APP 11 and the mandatory notifiable data breach scheme address personal information about individuals, not the broader range of non-identifying information about individuals and information relating to households and businesses and other entities that may be exfiltrated and used to cause harm to the data subject. The data security risks that need to be addressed through targeted regulation are much broader than risks of exfiltration and improper use of personal information about individuals. The Privacy Act does not readily extend to security risks arising elsewhere within the multiparty data ecosystems that are now typical features of many service deployments, including provision of IoT device enabled services. Additionally, the current small business exception from the Privacy Act creates a substantial gap in the coverage it provides. We noted above how a certification and labelling scheme would provide consumers, business and governments with critical visibility and confidence that the devices and solutions they are purchasing and using independently meet vendor claims of security capabilities. We also noted the risk that a 'one size fits all' mandating of product 'security' under Australian Consumer Law would not create appropriate incentives for heighted levels of security or targeted accountability of the entities best able to address security risks for the clients of targeted businesses.

9.	What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?	Our response to Q.8 above noted why we do not consider that the Privacy Act is the best legislative instrument to address cyber security risks. Often cyber security, particularly with embedded IoT 'smart' devices, is confused with safety and privacy; the three are distinctly different, and while security can underpin safety systems and privacy mechanisms, these are separate policies. Our earlier responses address why we consider that mandatory standards are not an optimal regulatory response. We propose a consumer-informed, voluntary, market driven, industry-led certification and labelling scheme supported by Government.
10.	What technologies, sectors or types of data should be covered by a code under the Privacy to achieve the best cyber security outcomes?	See our responses to Q.8 and Q.9 above.

Chapter 6: Standards for smart devices		
11.	What is the best approach to strengthening the cyber security of smart devices in Australia? Why?	IoTAA proposes a consumer-informed, voluntary, market driven, industry-led certification and labelling scheme, supported by Government (Security Trust Mark – STM). This will provide consumers, business and governments with critical visibility and confidence that the devices and solutions they are purchasing and using meet the vendor's claims of its security capabilities independently.
12.	Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt 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?	IoTAA recommends security implementation and claims in accordance with recognised international IoT device standards and a minimum security baseline such as ETSI EN 303 645, Cyber Security for IoT: Baseline Requirements (which is similar to the Australian IoT Device Voluntary Code of Conduct (published by the Department of Home Affairs on 3 September 2020). A minimum mandatory scheme with lesser requirements risks setting false consumer security expectations while reducing the incentive for vendors to invest in higher levels of security in their products and services. It also risks 'Australian only' implementation and costs, which international vendors may baulk at. International alignment is critical. The right level of cyber security for IoT devices is context and technology specific. Some devices will need to be more robust than others in areas of safety and information privacy, for example. A minimum mandatory standard fails to incentivise better security for the most vulnerable (and

	b. If not, what standard should be considered?	sensitive) contexts. It also risks imposing additional costs on IoT devices where such a requirement is not needed.
13.	*[For online marketplaces]* **Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?**	No response
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?**	Independent third-party testing of devices and/or end-to-end solutions provides a credible approach to assessing vendor claims. Importantly, the cost of independent testing will scale with the complexity of the device. A single vector sensor (e.g. temperature) is far less complex than a smartwatch, both in terms of development cost and testing cost. Hence testing cost will broadly remain a consistent percentage of the development cost, which will be single-digit percentage – less than 5% in most cases.
15.	**Is a standard for smart devices likely to have unintended consequences on the Australian market? Are they different from the international data presented in this paper?**	Devices operating in combination, including solutions comprising both devices and other system components such as cloud storage and analysis of data, are difficult architectures for a single (or even multiple) standards to encompass. While a specific standard (e.g., ETSI EN 303 645) in its specific context (devices) may not have any gaps or unintended consequences per se, consumers may nevertheless obtain an inflated sense of security from simple compliance to a standard. The certification and labelling scheme we have described in the body of our submission applies both to devices in isolation and in combination as part of a system or solution. It is possible to assess the end-to-end security of a service provided to consumers and businesses.

Chapter 7: Labelling for smart devices		
16.	**What is the best approach to encouraging consumers to purchase secure smart devices? Why?**	Cyber security events are a daily occurrence and industry and consumers are becoming acutely aware of the financial and non-financial cost of these events. As a result, businesses and consumers are increasingly seeking out devices with higher security credentials to minimise their risk of becoming the victim of an attack. By labelling certified vendors' security claims, consumers and buyers can be informed and empowered to choose devices and services that are certified against security standards. In this way, a market driven incentive is enabled to drive manufacturers to invest in and certify their product and/or end-to-end service security.
17.	**Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?**	Yes, the labelling can indicate the level of compliance to the standard. The labelling scheme might be capable of applying to all devices (consumer and business) and cover the recommended minimum requirements of ETSI EN 303 364. Adherence to ETSI EN 303 364 might be considered sufficient for a minimum IoT security claims 'Pass'. Additional security standards applied may be identified by various methods.
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?**	Yes. The security of IoT devices is an issue that is actively considered by consumers. Businesses and suppliers that offer independently verified information about the security of their devices will have an advantage in the marketplace. IoTAA has been proposing to Government an Industry led Security Trust Mark since 2017. We are working with Standards Australia to ensure the scheme can be globally recognised with appropriate and recognised governance, compliance, testing and labelling processes. We propose the progression and adoption of this scheme.
19.	**Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?**	While the concept of such a marking on smart devices may be good in theory (and certainly imposes a minimum 'minimum' on product manufacturers), the IoTAA urges significantly more thought and design be given to ensure that consumers are not misled into believing that such a label confers any level of 'security' is provided with a guarantee of inherent safety and privacy. A security expiry date label should state that after a specified date the product will no longer be supported with security updates from the vendor, whereas prior to this date, such security patches, checking and updates are necessary, automatic and enforced (i.e. cannot be disabled). Additionally, consideration should be given to the actions for consumers and vendors past the expiry date.

Page 39, Figure 2 of the consultation paper under the heading "Option 2 – Mandatory expiry date label" displays an example of an expiry date label.

Figure 2: Example expiry date label

A consumer viewing such a label would be led to believe that the device carrying this mark bears cyber protection until 2025. With software, hardware, firmware and systems vulnerabilities being discovered daily it would be impossible for an IoT vendor to make such a claim.

History with ICT demonstrates that a key risk is legacy devices that are no longer supported from a security perspective remaining online. The onus should NOT be left up to or placed on smart device consumers to be aware and actively remove such devices from their networks. How will the Government police and enforce manufacturers' compliance with this marking of their products given there are so many entry points into the Australian market? Will there be penalties for non-compliance etc.?

Furthermore, a minimum mandatory scheme with lesser requirements than the existing Australian Code of Practice ~ Securing the Internet of Things for Consumers (2020) risks setting false consumer security expectations while reducing the incentive for vendors to invest in higher level security. It also risks non-alignment with international standards and Australian-only implementation and costs, which international vendors may baulk at.

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

		Additionally, a possible unintended consequence of introducing a labelling scheme for these devices may be that the vendor restricts capabilities to a limited set of known applications at the time the device was developed, thereby potentially triggering early obsolescence with users wanting to add more recent applications.
21.	Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?	As a minimum, the security status of consumer devices should be maintained online, including any reported vulnerabilities and available security updates. As previously mentioned, any marking with the date would need to be well qualified in the mind of the consumer so that there is no implied assurance of security, safety and privacy through a vendor applying such a label to their smart device. For maximum consumer effect, visible device security at point of purchase would be best. This may be by signage at point of sale or placed on each device. The former may be a faster and more cost-effective early mechanism to consider.
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?	We support measures to encourage the consideration and implementation of vulnerability disclosure policies. Cyber security standards and regulations predominantly focus on measures that can be taken to reduce vulnerabilities and manage them when they occur. Not enough attention is paid to the role of the cyber research and the IT community in helping to identify vulnerabilities and manage and eliminate them before they are exploited by bad actors. The second six security requirements specified in ETSI EN 303 645 and the IoT voluntary Code of Conduct require providers to have a system that can 'implement a means to manage reported vulnerabilities'. This requirement assumes that vulnerabilities will be reported. A vulnerability disclosure policy is an important part of encouraging and managing the reporting of vulnerabilities.
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. Availability of this service would be beneficial.

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?**	Small businesses could be encouraged to participate by Government providing support for the program. Significant benefit might be obtained by providing easy to understand and implement guidance suitable for small businesses that are not IT suppliers with sophisticated needs and material risk exposures.
25.	**Is there anything else we should consider in the design of a health check program?**	It would be of benefit for information about consumer devices to be maintained online including any reported vulnerabilities and available security updates.
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.
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?**	Yes. There are no other actions necessary in this area.

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?**	Key strategies that help to reduce the risk of loss arising from a data breach include: • maintaining effective, regular and independent backups; and • destroying or deleting all data no longer needed or being used (particularly when held by third party services providers). In addition to conducting a cybersecurity health check-up, small and medium enterprises should be assisted with data back-up and retention practices.