Jen Ellis
VP, Community & Public Affairs
Rapid7
Two Waterside Drive
Arlington Business Park, Theale
Reading RG7 4SW
rapid7.com
[redacted]

Australia Department of Home Affairs
Cyber, Digital and Technology Policy Division

Rapid7 Response to Australia Department of Home Affairs call for information on "Strengthening Australia's cyber security regulations and incentives"

August 2021

The below details Rapid7's response to the Department of Home Affairs' call for information on "Strengthening Australia's cyber security regulations and incentives". Thank you for the opportunity to provide input and support efforts to strengthen cybersecurity and protect Australian internet users and organisations. In general, Rapid7 supports most of the proposals included in this Call for Views and we are encouraged to see the Australian government taking action to advance cybersecurity. The breadth of these proposals seems to indicate that cybersecurity is a priority and it is clear that a very thoughtful approach is being taken to balance security concerns with the need to not over-burden industry. We also appreciate that the approach makes reference to aligning with existing or parallel international efforts, which is the most practical means to supporting a global digital economy.

As a brief aside, I would also like to commend the Department of Home Affairs for framing these proposals in a succinct and highly-accessible format, and with accompanying aids that made it easier to quickly grasp and discuss the information.

Rapid7 is a US-based cybersecurity and data analytics firm with offices around the world, including in Sydney. Rapid7's solutions and services manage cybersecurity risk and simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and respond to attacks, and automate routine tasks. Over 9,300 customers worldwide rely on Rapid7 technology, services, and research to improve cybersecurity outcomes, protect consumers, and securely advance their organisations.

* * *

Part 1 — Set clear minimum expectations

Governance standards for large businesses

Q5. What is the best approach to strengthening corporate governance of cyber security risk? Why?

Rapid7 believes it is most important and impactful to drive adoption of cybersecurity risk management strategies in the critical infrastructure sectors, and we are supportive of requirements for these organisations being carved out and addressed in the Security Legislation Amendment (Critical Infrastructure) Bill 2020[1]. We believe the standards should be mandatory for organisations in these sectors.

More broadly, we agree that adoption of governance standards among large businesses is inconsistent. We also agree this needs to change and organisational leaders need to play a more proactive role in security oversight and adoption. The relationship between boards and cybersecurity is still unclear and informal, and we hear anecdotally that communication between boards and security teams can be sporadic and confusing, with a lack of clear expectations on both sides. The development of a standard or framework for board engagement would help address this confusion and create a better foundation for expectation-setting and determining roles and responsibilities. It would also create an established baseline upon which sector-specific governance requirements could be built as appropriate and needed.

We are encouraged that the proposal suggests the standard would be developed through collaboration with industry, aligned with international standards, and designed to complement existing regulatory requirements. Rapid7 agrees that this approach will make any standard more practical and likely to succeed.

In terms of whether the standard should be voluntary or mandatory for all large businesses, we believe it is reasonable to introduce the standard as voluntary to start and monitor and evaluate its efficacy. The Department of Home Affairs can revisit the situation and determine whether legislation is warranted after an appropriate period of time, just as it is currently doing with consumer smart devices. This approach gives organisations with greater interest and capability to lead, and provides opportunities to learn from their experiences before requiring less mature organisations to adopt the standard.

[1] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6657

Q6. What cyber security support, if any, should be provided to directors of small and medium companies?

Small and medium businesses will benefit from support in a number of areas. Firstly, there needs to be more effort to engage business leaders and help them understand the dynamics of cybersecurity risk and the relevance to their own organisations. For example, there needs to be greater understanding that organisations do not need to be specifically individually targeted to fall victim to cyberattacks. They also need to understand that an incident, for example, a ransomware event, will likely have impact across the entire business and could even represent an existential threat to the business. Even education around the broader societal impact of paying ransoms can help small and medium business leaders better understand the cybersecurity ecosystem within which they operate.

In addition, operational or technical guidance should be provided that is practical, actionable, and realistic for the resources and capabilities of small and medium organisations. Guidance should be prioritised to be manageable and achievable with paths towards greater maturity clearly signaled.

As indicated in the section 9 of *Strengthening Australia's cyber security regulations and incentives,* small and medium businesses typically face challenges of "limited time, limited money and limited cyber security expertise." The Department of Home Affairs should review opportunities to help address these constraints. Budget constraints can potentially be addressed through financial incentives and support such as tax breaks and funds. Another way this could be done is by providing free technical assistance and helping organisations understand what other free cybersecurity tools and expertise are available to them; however adoption of these offerings can be impeded by the limitations on time and cybersecurity expertise.

For this reason, it may be necessary to look upstream to create the desired impact. Many small businesses rely entirely on third parties for all their technical support, yet few managed service providers (MSPs) that meet these needs offer security coverage or awareness. The recent ransomware attack on Kaseya[2] highlighted the breadth of impact that can be created among the SMB community when MSPs are impacted by a security incident. Many security experts have stated that the success of the Kaseya attack is driving more attackers to target MSPs[3]. The Department of Home Affairs should engage MSPs and encourage them to adopt cyber hygiene best practices and assist in educating customers on security risks.

Q7. Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

Yes, business leaders in all sizes and sectors of organisation need more engagement and education. Effective models for this will vary depending on the specific target audience, for example, small

[2] https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/

[3] https://www.reuters.com/technology/kaseya-ransomware-attack-sets-off-race-hack-service-providers-researchers-2021-08-03/

business leaders are harder to reach, but could perhaps be achieved by partnering with organisations that have reach into regional small business networks, for example the Australian Chamber of Commerce and Industry[4].

Partnering can also be effective as a means of engaging leaders in larger organisations, for example with organisations such as the Corporate Leaders Network[5] and The Executive Connection[6]. There could also be opportunities to engage business leaders through partnering with entities such as the Australian Securities Exchange[7] or the National Stock Exchange of Australia[8] if they have outreach program for companies listed with them.

Minimum standards for personal information

Q8. 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?

Rapid7 believes a cyber security code under the Privacy Act would effectively promote the uptake of cyber security standards in Australia. We share the Call For View's calculation that such a code would only apply to personal information and Australian Privacy Principle (APP) entities, but that the code would nonetheless protect consumers and have ripple effects that strengthen cybersecurity in areas unrelated to personal information.[9] We note that Australia has already issued guidance on how to comply with APP 11,[10] and security best practices frameworks are broadly available, so we are not confident that additional voluntary guidance will prompt widespread strengthening of personal information security practices. At the same time, we also share the Call For View's motivation to avoid overburdening industry and provide for flexibility that keeps the code relevant in the future.[11]

Q9. What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?

We recommend considering inclusion of the following achievable technical controls:

- Multi-factor authentication;
- Strong credentials or passwords;

---

[4] https://www.australianchamber.com.au/
[5] https://www.cln.com.au/
[6] https://tec.com.au/
[7] https://www2.asx.com.au/
[8] https://www.nsx.com.au/
[9] Call for Views, pg. 27: https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf
[10] See the APP 11 guidelines: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information/ See also the Office of the Australian Information Commissioner's guide to securing personal information, https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/
[11] Call for Views, pg. 27.

- Avoidance of exposing protocols that are not secure, such as SMB, RDP, and Telnet;[12]
- Appropriate DMARC configuration;[13]
- Efficient deployment of critical security updates;
- Encryption of personal information at rest and in transit.

However, the code should also consider including fundamental security processes that are not strictly technical controls, such as:

- Maintain a written security plan, with personnel designated to oversee the plan;
- Conduct an assessment of the risk to personal information;
- Monitor the effectiveness of controls to personal information;
- Implement processes to detect and respond to significant security incidents and breaches affecting personal information.

Standards for smart devices

Q11. What is the best approach to strengthening the cyber security of smart devices in Australia? Why?

Rapid7 strongly supports the adoption of secure-by-design principles in the development of smart devices. We agree with the principles outlined in the Code of Practice: Securing the Internet of Things for Consumers[14] and appreciate the complementary IoT guidance provided by the Australian Cyber Security Centre[15]. We also acknowledge that, as highlighted by the Department of Home Affairs' research, adoption of these principles is too slow, particularly at lower ends of the market, exposing consumers to risk. For this reason, we have supported[16] legislative proposals in the US[17] and the UK to require the adoption of secure-by-design principles in the development of IoT devices. We likewise support the adoption of a similar approach in Australia. As the Department of Home Affairs' proposal references the UK proposal as an exemplar, we have included the supplemental comments we submitted to the UK Department for Digital, Media, Culture and Sport's call for views (see accompanying attachment).

We appreciate that this approach creates alignment with existing standards, making adoption more practical for manufacturers that operate in multiple regions, and presumably increasing the amount of information resources available to consumers. Efforts to align standards with existing frameworks are always essential to minimise complexity and confusion, and as such, we also urge the

---

12 https://www.rapid7.com/blog/post/2021/05/14/rapid7s-2021-icer-takeaways-high-risk-services-among-the-fortune-500/

13 https://www.rapid7.com/blog/post/2021/04/26/rapid7s-2021-icer-takeaways-email-security-among-the-fortune-500/

14 https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

15 https://www.cyber.gov.au/acsc/view-all-content/advice/internet-things-devices

16 https://www.rapid7.com/blog/post/2020/08/27/internet-of-things-cybersecurity-regulation-and-rapid7/

17 https://www.rapid7.com/blog/post/2020/09/17/a-step-closer-to-stronger-federal-iot-security/

Department of Home Affairs to ensure that the requirements for consumer smart devices do not conflict with guidance for sector-specific regulated connected technologies, for example for connected medical devices[18] or ICS technologies[19]. It can be challenging to draw lines between categories of connected technologies, so any requirements should be developed with existing controls in mind to create alignment wherever possible.

Where relevant, regulatory agencies should be required to clarify how their existing authorities extend to the security of consumer smart devices within their areas of jurisdiction.[20] This should include security-by-design principles and post-market security support.

In addition, it should be clear to smart device manufacturers and operators how Australian Privacy Principle 11 applies to the security of personal information collected or processed through smart devices, as well as how product safety requirements under the Australian Consumer Law apply to smart devices.

In promulgating these requirements and guidelines, the regulatory bodies should work in a coordinated fashion to achieve consistency wherever possible.

Finally, Rapid7 believes that supporting security research is an essential part of advancing the cybersecurity of connected devices[21]. It is critical to ensure that existing computer access laws recognise the role and importance of security research and provide a clear path for researchers to safely and legally test devices that they own in a non-production environment[22]. This reduces the risk for researchers and encourages them to disclose any cybersecurity findings in a coordinated manner that gives manufacturers an opportunity to remediate the issue and protect their customers.

Mandatory standards (Option 2)

Q12. Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt as a standard for smart devices?

Rapid7 supports EN 303 645 and believes it does a good job of identifying key measures that will make a meaningful impact on advancing the cybersecurity of consumer smart devices, with the desire to provide a framework that is practical, actionable, and not overly burdensome.

---

[18] https://www.tga.gov.au/sites/default/files/medical-device-cyber-security-guidance-industry.pdf
[19] https://www.cyber.gov.au/acsc/large-organisations-and-infrastructure/operational-technology
[20] For example, the Therapeutic Goods Administration includes cybersecurity requirements in its "Medical devices essential principles checklist" at 12.1(5): https://www.tga.gov.au/sites/default/files/essential-principles-checklist-medical-devices.pdf
[21] Section 4, page 10 "Avoid chilling independent security research": https://www.rapid7.com/globalassets/_pdfs/policy/iot-security-testimony---043019.pdf
[22] https://www.rapid7.com/blog/post/2015/10/28/new-dmca-exemption-is-a-positive-step-for-security-researchers/

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

An argument could be made to include many of the principles of EN 303 645 as they all add value; however, Rapid7 believes it is appropriate and practical to start by prioritising the most fundamental measures to create a minimum baseline.

The top three requirements indicated will help address two of the most significant issues (use of universal default passwords and unpatched vulnerabilities), while also introducing a shift towards a more security-oriented culture and approach. At the same time, by limiting the requirements to these three, the Department of Home Affairs can make the mandate less intimidating and burdensome for manufacturers at the lower end of the market.

The impact of the regulation should continue to be monitored and evaluated to determine whether it makes sense to add more requirements in the future.

Q15. 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?

It is not necessarily a harm, but consideration needs to be given to the impact for second hand device markets, particularly given the desirable shift towards longer device lifespans and less technical waste.

Part 2 — Increase transparency and disclosure

Labelling for smart devices

Q16. What is the best approach to encouraging consumers to purchase secure smart devices? Why?

The government should encourage IoT manufacturers and vendors to ensure reasonable security for smart devices before the devices are on the market, thereby relying less on a label to educate consumers on security differences between products at the point of purchase. However, user awareness plays an important role in security, and consumers would ideally evaluate device security as a routine part of purchasing.

A security label for smart products is worth exploring. While consumers already have access to many generic online resources on how to help secure their smart devices, consumers often have little insight into the presence of security features in a specific smart device prior to purchase, which hinders informed buying decisions. Survey data indicate[23] that many consumers are concerned about the security of smart devices, would find[24] a label communicating security information helpful, and

[23] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950429/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report_V2.pdf

[24] https://arxiv.org/pdf/2002.04631.pdf

would change purchasing behavior[25] based on the label content. However, these studies were limited in scope and more research is needed in live settings to measure the effectiveness of a security label on device purchase decisions.

We suggest the government consider initiating a voluntary pilot program - as the US government is preparing to do[26] - for consumer smart device labeling to conduct such research prior to requiring a security label. A security label should aim to underscore security as a market differentiator for smart devices. To accomplish this, the security label should be developed to achieve the specific purpose of helping purchasers of smart devices make informed choices based on security information communicated through the label. Success metrics for the pilot program should include whether the label is readily understood by consumers, presents the most salient security information for consumers, and is actionable for consumer purchase decisions.

Q17. Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?

Security standards and labeling would likely be an effective combination. As noted above, we encourage additional research on security labels and consumer purchase decisions. However, any security label should add value to consumers beyond regulatory requirements - there is little value in a label that recites security features that a regulation already requires vendors to include in their devices. The label is most useful to make security a differentiator among otherwise similar products. So, if a security regulation requires a baseline of smart device security, the label should enable consumers to distinguish devices that are either not covered by the standard or exceed the baseline.

Voluntary star rating (Option 1)

Q18. 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?

Although we support voluntary labeling program in concept, it is unclear whether there would be sufficient industry uptake of a voluntary label for smart devices in the absence of more data on its effectiveness with consumers. Although there has been encouraging uptake for voluntary labeling in other areas, such as energy efficiency and organic food, there has been less experience and research on whether a security label would affect consumer purchase decisions. Uptake of a voluntary security label would be more likely if a security label does impact consumer purchases or increases the likelihood that consumers will take appropriate security steps, if the label is cost effective for industry, and if multiple large companies participate in the labeling program.

[25] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6980634/pdf/pone.0227800.pdf

[26] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/workshop-and-call-papers-cybersecurity-labeling

Mandatory expiry date label (Option 2)

Q19. Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?

An estimated date through which the device vendor will offer security support is a potentially worthwhile item to include on a security label, but possibly not the most effective item. The date would require additional context - what does security support entail? Over-the-air security updates for the device, or just a toll-free helpline to call if the consumer experiences a security incident? In addition, the date itself is not an accurate indication of the product's security. A label that includes only the date may therefore give consumers a false sense of security, which undermines the purpose of the label.

A potentially more effective approach for conveying a device's actual state of security would be to simply state whether or not the device conforms to a designated security baseline, standard, or best practices framework. In such a scheme, the government (or other public or private sector authority) would recognise multiple credible standards, best practices frameworks, and a smart device security baseline[27] as appropriate security criteria for smart devices. Smart device vendors could self-attest to conformity, but would be penalised for false or misleading attestations. The label would then indicate whether or not the device conforms to a specific standard, framework, or baseline recognised by the labeling program. For example, a smart device that conforms to ETSI EN 303 645 could bear a shield label, and a device that does not conform to any designated framework bears a crossed-out shield label.

The advantage to this system is that conformity to a standard or baseline would give a more representative indication of device security. In addition, it would require less nuance for the consumer to understand what the label means compared to the support timeline alone. However, it would require the government to designate credible standards, best practices, and a baseline for inclusion in the labeling program (such as, but not limited to, ETSI EN 303 645), and conduct enforcement activities against false or misleading attestations. The government should also gather consumer feedback data on whether the label was easily understood and actionable.

Q20. Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?

The class of devices that should be included in the security labeling scheme depends on whether the label would influence consumer behavior to reduce security risk. It is unclear if the security risks presented to consumers by mobile phones can be adequately addressed with a security label that is also used for other consumer smart devices. For example, while weak or shared default credentials are present on some low-cost consumer smart devices, this is not a common vulnerability for most mobile phones (excluding third party apps).

[27] Such as, among others, ETSI EN 303 645, and NIST 8259A.

It would be possible to provide for a labeling scheme that covers both IoT devices and conventional IT. Using the format we propose above, vendors could attest to conformity with designated security standards for mobile phones or secure software development. However, this would require the government to designate non-IoT security frameworks, in addition to IoT security frameworks, for inclusion in the labeling program. Presently, Home Affairs' proposal refers to alignment with ETSI EN 303 645[28] (which also forms the baseline in Singapore's labeling scheme) - but this is a consumer IoT standard.[29] The government would also need to ensure the label provides salient and understandable security information to consumers about mobile phones, while still presenting a consistent format to consumers to avoid impeding their decision making with too many different security labels.

This level of complexity may not be warranted at this stage, as we recommend the government first aim to gather more data about the effectiveness of a security label for smart devices - before moving on to mobile phones.

Q21. Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?

"Labeling" should be understood to include many forms of communication, not just a physical sticker on a physical product. The "label" concept centers on transparency and effective communication of information to consumers prior to purchase. A "label" could include, for example, e-labels, or dynamic text in a product description listed in an online marketplace. The format should be adapted for the context in which the consumer is considering purchase of the product.

Regardless of the precise format, we recommend that the government explore a layered approach in which the consumer is first presented with high level information, but is then able to access more detailed information hosted elsewhere (such as a product information webpage via a link or QR code). For example, the consumer-facing layer could include a symbol or phrase indicating participating in the labeling program, as well as the most critical security features related to that device. This layer would also include a pathway (such as a link) to the second layer. This second layer would provide more detailed information, such as the specific security standards to which the device conforms, the steps the consumer should take to secure the device, etc.[30]

[28] Pg. 38, https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf
[29] We also recommend consideration of NISTIR 8259A as an IoT security baseline. https://csrc.nist.gov/publications/detail/nistir/8259a/final
[30] https://iotsecurityprivacy.org/

Responsible disclosure policies

Q22. Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

Vulnerability disclosure processes are increasingly recognised as a key cybersecurity activity that should be included as a basic component of organisational cybersecurity program. Existing standards and guidance have strengthened general consensus around best practices for coordinated vulnerability disclosure, leading to greater consistency in implementation and expected outcomes. Establishing a coordinated vulnerability disclosure and handling process can help organisations detect and respond to vulnerabilities reported to them by external and internal sources, leading to mitigations that enhance security, data privacy, and safety.

Voluntary guidance would likely encourage some Australian businesses to implement vulnerability disclosure policies. We encourage Home Affairs to issue such guidance, and to ensure it is aligned with international standards and current industry best practices, such as ISO/IEC 29147 and ISO/IEC 30111. In addition to standalone guidance to vulnerability disclosure, we suggest the government also incorporate vulnerability disclosure into recommended cybersecurity practices in sectoral guidance and best practices, as the government has done with its IoT Code of Practice guidance for manufacturers[31] - again, with reference to international standards.

To further encourage businesses to adopt coordinated vulnerability disclosure practices, we highly recommend civilian Australian government agencies at all levels adopt internal vulnerability disclosure policies, and provide those agencies with the necessary resources to implement the policies.[32] This was recently implemented in the United States among federal civilian agencies.[33]

Health checks for small businesses

Q23. 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?

Rapid7 is generally supportive of efforts to create more transparency and accountability around cybersecurity, and efforts to enable consumers of products or services to make more informed buying choices that factor in cybersecurity. In principle, the health check program would do this, but the efficacy will be determined by the details of what is covered, how small businesses are held accountable to the information provided, and the degree of adoption. The biggest challenge with a scheme like this is how to drive outcomes that create real impact without over-burdening small businesses, which as noted in the proposal, have "limited time, limited money and limited cyber

[31] https://www.cyber.gov.au/acsc/view-all-content/publications/iot-code-practice-guidance-manufacturers
[32] Pg. 9, https://www.cybersecuritycoalition.org/policy-priorities
[33] https://cyber.dhs.gov/bod/20-01/

security expertise." It is unclear whether most small businesses will really have sufficient resources and capability for a meaningful self-assessment.

Additionally, it is likely there will be a certain bias in terms of the organisations that will engage on a voluntary scheme such as this. It is most likely to be organisations that are already engaged on cybersecurity topics - for example cloud providers or financial institutions - as those are the ones that are likely to see demand from their customers for security information. While having the check mark will make it easier for these businesses to respond to requests for information on cybersecurity, the scheme is unlikely to create much additional impact in sectors that are not currently engaging on cybersecurity.

Q24. Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

As noted above, small businesses operating in areas that already prioritise some level of cybersecurity engagement and information will likely benefit. The health check scheme will make it easier for businesses in these areas to communicate security information with their potential customers, and will streamline the kinds of information being provided, which in turn, may benefit the customers. This can eliminate some of the friction in the procurement process and potentially reduce the cost of sale for small businesses.

These benefits will likely only be realised in sectors that already engage in cybersecurity discussions.

* * *

Thank you for giving us the opportunity to share our views. For any additional questions or feedback, please contact Jen Ellis at [redacted].