Office of the Victorian Information Commissioner

t 1300 006 842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D21/13949

27 August 2021

Cyber, Digital and Technology Policy Division
Department of Home Affairs

By email: techpolicy@homeaffairs.gov.au

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

Thank you for the opportunity to make a submission in response to the discussion paper 'Strengthening Australia's cyber security regulations and incentives – A call for views' (**discussion paper**).

The Office of the Victorian Information Commissioner (**OVIC**) has a unique regulatory focus, with combined oversight of privacy, information security and freedom of information in Victoria, administering both the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) and the *Freedom of Information Act 1982* (Vic).

As the only jurisdiction in Australia with legislated information security standards, OVIC is at the forefront of information security regulation in Australia. Since 2014, OVIC has been responsible for setting the Victorian Protective Data Security Standards (**Victorian Standards**), and monitoring and assuring the security of public sector information against the Standards, under the Victorian Protective Data Security Framework (**Victorian Framework**). Part 4 of the PDP Act provides authority for developing the Victorian Framework and setting the Victorian Standards.

Consequently, the concepts and terminology used in the discussion paper are familiar to OVIC. For example, the definition of 'cyber security incident'[1] in the discussion paper is similar to the Victorian Framework and Standards' reliance on protective data security principles to maintain the confidentiality, integrity and availability of digital and non-digital public sector information.

This submission responds to questions in chapters 2-9 and 11 of the discussion paper.

Chapter 2: Why should government take action?

Response to question 1 – What are the factors preventing the adoption of cyber security best practice in Australia?

1. In addition to the factors identified in the discussion paper,[2] OVIC notes that cyber security is a niche field, requiring specialised knowledge, skills, and capability. As a result, it is understandable that the average small medium enterprise (**SME**), and some large businesses:

    - do not know that their business is vulnerable to cyber security incidents;

[1] Discussion paper, chapter 1, page 5: 'cyber security incident' is defined as 'a single event or series of events that threatens the integrity, availability or confidentiality of digital information'.
[2] Discussion paper, chapter 2, pages 9-11.

- do not understand how to implement safeguards to prevent and respond to cyber security incidents; and

- encounter financial difficulties and resourcing issues that prevent the adoption of best practice cyber security measures.

2. This has been OVIC's experience in regulating and upskilling the Victorian public sector. It is not that public servants and contract service providers do not want to protect the security of public sector information. It is that they need funding, resources, education, and assistance to do so.[3]

3. The majority of Victorian public sector agencies are small and only some larger government agencies have dedicated information security staff. OVIC, through its ongoing stakeholder engagement program, aims to improve information security capability and uplift among Victorian public sector agencies. In OVIC's experience there is great appetite for upskilling in information security, however the lack of capability, funding and resources remain obstacles that could be addressed through funding of skills-based positions as well as education and awareness.

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

4. As the discussion paper highlights,[4] there are a number of clear and evident negative externalities and information asymmetries impacting the adoption of effective cyber security practices by business. It is difficult to conceive how these factors can or could be overcome without government intervention.

5. The increasing threat environment, combined with a lack of knowledge, capability, and resources to implement effective cyber security, means that government must do more to put cyber security on the agenda, and to set the expectations of what is required to implement effective cyber security. The need for effective cyber security will only grow stronger, and Australia will only become more vulnerable if action is not taken. Since the introduction of the Victorian Framework and the Victorian Standards, OVIC has seen information security become an agenda item at the executive level, rather than stay at the practitioner level. This is because Part 4 of the PDP Act makes the agency Head accountable for information security by requiring the agency Head to sign the agency's Protective Data Security Plan (**PDSP**) that is submitted to OVIC, and annually attest to OVIC that the agency's security program meets the requirements of the Victorian Standards.

6. Additionally, since the introduction of the Victorian Standards, OVIC has anecdotally observed a shift wherein the responsibility for information security sits within an agency. In the 2018 PDSP reporting cycle, OVIC observed that IT teams typically led information security programs within their agency, however it now appears there has been a shift towards corporate services taking ownership of information security. Rather than purely an IT responsibility, information security is now seen as a whole-of-agency responsibility.[5]

[3] Public sector agencies subject to the Victorian Standards are required to submit a Protective Data Security Plan (**PDSP**) to OVIC every two years. In the 2020 PDSP reporting period, over one in three responses (35.88%) identified that capability was a challenge or barrier to the adoption of best practice information security measures prescribed by the Victorian Standards. Higher rated challenges and barriers include financial (46.18%) and resourcing (76.08%), while comparably lower rated challenges and barriers include third-party arrangements (32.56%), lack of understanding around the Victorian Standards (21.93%) and lack of clarity around roles and responsibilities within the agency (21.93%).
[4] Discussion paper, chapter 2, pages 10-11.
[5] OVIC has not been able to draw direct comparisons between our 2018 and 2020 reporting periods because of the significant changes to the Victorian Standards during these periods.

Chapter 3: The current regulatory framework

Response to question 3 – What are the strengths and limitations of Australia's current regulatory framework for cyber security?

7. The strengths of utilising high-level, risk-based principles in a regulatory framework include:

    - High level principles can be adapted to all types of organisations (small organisations with few employees through to large corporations), because the organisation is required to implement the principles through specific controls that are relevant to that organisation.

    - Risk-based principles ensure that controls are implemented for a particular purpose and are tailored to the circumstances of the organisation, rather than a compliance-based model where controls are implemented because the organisation was told to do so.

8. OVIC agrees with the limitations identified in the discussion paper[6] and would add the following additional limitations of Australia's current regulatory framework:

    - There is no legislated regulation of cyber security at the federal level:

        – The *Privacy Act 1988* (Cth) (**Privacy Act**) only applies to personal information. The narrow-scope and difficulties in determining what is 'personal information' and therefore subject to the Privacy Act in the digital world, is one of the matters being considered in the current review of the Privacy Act. Regulating cyber security by first requiring an assessment of whether data is or is not personal information is ineffective and incomplete.

        – Cyber security incidents involve a compromise in the confidentiality, integrity or availability of any or all digital information held by a business, not just personal information. For example, a ransomware attack affects the availability of all information held by a business, not just its personal information holdings, and the harmful effects of a ransomware attack on the economy and Australian society are different to the harms that flow from interferences with information privacy.

        – The limitation of using the Privacy Act and Australian Privacy Principle (**APP**) 11 to regulate cyber security in the public and private sectors is significant and will continue to be a problem until there is legislation that squarely regulates cyber security, and more broadly, information security.

    - To be effective, high-level principles require an understanding of security risk management. As security has traditionally been compliance based, it would be wrong to assume that a risk-based approach to security is well understood by organisations. In Victoria, the move to a risk-based approach in the Victorian Standards has required OVIC to develop extensive supporting resources to explain foundational concepts, and to guide agencies through the risk assessment process. The Australian framework would benefit from similar supporting resources, to help empower organisations to implement security controls based on their own security risks.

    - Equally, high-level frameworks lack granularity to enable individual organisations to implement principles in practice. To overcome this in the Victorian Standards, OVIC developed security measures called 'elements' to support each standard. The elements set the expectations of what is meant by each standard, and guide the implementation of each standard. Unlike a compliance model, the elements still retain a level of flexibility, by allowing public sector agencies to choose the individual controls to implement under each element, that best respond

[6] Discussion paper, chapter 3, pages 15-16.

to the agency's particular circumstances. A similar approach could be taken to regulating cyber security.

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

9. A key theme borne out from the topics raised in the discussion paper is that Australia does not have any legislation at the federal level regulating cyber security, and Australia does not have a regulator at the federal level with the relevant skills, expertise and resources to develop, administer, monitor and assure cyber security standards for the private sector.

10. This is a significant limitation on the goal of strengthening Australia's cyber security regulations that is not addressed in the options for reform set out in the discussion paper. That is, there are no proposed options to introduce legislation that would directly regulate cyber security and no proposed options to equip Australia with a cyber security regulator.

11. A second key theme in the discussion paper is that voluntary standards for the private sector, with no regulatory oversight, are ineffective in strengthening the private sector's ability to prevent and respond to cyber security incidents. The discussion paper notes that there are weak commercial incentives to make the right investments in cyber security and that businesses find it difficult to compete on the basis of cyber security.[7] That is, there is a market failure and little incentive for businesses to uplift cyber security, whether a voluntary standard exists or not.

12. The discussion paper draws attention to the UK government's decision in January 2020 to introduce a legislated standard for smart devices, because its voluntary *Code of Practice for Consumer IoT Security* did not have sufficient uptake.[8] Despite knowledge of the UK's experience, Australia adopted a voluntary Internet of Things Code of Practice in September 2020. The discussion paper notes that industry uptake of the Internet of Things Code of Practice is low, even for low-cost high priority recommendations.[9]

13. With the above themes in mind, OVIC makes two specific recommendations that would improve clarity, coverage, and enforcement:

    - ***Recommendation 1***: Legislate not only cyber security requirements, but information security requirements more broadly.

    - ***Recommendation 2****:* Equip one regulator to oversee and enforce the new information security requirements.

Recommendation 1: Legislate not only cyber security requirements, but information security requirements more broadly

14. To address the limitation of not having any federal legislation regulating cyber security, OVIC recommends these requirements be regulated via legislation in a similar manner to Part 4 of the PDP Act. This could be achieved by developing standalone legislation, or inserting a new part into an existing regulatory framework, such as the Privacy Act. Further, OVIC suggests that any legislative reform should regulate the broader concept of information security, not just cyber security. Information comes in all formats, not just digital, and represents a security risk whether it is digital or not.[10]

[7] Discussion paper, chapter 2.
[8] Discussion paper, chapter 6, page 32.
[9] Discussion paper, chapter 6, page 31.
[10] For further information see paragraphs 69-71 of this submission, in response to question 28 of the discussion paper.

15. Legislating "information security" recognises that cyber security is only one facet of good information security risk management. In Victoria, the PDP Act uses the term "data protection", which is not an accurate description of the subject matter that is regulated under Part 4 of the PDP Act. Recognising this, OVIC uses the term "information security" in its guidance and messaging (outside of legislation), to ensure that stakeholders are not misled into thinking they only need to secure electronic information.

16. Any reform to regulate information security via legislation:

    - should cover all types of information held by an organisation (for example, financial, operational, critical infrastructure, legal and personal information). This would address the current limitation, as recognised in the discussion paper,[11] of using the Privacy Act to regulate the cyber security of all information, when the Privacy Act only regulates personal information.

    - should apply to both the Commonwealth public sector and the private sector. This would promote greater trust in the Government's own cyber security capabilities and greater trust for consumers to participate in the economy, because they will be able to rely on the private sector meeting legislated baseline cyber security standards.

17. Victoria's legislated information security Framework and Standards leads the way in Australia and provides a positive precedent for what regulatory reform might look like at the national level. Part 4 of the PDP Act outlines the protective data security (information security) requirements of regulated entities – and the obligations of OVIC as a regulator – with a focus on maintaining the confidentiality, integrity, and availability of public sector data and data systems.[12] The Victorian Standards, updated in 2019, reflect and are expressly cross-referenced to national and international best practice approaches towards information security, tailored to the Victorian public sector environment. The Victorian Framework, updated in 2020, monitors and assures the security of public sector information and information systems across the Victorian public sector and provides a model for monitoring and measuring the extent to which regulated entities implement the Victorian Standards and comply with the PDP Act.[13]

18. Recommendation 1 should be kept front of mind, as an effective solution for implementing the mechanisms and achieving the outcomes discussed in chapters 4 and 5 of the discussion paper, and which are discussed later in this submission.

Recommendation 2: Equip one regulator to oversee and enforce the new information security requirements

19. Given that many private sector businesses appear unlikely to improve their ability to prevent and respond to cyber security incidents on their own, regulatory oversight will likely be required to properly respond to the issues identified in Part 1 of the discussion paper. The discussion paper identifies the Office of the Australian Information Commissioner (**OAIC**) as a regulator that could respond to the issues identified in chapter 5. However, as noted in the discussion paper, a limitation of the current regulatory environment overseen by the OAIC, is that the Privacy Act only regulates personal information, not all information.[14] Chapters 4 and 6 state more generally that a regulator does not exist and would need to be found if the proposed reform options are adopted.[15]

[11] Discussion paper, chapter 5, pages 25 and 27.
[12] 'Public sector data' is defined in section 3 of the PDP Act as 'any information (including personal information) obtained, received, or held by an agency or body to which Part 4 applies, whether or not the agency or body obtained, received or holds that information in connection with the functions of that agency or body'.
[13] Further information about Victoria's legislated security framework can be found in OVIC's submission to the 'Protecting Critical Infrastructure and Systems of National Significance' Consultation Paper, available here https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/Submission-040-Office-of-the-Victorian-Information-Commissioner.PDF.
[14] Discussion paper, chapter 5, pages 25 and 27.
[15] Discussion paper, chapter 4, page 22 and chapter 6, page 33.

20. OVIC's view is that only one regulator, not multiple regulators, should be tasked with responding to the issues raised in chapters 4, 5 and 6. Properly resourcing only one regulator will reduce the costs to government, and the compliance burden and regulatory confusion for business.

21. Of the existing Commonwealth regulators, the OAIC appears to be the most appropriate given the Information Commissioner is already tasked with regulating information privacy of the private sector, which includes the APP 11 requirement to take reasonable steps to protect personal information.

22. However, to be an effective regulator, the OAIC would require significantly more staff and resources to enable it to carry out any new functions and responsibilities. The OAIC's educatory function, to publish guidance and support businesses to respond quickly to a changing environment, would be particularly important to the success and uplift of cyber security practices in the private sector.

23. If the OAIC is chosen as the regulator, the small business exemption should be removed from the Privacy Act. If it is not removed, 97.4%-98.4% of all businesses in Australia[16] would be left unregulated.

Chapter 4: Governance standards for large businesses

Response to question 5 – What is the best approach to strengthening corporate governance of cyber security risk? Why?

24. OVIC understands the discussion paper is looking at ways to apply cyber security governance standards to a wider range of businesses than critical infrastructure owners and financial institutions who are covered by the *Security of Critical Infrastructure Act 2018* and APRA's prudential standard respectively. OVIC understands feedback is sought on the best way to encourage stronger cyber security risk management within large businesses. The discussion paper outlines two options: (1) a voluntary governance standard or (2) a mandatory governance standard.

25. OVIC understands that the governance standard is intended to be high-level and may include principles to describe the responsibilities of large businesses and processes for managing cyber security risk.[17] OVIC agrees it is important to have adequate governance arrangements in place for large businesses. The governance arrangements should denote who is responsible for cyber security; to document risks, review cycles, policies and procedures, and ensure adequate information lifecycle and access control, and robust HR policies.

26. OVIC's view is that a *voluntary* standard is unlikely to be successful. A voluntary standard relies on the goodwill of large businesses, operating in an economic and regulatory environment that requires businesses to preference their own interests. As noted in the discussion paper, this necessarily curtails the ability for the market to effectively protect against cyber security incidents.[18] OVIC's view is that a voluntary governance standard would head the same way as the voluntary Internet of Things Code of Practice. That is, it will likely have minimal uptake and be ineffective.

27. OVIC instead recommends the adoption of a *mandatory* standard. A mandatory standard will likely result in businesses taking cyber security seriously and will ensure that cyber security is a priority of company boards. As previously noted, the mandatory Victorian Standards have proven to be successful in putting information security on the agenda at the executive level.

[16] The Australian Small Business and Family Enterprise Ombudsman, *Small Business Counts December 2020*, available at https://www.asbfeo.gov.au/sites/default/files/ASBFEO%20Small%20Business%20Counts%20Dec%202020%20v2.pdf.
[17] Discussion paper, chapter 4, page 20.
[18] Discussion paper, chapter 2.

28. Under a mandatory standard, consideration should be given to the type of assurance that needs to be given by businesses, and to whom. Under the Victorian model, the agency Head is required to annually attest to the agency's compliance with the Victorian Standards. This requirement has introduced accountability for information security and resulted in improvements to the way security is implemented, discussed, and managed by agencies. A mandatory governance standard for large businesses may consider adopting a similar approach to the Victorian model.

29. The Victorian model uses a risk-based approach to implementing the principles in the Victorian Standards. OVIC has found this model works well, as security in practice is risk-based. A governance standard based on high level principles, would allow businesses to use a risk-based approach to implementing the principles according to their own unique operating environment, and has the potential to result in best practice, rather than bare minimum compliance. However, the success of a principles-based approach relies on good risk management, which is not universally understood and can be difficult to achieve in practice without the right skills, capability, support, and guidance. If a principles-based approach is taken, the government should commit to resourcing improved education around risk management and provide ongoing support for businesses as they implement the principles.

30. On balance, OVIC's view is that a combination of risk-based governance standards and compliance with minimum technical standards (discussed in chapter 5 of the discussion paper) is appropriate for larger businesses.

31. Given that large businesses would be required to comply with the two regulatory approaches (outlined in chapters 4 and 5 respectively), consideration could be given to creating only one mandatory standard, that includes the governance standards for large businesses sought in chapter 4 and the technical requirements for all businesses sought in chapter 5 of the discussion paper. One set of standards has the potential to reduce the regulatory burden on large business as they will only be required to help co-design and comply with one set of standards, not two.

32. One set of standards also improves applicability, as it will be easier for businesses to enter agreements, if the parties to the agreement are already aware of and implementing the same requirements. Even though the risk-based principles in the standard would not be coupled with an assurance program for small businesses, the existence of the principles in the same document as enforceable minimum technical standards, would help to convey the message to small business that cyber security is important.

33. Finally, if there is to be a reporting requirement as part of the standards, consideration should be given to harmonising similar reporting requirements that businesses may have with other regulators, and improving the ability for regulators to share information, so that businesses only report once.

Response to question 6 – What cyber security support, if any, should be provided to directors of small and medium companies?

34. As previously noted, SMEs are unlikely to possess the required level of knowledge, skill and capability to manage the risks of cyber security incidents. Based on OVIC's experience regulating small agencies in the Victorian public sector, enhanced cyber security and risk-management education will be necessary to build organisational capability and security awareness. To reach the breadth of small and medium companies in Australia, there would likely need to be significant investment in awareness raising initiatives through professional associations, social media and broadcast media.

35. Education and guidance will be a key role for the chosen regulator, in uplifting the cyber security practices of the private sector. In OVIC's experience, an effective regulator will, at a minimum, require resources to promote the standards, raise security risk management awareness, undertake

stakeholder engagement and outreach activities, develop specific guidance, deliver training and awareness through various mediums, conduct reviews and audits of organisations, and develop and share insights.

Response to question 7 – Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

36. As mentioned earlier, cyber security is a specialised field, which means that businesses are unlikely to possess the required level of knowledge, skill, and capability to manage the risks of cyber security incidents. As such, additional education and awareness raising initiatives will also be required.

37. Once again, the chosen regulator is likely to play a key role in education and awareness raising initiatives, if properly resourced. For example, OVIC has published an information sheet that contains suggested questions an Audit and Risk Committee can ask of its agency, to identify how its Standards uplift program is progressing and how assurance will be achieved.[19] This type of guidance is likely to be useful for senior business leaders, to help them understand their businesses cyber security risks and how the business will implement a mandatory standard.

Chapter 5: Minimum standards for personal information

Response to 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?

38. The heading to the chapter is about minimum standards for personal information. However, the content of the chapter primarily looks at the need for minimum technical standards to encourage uptake of cyber security best practices.[20]

39. OVIC supports the proposal to create minimum technical standards that would apply to all businesses not already covered by a higher level of technical standards. Minimum technical standards will make it clear to businesses what they need to do and has the greatest potential to create a baseline level of resilience to cyber security incidents across the Australian economy.

40. The discussion paper notes that creating an enforceable code under a federal piece of legislation is one option to increase the adoption of cyber security standards across the economy.

41. The discussion paper then notes that there is no single existing Act that governs cyber security expectations across the whole economy. The discussion paper puts forward the option of establishing a code under the Privacy Act to set "broad cyber security standards (albeit only in relation to personal information)".[21] The discussion paper notes two serious limitations of this approach, namely that the Privacy Act only protects personal information and does not apply to businesses with an annual turnover of less than $3 million.[22]

42. To overcome the two serious limitations of using the Privacy Act to regulate information security, as stated in paragraphs 14 to 18 above, OVIC recommends developing standalone legislation, or inserting a new part into an existing regulatory framework, such as the Privacy Act, to regulate information security.[23]

[19] OVIC, 'Top Questions for the Audit and Risk Committee Members', available at https://ovic.vic.gov.au/data-protection/top-questions-for-the-audit-and-risk-committee/.
[20] Discussion paper, chapter 5, page 24.
[21] Discussion paper, chapter 5, page 25.
[22] Discussion paper, chapter 5, page 27.
[23] If a new Part is introduced into the Privacy Act, the small business exemption should be repealed.

43. If OVIC's recommendations are not considered feasible, a code under the Privacy Act would be better than no regulatory framework at all. However, OVIC's notes the following matters of concern:

    - An attempt to regulate cyber security, or using a legislative mechanism, that is not designed for this purpose may be detrimental to the overall policy objectives, and will result in a need for further reform sooner rather than later.

    - At present, the Privacy Act does not apply to small businesses. Consequently, a Privacy Act code would only apply to the same audience as chapter 4's proposed governance standards, leaving 97.4%-98.4%[24] of all businesses in Australia unregulated.

    - If the proposal in chapter 4, to create governance standards for large business (either voluntary or mandatory) proceeds, the introduction of a Privacy Act code would result in two separate pieces of regulation for large businesses to design and comply with, and potentially two regulators to report to.

44. OVIC suggests that consideration be given to merging option 2 in chapter 4 and option 1 in chapter 5 of the discussion paper, so there is only one mandatory standard, that includes both high level governance principles and baseline technical standards, overseen by an appropriate regulator. As OVIC has recommended, this could be achieved by legislating information security requirements.

45. However, if the preference is to use the Information Commissioner's code making powers in Part IIIB of the Privacy Act, as suggested in the discussion paper,[25] OVIC draws attention to and agrees that the following recommendations in the OAIC's submission to the Privacy Act Review[26] should be implemented as part of the Attorney General's Department's current review of the Privacy Act:

    - Recommendation 14, to amend the APP code framework in the Privacy Act, to give the Information Commissioner greater flexibility and discretion to develop APP codes; and

    - Recommendation 68, to amend the Privacy Act to provide an express power for the Information Commissioner to share information with other bodies where necessary, including other regulators and government agencies. With respect to cyber security, it will be particularly important for the Information Commissioner to be equipped with power to share information with the Australian Cyber Security Centre (**ACSC**), as appropriate.

46. For this proposed reform to be effective, the OAIC would need to be properly staffed and resourced to co-design, oversee, and enforce minimum technical standards.

Response to 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)?

47. The discussion paper considers it unrealistic to mandate the Australian Signals Directorate's Essential 8 (**Essential 8**)[27]. However, while OVIC agrees that mandatory standards are more difficult to implement and enforce than risk-based standards, a code could provide items drawn from the Essential 8 in a series of Elements informing risk-based standards. At the very least a code should include the examples given on page 24 of the discussion paper of some of the Essential 8.[28]

---

[24] The Australian Small Business and Family Enterprise Ombudsman, *Small Business Counts December 2020*, available at https://www.asbfeo.gov.au/sites/default/files/ASBFEO%20Small%20Business%20Counts%20Dec%202020%20v2.pdf.
[25] Discussion paper, chapter 5, page 26.
[26] OAIC, *Submission to Privacy Act Review – Issues Paper*, available at https://www.oaic.gov.au/assets/engage-with-us/submissions/Privacy-Act-Review-Issues-Paper-submission.pdf.
[27] Discussion paper, chapter 5, page 26.
[28] The examples given are encryption of data in transit and at rest, strong passwords, multi-factor authentication and timely application of critical patches.

48. The mitigation strategies in the Essential 8 are informed by the ACSC's experience in responding to cyber security incidents.[29] OVIC's view is that unless businesses can demonstrate justifiable reasons why they cannot implement the Essential 8, the Essential 8 provide a good starting point and baseline level of protection.

49. In the longer term, Australia could look towards adopting international standards, such as those in the ISO/IEC 27000 series (for example, ISO/IEC 27001 and ISO/IEC 27002).[30] Adopting international standards would fulfil one of the stated purposes of a cyber security code, which is to "harmonise international standards and offer opportunities to Australian businesses to market their security credentials internationally".[31] It also aligns with the best practice principles in the discussion paper to apply international standards where relevant to reduce regulatory burden.[32]

50. As stated in the discussion paper, avoiding conflicts between a future code and existing guidance will be important. In OVIC's view, creating a future code that sets different expectations to the requirements in the Essential 8 can undermine the good work that has gone into uplifting and maturing information security thus far.

51. Whilst adopting specific technical standards in a code may result in the need to update the code more regularly than a principles-based code, this could be mitigated by amending the Information Commissioner's code making power, to provide greater flexibility for the OAIC to update the baseline requirements as the threat environment evolves.

Response to 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?

52. If the intention of the code is to include only minimum technical standards, in OVIC's view the code should apply to all technologies, sectors and types of data. This will help to future-proof the code and makes it easier for businesses and the wider public to understand what is required and by whom. Picking and choosing specific sectors, technologies and types of data would not appear to solve the stated intention of this reform, which is to increase the adoption of cyber security standards across the economy[33] and would not overcome one of the stated common barriers to standards adoption, which is uncertainty about which standards to adopt.[34]

Chapter 6: Standards for smart devices

Response to question 11 – What is the best approach to strengthening the cyber security of smart devices in Australia? Why?

53. The discussion paper proposes a mandatory standard for smart devices, following in the footsteps of the UK's decision to introduce a legislated standard for smart devices after finding that its voluntary *Code of Practice for Consumer IoT Security* did not have sufficient uptake.[35]

54. OVIC agrees with the proposal to adopt a mandatory standard and recommends that, similar to the UK, smartphones be included in the scope of the new reforms.[36] The inclusion of smartphones is particularly important given the recent revelations of wide-spread use of covert spyware on

[29] See Australian Cyber Security Centre, 'Strategies to Mitigate Cyber Security Incidents' available at https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.
[30] See ISO, 'Popular Standards' available at https://www.iso.org/isoiec-27001-information-security.html.
[31] Discussion paper, chapter 5, page 27.
[32] Discussion paper, Appendix B, page 60.
[33] Discussion paper, chapter 5, page 26.
[34] Discussion paper, chapter 5, page 25.
[35] Discussion paper, chapter 6, page 32.
[36] See Discussion paper, chapter 6, page 32.

smartphones, uncovered by the Pegasus Project.[37] A mandatory standard could assist in preventing this serious invasion of privacy and cyber security incident from occurring in future.

Part 2 – Increase transparency and disclosure

Chapter 7: Labelling for smart devices

Response to question 20 – Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?

55. The discussion paper does not explain why mobile phones are being considered for exclusion from both a voluntary and mandatory labelling scheme. In OVIC's view there is no reason in the public interest for mobile phones to be excluded.

56. Mobile phones are almost ubiquitous in Australian society. The mobile phone is on our person, or within arms-reach, wherever we go. Mobile phones also hold significant amounts of personal information of their owner, such as private messages, photographs, contacts, location history and documents. A mandatory labelling scheme would go some ways to assist consumers in understanding the level of cyber security of their device and its vulnerability to cyber-attacks. The recent revelations of the Pegasus Project further bring home the importance of uplifting the security of the mobile phone.

Chapter 8: Responsible disclosure policies

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

57. In OVIC's view, visibility and accessibility of the guidance is critical to achieving the desired policy outcome. As such, it may be more appropriate to include the guidance in the governance standards/code, rather than as a stand-alone, isolated, document.

Chapter 9: Health checks for small businesses

Response to 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?

58. A self-assessed health check for SMEs may assist to improve Australia's cyber security. However, this should not be coupled with the use of a trust mark. When applied to services rather than products, trust marks require an ongoing assurance process to ensure the service remains trustworthy. In OVIC's view, trust marks are not viable in cybersecurity, where environmental conditions can change at any moment, rendering the trust mark untrustworthy. Further, as highlighted below in paragraphs 66-68, elements of this proposal are problematic unless there is some level of oversight and audits on self-assessments undertaken by SME's.

59. For the health check program to gain credibility and widespread adoption, it should align where possible with established standards to allow comparisons to be made and a consistent application.

60. There are numerous international standards about supply chain risk (that are currently being reviewed for currency). For example, ISO 28000 Security Management System for the Supply Chain and ISO 27036 Information security for supplier relationships. There are also certifications that businesses can achieve to show their stakeholders that they have a certain level of security. For example, the ISO 27001 certification.

[37] For further information see https://www.theguardian.com/news/series/pegasus-project.

61. Certification is also not the end of the story and creates the risk of a 'tick and flick' mode of compliance. There is a misconception that systems that are 'certified' just need to be installed with nothing further to be considered.

62. We should be wary of businesses relying on a health check and taking no other ongoing assurance measures. The threat environment is continually evolving, and businesses should have security programs that are adaptive, suitably resilient, and built with continual improvement in mind.

63. Businesses will also need to confirm the scope and coverage of the health check. For example, a health check may only have been applied to the finance area, not the sales and product area of the business.

64. These are reasons why a risk-management approach is crucial and why there should be education about the role a health check program plays in relation to a business's overall information security management framework.

Response to 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?

65. When engaging a third-party business, a business should still undertake its own due diligence to confirm the third party's claims and make a risk informed decision. However, a health check program would certainly uplift the discussion and knowledge around cyber security and provide an at-a-glance indicator that the third-party business is trying to do the right thing. If coupled with a set of common standards and elements, and a regulator empowered and funded to carry out assurance, supply chain businesses and customers would be better assured as to the level of cybersecurity of the small business.

Response to question 25 – Is there anything else we should consider in the design of a health check program?

66. Self-assessments by their very nature are not independently verified and therefore need to be taken with a grain of salt. However, as a regulator, OVIC understands there is no other cost-effective way to implement such a program, given the high number of SMEs.

67. OVIC recommends governance arrangements are built around the program before it commences. For example, it will be important to ensure that an auditor or regulator is tasked and resourced to check self-assessments. If there are no governance arrangements to check self-assessments, SMEs are likely to err on the positive side of the assessment.

68. OVIC recommends, as far as is possible, that health checks reflect a scaled assurance model of the minimum standards discussed in chapters 4 and 5 of the discussion paper. That is, there should be minimum standards set across the board for all types of businesses, and the model for implementation and assurance is scaled. For example, low to medium risk businesses complete a self-assessment, and large enterprises are required to obtain certification that is independently verified. This will ensure that consistent standards are applied across the Australian economy, and management of the program is cost-effective and scalable to the risk posed to Australia's national interest from a cyber security incident.

Chapter 11: Other issues

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

69. It is important that any proposed policies consider all aspects of cyber security, not just ICT.

70. If a cybercriminal gains unauthorised access to a server room and infiltrates a network, it's just as much a **physical** security issue as a cyber issue. If an employee gains unauthorised access to a network and uses it for malicious purposes, this is a **personnel** security issue. If sensitive information is being leaked or miscommunicated, adequate control over **information** security may be lacking.

71. The security areas of people, process and technology must be considered equally. Even if the system purchased is "secure", the way in which it is used from the end user perspective also plays a role. A high percentage of cyber security incidents have a human element.[38] For example, a device can have the best threat protection mechanisms, but if people are not locking the device after use, it can represent a new set of issues. It is therefore important that education around cyber hygiene is a focus of any new strategy to uplift the cyber security practices of the private sector.

Thank you again for the opportunity to make a submission on strengthening Australia's cyber security regulations and incentives. I have no objection to this submission being published without further reference to me. I also propose to publish a copy of this submission on the OVIC website but would be happy to adjust the timing of this to allow you to collate and publish submissions proactively.

If you would like to discuss this submission, please do not hesitate to contact me directly or my colleague Emma Stephens, Senior Policy Officer, at [redacted]

Yours sincerely

[redacted]

Sven Bluemmel
Information Commissioner

[38] 85% of the data breaches in the Verizon data breach investigations report had a human element: Verizon (DBIR) 2021 https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf.