Office of the Victorian Information Commissioner

**Phone:** 1300 00 6842
**Email:** enquiries@ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

5 April 2023

Expert Advisory Board
Department of Home Affairs

**By email only:** auscyberstrategy@homeaffairs.gov.au

Dear Expert Advisory Board,

**Submission in response to the 2023-2030 Australian Cyber Security Strategy Discussion Paper**

Thank you for the opportunity to make a submission in response to the 2023-2030 Australian Cyber Security Strategy Discussion Paper (**discussion paper**).

My office, 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 relevant regulator in the only jurisdiction in Australia with legislated information security standards, OVIC considers it is able to provide unique and valuable insights into cyber security matters.

This submission outlines the Victorian approach to regulating information and cyber security, and responds to questions 2, 5, 6, 13 and 15 of the discussion paper. Where relevant, this submission directs the Expert Advisory Board to OVIC's views expressed in previous submissions in response to consultations on:

- amendments to the *Security of Critical Infrastructure Act 2018* (Cth) (see OVIC submission);
- *Strengthening Australia's Cyber Security Regulations and Incentives* (see OVIC submission); and
- *National Data Security Action Plan* (see OVIC submission).

## Victorian approach to regulating information and cyber security

1. OVIC is responsible[1] for setting the Victorian Protective Data Security Standards (**Victorian Standards**)[2] and monitoring and assuring the security of public sector information and information systems (data systems) against the Victorian Standards, under the Victorian Protective Data Security Framework (**Victorian Framework**).[3]

2. The Victorian Framework, Standards, and accompanying guidance materials are designed to assist entities to mitigate information security risks and build the information security capability and maturity of the Victorian public sector (**VPS**). The reporting mechanisms under the Framework provide OVIC with insight into information security practices across the VPS.

3. Part 4 of the PDP Act provides authority for developing the Victorian Framework and setting the Victorian Standards. Over 3,000 VPS organisations are bound by Part 4 of the PDP Act.[4]

4. Part 5 of the PDP Act specifically highlights law enforcement and crime statistics data security as special cases within the broader framework of information security. Part 5 establishes OVIC's jurisdiction over Victoria Police and the Crime Statistics Agency with respect to their data, data systems and protective data security practices.

5. The Victorian Framework and Standards regulate all public sector information (not just personal information) and all forms of public sector information and information systems (digital, hardcopy and verbal).[5]

6. To OVIC's knowledge, the Victorian Standards are the first mandated general information security standards for government anywhere in the world. They establish 12 high level mandatory security measures across each of the protective security domains (governance, information, personnel, information communications technology and physical security), to protect the confidentiality, integrity and availability (**CIA**) of public sector information assets and systems. The Victorian Standards use a risk-based approach and reflect national and international best practice approaches towards security, tailored to the VPS.

7. Sections 88 and 89 of the PDP Act outline the compliance obligations of VPS organisations with respect to the Victorian Standards. VPS organisations are required to:

---

[1] Sections 85(1), 85(1A) and 86(1) of the PDP Act.

[2] The Victorian Protective Data Security Standards 2.0, issued in October 2019, are available at https://ovic.vic.gov.au/information-security/standards/.

[3] The Victorian Protective Data Security Framework 2.0, issued in February 2020, is available at https://ovic.vic.gov.au/information-security/framework-vpdsf/.

[4] Section 84 of the PDP Act outlines the categories of organisations to which Part 4 applies.

[5] Section 3 of the PDP Act defines 'public sector data' 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'.

- undertake a Security Risk Profile Assessment, which enables VPS organisations to identify, analyse, evaluate and treat information security risks, including cyber risks; and
- develop a Protective Data Security Plan, which is a reporting tool used to advise OVIC of the organisation's maturity level, implementation status of the Victorian Standards and security profile, and to attest to the implementation activities required by the Victorian Standards.

8. The Victorian Framework and Standards underpin Victorian Government initiatives involving the security of information and information systems, including cyber security. The Victorian Cyber Strategy aligns with and refers to the Victorian Framework and Standards.[6] The Cyber Security Branch within Digital Victoria adopts the Victorian Standards issued by OVIC, and in turn assists agencies and bodies in their application of the Standards.

## Resourcing and planning will be crucial to the success of the 2023-2030 Australian Cyber Security Strategy

9. OVIC's experience in regulating and upskilling the Victorian public sector demonstrates that public servants and contracted service providers (**CSPs**) are motivated to protect the security of public sector information, but to do this well, they need capability, funding, resources, education and assistance.[7]

10. Providing appropriate resources to education and awareness, communications, monitoring, and assurance, to reach the wide array of stakeholders covered by the 2023-2030 Australian Cyber Security Strategy (**Strategy**), will be important if the goals of the Strategy are to be attained. Government incentives, such as free or low-cost education and training, will likely be required, to address the critical skills shortage and increase the numbers of data and information security professionals working in the public and private sectors.

11. Without these measures, there is unlikely to be sufficient capability and resources to successfully uplift cyber security practices across the nation.

[6] See Victorian Government, 'Victoria's Cyber Strategy 2021: Mission Delivery Plans 2021-2022', available at https://www.vic.gov.au/victorias-cyber-strategy-2021-introduction#download-the-pdfs.

[7] 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 2022 PDSP reporting period, 41% of responses 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 (48%) and resourcing (79%), while comparably lower rated challenges and barriers include third-party arrangements (30%), lack of understanding around the Victorian Standards (24%) and lack of clarity around roles and responsibilities within the agency (16%).

**Question 2 – What legislative or regulatory reforms should Government pursue to enhance cyber resilience across the digital economy? Should Australia consider a Cyber Security Act, and what should this include?**

12. OVIC agrees that legislative and regulatory reform is necessary to strengthen Australia's cyber resilience.

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

13. In OVIC's view, it would be preferable for legislative reform to encompass information security in the broader sense, capturing all forms of information – both digital and non-digital, and all types of information (not just personal information), utilising all protective security domains to maintain the CIA triad.

14. Legislating 'information security' rather than 'cyber security', recognises that cyber security is only one facet of good information security risk management, and broadens legislative protections to cover digital and non-digital information and systems.

15. Victoria's legislated information security Framework and Standards under Part 4 of the PDP Act lead the way in Australia and provide a positive precedent for what regulatory reform could look like at the national level.

16. The Victorian Standards 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 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.

17. OVIC recommends the federal government's cyber security policy initiatives sit underneath, not alongside, a broader information security strategy. That is, OVIC recommends a hierarchical approach is taken, rather than viewing cyber security as a separate requirement to information or data security.

18. By providing a legislative basis for information security, a common language and approach could be formally established, improving clarity and consistency for stakeholders, and reducing the number of overlapping, and potentially contradictory, requirements. This approach is taken in Victoria, placing Part 4 of the PDP Act at the top of the hierarchy with Victoria's cyber strategy sitting underneath it. This approach ensures stakeholders are presented with harmonised material and avoids duplication of effort across organisations and business units.

Legislate to protect all forms and types of information

19. The Strategy refers at various times to protecting "customer data" and "personal data".[8] In OVIC's view, the Strategy should protect all information (for example, financial and legal information), not just personal information.

20. OVIC recognises that information presents in many different formats, not just digital, and represents a safety and security risk when the CIA of verbal or hardcopy material, or non-personal information (such as financial and legal information), is not adequately protected.

21. A siloed focus on electronic information, or personal information, has the potential to expose Australia to harm or damage that could be avoided if a more holistic approach to information security is adopted. For example, a cyber-attack on a banking, water, communications, or electricity grid, caused by an employee leaving a hardcopy record of their username and password on a bus seat, that is used by a cybercriminal to access and bring down the network, is an information security issue that may not be addressed if the Strategy focusses exclusively on digital information and systems, and is a threat that causes harm to individuals, even though no personal information is misused or accessed.

Legislate all protective security domains and the full CIA triad

22. In OVIC's view, all protective security domains and the full CIA triad should be represented in any proposed legislative reform, to ensure a holistic approach to the protection of information and information systems.

23. With respect to protective security domains, 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.

24. With respect to the CIA triad, cyber security tends to emphasise the need to protect information from unauthorised access, which goes to the confidentiality arm of the CIA triad. Focussing too heavily on unauthorised access, may not adequately protect the integrity and availability of the same information and systems. In OVIC's view, all parts of the triad are important to implementing best practice information security.

Use a risk based regulatory approach

25. The discussion paper states:

> "The Strategy must … ensure that all organisations have the right cyber security settings in place to make Australia the most cyber secure nation in the world by 2030.
>
> …

[8] Discussion paper, pages 7, 10, 11 and 17.

> "…it is clear from stakeholder feedback and the increasing frequency and severity of major cyber incidents, that more explicit specification of obligations, including some form of best practice cyber security standards, is required across the economy to increase our national cyber resilience and keep Australians and their data safe".[9]

26. To ensure that organisations have the right security settings in place, the Victorian model deliberately uses a risk-based approach to implementing the principles in the Victorian Standards, not a compliance-based approach. OVIC has found this model works well, as security in practice is dynamic and therefore the response needs to be risk based.

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

- high level principles can be adapted to all types of government 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; and
- risk-based principles help to lift the oversight of cyber security to the executive level of an organisation.

28. The challenge of risk-based principles is that risk management is not universally understood and can be difficult to achieve in practice without the right skills, capability, support, and guidance. 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.

29. To support organisations to implement the Standards, OVIC developed security measures called 'elements'. The elements set the expectations of what is meant by each standard and guides the implementation of each standard. Unlike a compliance model, the elements still retain a level of flexibility, by allowing VPS organisations to choose the individual controls to implement under each element, that best respond to the organisation's particular circumstances. A similar approach could be taken to regulating federal government organisations and the private sector.

30. If a principles-based approach is taken, the government should commit to resourcing improved education around risk management and ensure that ongoing support is provided to government organisations and businesses to empower them to implement security controls based on their own security risks. Tangible and ongoing support to implement security controls will be necessary.

[9] Discussion paper, page 17.

31. For a detailed explanation of OVIC's views on risk-based vs compliance-based approaches read OVIC's submission responding to questions 5, 8 and 9 of the *Strengthening Australia's cyber security regulations and incentives – A call for views* discussion paper.

Harmonising regulatory frameworks

32. The discussion paper speaks to creating an "effective national response" to cyber security threats and states that "[i]f we are to lift and sustain cyber resilience and security, it must be an integrated whole-of-nation endeavour".[10] OVIC agrees with these statements.

33. In OVIC's view, to ensure a national response is effective, there needs to be an alignment in frameworks, response capability and interoperability across the state, territory, and federal jurisdictions. This includes adopting common terminology and definitions, and clearly identifying which jurisdiction is the lead responder.

34. At present, OVIC's information security unit spends considerable time discussing the applicability of various state and federal requirements with its stakeholders. If requirements were clear, OVIC would have more time available to it, to provide practical security advice to stakeholders, to help uplift information security practices across the Victorian public sector.

35. For a detailed explanation of the complexity of cyber and data security settings and requirements within Australia, and OVIC's views on how these requirements could be better harmonised across jurisdictions read pages 2-6 of OVIC's submission in response to the National Data Security Action Plan discussion paper.

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

36. In OVIC's view, there should only be one regulator at the federal level to administer, oversee and enforce legislated information security requirements for federal government organisations and the private sector.

37. Additional funding and strong oversight and assurance mechanisms will be necessary, to support the uplift of information and cyber security practices, and to properly monitor and manage how parties interact with and adopt the requirements of any regulated standards.

38. OVIC expends substantial effort to engage and provide VPS organisations with education and information. This includes engagement officers assigned to various sectors, to ensure continuing and effective communication. The success of any regulatory framework will depend upon sustained and capable personnel to assist organisations in meeting their commitments.

39. The regulator should be given powers to audit and monitor the maturity levels of an organisation's implementation of standards, including powers to enquire into the maturity

[10] Discussion paper, page 7.

of a government organisation's CSPs. That is, the regulator should have the power to conduct preventative assurance, to assess that maturity levels are, in fact, reasonable, in addition to powers to respond to breaches. This should include powers to find out whether a CSP to a government organisation is in fact deleting unnecessary data, rather than trusting that the CSP's contractual obligation to the outsourcing organisation is being implemented in practice.

**Question 5 – How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?**

40. Australia is already a large contributor to international standards and has well established Standards Australia (SA) mirror committees to support and contribute to both national and international standards. For example:

    - *IT-012 Information security, cybersecurity and privacy protection* is the Australian mirror committee to ISO/IEC JTC1/SC27, which leads the work on 27000 series documents; and
    - *MB-025 Security and Resilience* is the Australian mirror committee to ISO/TC 292, which includes protective security.

41. A good example of where Australia influences international standards is the current project *ISO 22340: Protective security – Guidelines for an enterprise protective security architecture and framework*. Australia is leading the development of this standard based off the Commonwealth Protective Security Policy Framework, to elevate it to the international stage.

42. As international standards are published, the SA mirror committees review them to determine whether they are fit to adopt as Australian Standards, rather than developing separate standards. For example, soon after publishing *ISO 27002:2022 Information security controls*, Australia was quick to directly adopt these international standards as *AS/NZS 27002:2022* to ensure alignment and consistency with international work.

43. In OVIC's view, Australia could better contribute to international standards-setting by including more federal government representatives in the SA committees. This work would build capability within the public service and in turn, minimise the need for the federal government to develop its own, separate security standards.

**Question 6 – How can Commonwealth government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?**

44. OVIC supports the aspirations of the discussion paper for government to stand as an exemplar of cyber security and agrees with the points made under 'securing government systems' at page 19 of the discussion paper.

45. In OVIC's view, to deliver cyber security best practice, the responsibility for cyber security needs to sit with the executive, not the IT team of an organisation.

46. Information security should be understood as a category of risk that requires managing, similar to occupational health and safety and financial risks. This approach moves information security out of compliance and into organisations' existing risk management frameworks. In OVIC's view embedding information security into business-as-usual risk activities gets more traction within an organisation and produces long term cultural change and uplift of information security practices, than an approach motivated only by compliance.

47. Since the introduction of the Victorian Framework and 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 that is submitted to OVIC, and annually attest to OVIC that the agency's security program meets the requirements of the Victorian Standards.

**Question 13a – Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?**

48. Yes. This will help to relieve some of the multiple reporting burden on organisations.

**Question 15(a) How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime? What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?**

49. Cyber security is a niche field, requiring specialised knowledge, skill and capability that small businesses are unlikely to possess. Investing in skills building is critical to assisting small business to manage their cyber security risks. This may involve funding skills-based positions and providing resources, education and assistance to improve the adoption of best practice cyber security measures.

50. For detailed recommendations on how to address this issue, see OVIC's submission in response to the discussion paper - Strengthening Australia's cyber security regulations and incentives – A call for views.

Thank you once again for the opportunity to contribute to the development of the 2023-2030 Australian Cyber Security Strategy.

I will be publishing a copy of this submission to the OVIC website and have no objection to the Expert Advisory Board publishing this submission.

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

Yours sincerely

[redacted]

**Sven Bluemmel**
Information Commissioner