

11 February 2021

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security

By email only: pjcis@aph.gov.au

Dear Committee Secretary

Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

Thank you for the opportunity to provide comment on the review into the *Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill)*. The Office of the Victorian Information Commissioner (OVIC) is pleased to provide this submission, which outlines OVIC's role and concerns regarding the Bill.

About OVIC

1. OVIC is the primary regulator for information security, freedom of information, and information privacy in Victoria, administering the *Privacy and Data Protection Act 2014 (PDP Act)* and the *Freedom of Information Act 1982 (Vic)*. This combined oversight provides OVIC with a unique perspective in promoting fair access to information held by the Victorian public sector (VPS), while ensuring it is properly used in a way that upholds the privacy rights of Victorians, and appropriately protected to ensure its confidentiality, integrity and availability.
2. Part 4 of the PDP Act sets out the protective data security requirements that apply to VPS entities,¹ with these requirements covering public sector data and data systems.² 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, and establishes the Information Commissioner's jurisdiction over Victoria Police and the Crime Statistics Agency with respect to their data, data systems and protective data security practices.

The Victorian Protective Data Security Framework

3. As Information Commissioner, one of my obligations under Part 4 of the PDP Act is to develop a protective data security framework for monitoring and assuring the security of public sector data, and to review or amend that framework from time to time.³ The Victorian Protective Data Security Framework (VPDSF) was first published in 2016 and most recently updated in 2020.⁴

¹ Section 84 of the PDP Act outlines the categories of entities to which Part 4 applies.

² 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'.

³ Sections 85(1) and 85(1A) of the PDP Act.

⁴ The VPDSF is available at <https://ovic.vic.gov.au/data-protection/framework-vpdsf/>.

The VPDSF provides a model to monitor and measure the extent to which VPS entities implement the associated Victorian Protective Data Security Standards (**VPDSS**) and comply with the requirements of the PDP Act. The VPDSF and accompanying guidance materials are designed to assist entities to mitigate information security risks and build the VPS' information security capability and maturity. It also provides OVIC with insight into information security practices across the VPS.

The Victorian Protective Data Security Standards⁵

4. Part 4 of the PDP Act also provides that the Information Commissioner may issue protective data security standards.⁶ The VPDSS were originally issued in 2016, representing the first mandated information security standards for government anywhere in the world, and later reissued as the VPDSS 2.0 in October 2019 following a review of the VPDSS. The VPDSS establish 12 high level mandatory requirements to protect public sector data across each of the security domains: governance, information, personnel, physical and information communications technology (cyber) security. The VPDSS employs a risk-based approach and reflects national and international best practice approaches towards security, tailored to the VPS.
5. Sections 88 and 89 of the PDP Act outline the compliance obligations of VPS entities with respect to the VPDSS. For example, VPS entities are required to undertake a Security Risk Profile Assessment (**SRPA**), which is a process that enables VPS entities to identify, analyse, evaluate and treat information security risks, including cyber risks. VPS entities must also develop a Protective Data Security Plan (**PDSP**), a reporting tool used by those entities to advise OVIC of their maturity level, implementation status of the VPDSS (referencing information security risks identified as part of the SRPA process), articulate the entity's security profile, and attest to the implementation activities required by the VPDSS.

The proposed regulatory regime

6. Given OVIC's role outlined above and existing information security requirements for VPS entities under the PDP Act, OVIC has concerns regarding the proposed amendments in the Bill, insofar as they would affect the information and information systems of VPS entities regulated under Parts 4 and 5 of the PDP Act that own or operate critical infrastructure.
7. OVIC's primary reason for this concern is the potential for confusion and duplication among entities covered by both regulatory regimes under the PDP Act and the *Security of Critical Infrastructure Act 2018 (SCI Act)* (as amended by the Bill), given the likely probability of overlap between the two regimes. Should the proposed regulatory regime overlap with OVIC's jurisdiction, OVIC considers this would cause uncertainty for these entities as to which law or regulator is appropriate in certain circumstances, as well as result in duplicative efforts on the part of regulated entities. Agencies may find it challenging to manage compliance with two different regulatory frameworks in respect of their information and information systems, even if the requirements across both frameworks are similar.
8. For example, the Bill introduces a requirement for responsible entities of critical infrastructure assets to have, maintain, and regularly review a critical infrastructure risk management program, the purpose of which is to identify potential hazards that could have a 'relevant impact' on an asset, minimise or eliminate the risk of that hazard occurring, and mitigate the impact of the hazard on an asset (clause 39 of the Bill). This is akin to the requirement in the VPDSS for VPS entities to undertake the SRPA process⁷.

⁵ From this point on, this submission will refer to 'data' and 'protective data security' as information and information security.

⁶ Section 86(1) of the PDP Act.

⁷ Standard 3 of the VPDSS 2.0. The VPDSS 2.0 is available at <https://ovic.vic.gov.au/data-protection/standards/>.

Similarly, the proposed cyber security incident notification scheme (clause 39 of the Bill) has elements comparable to OVIC's Information Security Incident Notification Scheme,⁸ which requires VPS entities to notify OVIC of incidents that compromise the confidentiality, integrity or availability of public sector information with a 'limited' business impact or higher on government operations, entities or individuals.

9. On a national level, other existing security frameworks such as the Protective Security Policy Framework (**PSPF**) and the Information Security Manual (**ISM**) – schemes in which the Australian Government has already heavily invested, and with which the Victorian model closely aligns – may also similarly overlap with the framework created by the Bill, resulting in potential duplication of security requirements. Instead, leveraging off and expanding these existing frameworks could be less resource intensive, and have the benefit of already being familiar to stakeholders.

Inclusion of a carve-out

10. In light of the above, OVIC supports the inclusion of a carve out in the Bill, to the extent that VPS entities are already regulated by OVIC under the VPDSF and VPDSS. This could be similar to the saving provision contained in section 3 of the *Privacy Act 1988 (Privacy Act)*, which has the effect of upholding State or Territory law (such as the PDP Act) with respect to the handling of personal information. A similar provision in the Bill could uphold the information security obligations and regulatory roles that already exist at State or Territory level over information and information systems, including functions that are constitutionally under State purview. OVIC is of the view that such a provision would minimise the risk of constitutional conflict and avoid the potential for confusion and duplication of information security obligations, allowing VPS entities to continue to enhance their information security risk management capability and maturity without the need for potentially duplicative efforts.
11. OVIC is well positioned to support VPS entities and perform this regulatory function, having developed constructive and effective relationships with its regulated entities since the PDP Act came into effect in 2014. My office has invested considerable resources into developing, administering, and refining the Victorian model, to produce a framework and standards that understand and reflect the needs of our stakeholders, and which have their support and buy-in. The second iteration of the VPDSS, for example – VPDSS 2.0 – was based on lessons from several attestation periods and extensive consultation with government agencies, their contractors, and consultants. VPDSS 2.0 represents a substantial investment in information security not only by my office, but also by the Victorian government and these stakeholders.
12. Moreover, the Information Commissioner has powers under Parts 4 and 5 of the PDP Act to issue, respectively, protective data security standards in relation to information and information systems, including, law enforcement data and crime statistics data.⁹ In particular, section 86(2)(b) of the PDP Act provides for the issuance of customised protective data security standards, that can apply to specified agencies or bodies, and any specified information or activity (or class of information or activity) of those entities. The Victorian regulatory model may therefore still be able to meet any specific needs required by the Commonwealth within the bounds of the PDP Act, were my office to develop and issue customised protective data security standards specific to critical infrastructure owners and operators, where those entities are covered by Part 4 of the PDP Act.

⁸ More information about OVIC's Information Security Incident Notification Scheme is available at <https://ovic.vic.gov.au/resource/ovic-information-security-incident-notification-scheme-v1-0/>.

⁹ Sections 86 and 92 of the PDP Act.

This would be similar to the development of sector-specific standards, as proposed by the Department of Home Affairs in its Consultation Paper *Protecting Critical Infrastructure and Systems of National Significance*.¹⁰

Proposed compulsive powers

13. Clause 45 of the Bill also proposes compulsive powers for the Commonwealth Government to enable it to respond to serious cyber security incidents, through Ministerial authorisation for the Secretary to give information-gathering directions, action directions, or intervention requests. Importantly, the Bill appropriately limits the circumstances in which these powers can be exercised.

14. The Explanatory Memorandum to the Bill notes at paragraph 866 that:

*Consultations have revealed strong community expectation that, in emergency circumstances and as a matter of last resort, the Government will use its significant technical expertise in cyber-defence to protect Australia's national interests and restore the functioning of essential services. However, consultations also highlighted that these powers must be used only in the most exceptional circumstances.*¹¹

15. OVIC recognises that community expectations and the evolving cyber threat environment provide some reasoning behind the need for these compulsive powers. However, OVIC considers that given their substantial nature (notwithstanding the limitations imposed on these powers), there should be further justification to support the need for such compulsive powers – for example, is there evidence to demonstrate that critical infrastructure entities will not collaborate or cooperate with Government in responding to incidents, including in emergency circumstances, unless compelled?

Definition of 'cyber security incident'

16. OVIC considers the proposed definition of 'cyber security incident' in the Bill (proposed section 12M of clause 32) could be enhanced to ensure consistency with national and international standards such as the PSPF and the ISM. For example, the definition could perhaps include some reference to the impact caused by the incident (such as 'relevant impact, within the meaning given by proposed section 8G in clause 21). Aligning the proposed definition of 'cyber security incident' closer to definitions in existing regulatory models such as the PSPF and the ISM may help to ensure some consistency across various protective security policies, frameworks and mechanisms that could potentially apply to responsible entities of critical infrastructure assets.

17. Further, the proposed definition in the Bill focuses solely on unauthorised access, modification and impairment. However, security incidents may also arise in circumstances where access *is* authorised, whether that incident is accidental or deliberate. It may therefore also be worth exploring the inclusion of authorised access that may lead to deliberate or accidental compromise of the confidentiality, integrity, and availability of the critical infrastructure asset, information systems, or business operations. This is particularly pertinent given human error continues to be a leading cause of data breaches.¹²

¹⁰ August 2020, available at <https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf>.

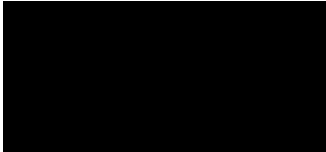
¹¹ Explanatory Memorandum, Security Legislation Amendment (Critical Infrastructure) Bill 2020, 866.

¹² In its [Notifiable Data Breaches Report: July – December 2020](#), the Office of the Australian Information Commissioner (OAIC) noted that 38% of data breaches notified during July to December 2020 were attributed to human error. This represented an increase in both the total number and proportion of human error breaches received by the OAIC.

Thank you once again for the opportunity to provide this submission into the Committee's review of the Bill. OVIC will follow the progress of the Bill with interest. I have no objection to this submission being published by the Committee without further reference to me. I also propose to publish a copy of this letter on the OVIC website, but would be happy to adjust the timing of this if necessary.

If you have any questions regarding this submission, please contact me or my colleague Anthony Corso, Assistant Commissioner – Information Security, at [REDACTED]

Yours sincerely

A large black rectangular redaction box covering the signature area.

Sven Bluemmel
Information Commissioner