Office of the Victorian Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D20/15682

16 September 2020

Critical Infrastructure Centre
Department of Home Affairs

Dear Sir/Madam

Submission to Department of Home Affairs: *Protecting Critical Infrastructure and Systems of National Significance* Consultation Paper

Thank you for the opportunity to provide comment on the Department of Home Affairs' (**Department**) proposal for an enhanced framework to protect Australia's critical infrastructure (**proposed framework**), as outlined in the *Protecting Critical Infrastructure and Systems of National Significance* Consultation Paper (**the paper**). The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide this submission regarding the proposed framework.

This submission briefly outlines OVIC's role, and its views on the proposed framework. To give effect to sections 16 and 17 of the *Security of Critical Infrastructure Act 2018*, particularly exercising relevant constitutional powers relating to State critical infrastructure, this submission suggests a carve out in the proposed framework, to the extent that Victorian public sector (**VPS**) entities' information and their information systems are already regulated by OVIC under Parts 4 and 5 of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) (and would otherwise be captured in the proposed framework). OVIC's reasons for this request are outlined below.

About OVIC

1. OVIC is the primary regulator for information security, freedom of information and information privacy in Victoria, administering both the PDP Act and the *Freedom of Information Act 1982* (Vic). This provides my office with a unique perspective in promoting fair access to information held by Victorian Government, while ensuring it is properly used in a way that protects the privacy rights of Victorians, and highlighting the information security obligations of regulated entities.

2. 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.[1] The security provisions under Part 4 apply to the categories of entities listed in section 84 of the PDP Act, and to

[1] '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'.

all types of information (including personal, financial and health information) regardless of its form or format (e.g. soft or hard copy, video, audio).[2]

3. 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 system and security practices.

The Victorian Protective Data Security Framework

4. Under Part 4 of the PDP Act, the Information Commissioner is required 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] First published in 2016 and recently updated in 2020, the Victorian Protective Data Security Framework (**VPDSF**) has been developed to monitor and assure the security of public sector information and information systems across the VPS. It provides a model for monitoring and measuring the extent to which VPS regulated entities implement the Victorian Protective Data Security Standards, and comply with the PDP Act.[4]

5. The VPDSF and accompanying guidance material adopt a risk-based approach and are designed to assist VPS entities to mitigate information security risks and build VPS information security capability and maturity, as well as provide OVIC with insight into information security practices across the VPS. This risk-based approach empowers organisations to identify and manage their unique information security risks, and to apply security controls that reflect their unique operating environment. This approach recognises that information security risks vary from organisation to organisation, informed by factors such as the type and nature of their information assets, their resource base, threat environment, and their risk appetite and tolerance.

The Victorian Protected Data Security Standards

6. Similarly, under Part 4 of the PDP Act, the Information Commissioner may also issue protective data security standards.[5] The Victorian Protective Data Security Standards (**VPDSS**) were first issued in 2016, and later reissued as the VPDSS V2.0 in October 2019. Employing a risk-based approach, the VPDSS focuses on the outcomes required to enable efficient, effective and economic investment in security measures.[6]

7. The VPDSS establishes 12 high level mandatory requirements to protect public sector information across each of the security domains (i.e. governance, information, personnel, information communications technology (cyber) and physical security). The VPDSS reflects national and international best practice approaches towards security, tailored to the Victorian Government environment.

8. Part 4 of the PDP Act also compels the heads of public sector bodies to ensure that any contracted service providers that have direct or indirect access to public sector information adhere to the VPDSS.

[2] In contrast, the information privacy provisions under Part 3 of the PDP Act only apply to 'personal information'.
[3] Sections 85(1) and 85(1A) of the PDP Act.
[4] The VPDSF is available to access and download at www.ovic.vic.gov.au/data-protection/framework-vpdsf.
[5] Section 86(1) of the PDP Act.
[6] The VPDSS is available to access and download at https://ovic.vic.gov.au/data-protection/standards/.

The proposed framework

9. OVIC recognises the need to ensure the resilience and security of Australia's critical infrastructure sectors (whether industry or government owned and operated), in the face of an evolving threat environment as noted in the paper. However, OVIC considers that the proposed framework is problematic in respect of VPS entities that own or operate critical infrastructure and are regulated under Parts 4 and 5 of the PDP Act. These entities already have existing information security obligations under legislation. OVIC's reasons for this view are outlined below.

Inconsistency and confusion

10. Per the paper, one element of the proposed framework is the introduction of a Positive Security Obligation, to be implemented through high-level security obligations, as well as 'sector-specific standards' developed by individual regulators in collaboration with critical infrastructure entities across different sectors. Notwithstanding that any requirements established as part of the proposed framework are intended to build on, rather than duplicate, existing regulatory frameworks,[7] the proposed framework's focus on security and aim to enhance entities' security capability aligns closely with OVIC's own information security remit and regulatory functions.

11. As such, there is a high probability that security obligations or standards that may be implemented as part of the proposed framework will overlap with or override those which regulated VPS entities are already required to comply with under the VPDSS. Should the proposed framework overlap with OVIC's jurisdiction, OVIC considers this would cause widespread confusion amongst those Victorian entities. Having multiple regulators and potentially overlapping frameworks to comply with is unlikely to be helpful for those entities, causing uncertainty as to which law or regulator is relevant in certain circumstances.

12. Additionally, the existence of two sets of frameworks at a State and Commonwealth level, based on what appear to be different approaches, would only serve to create more uncertainty and confusion for regulated entities. The VPDSF and VPDSS promote a risk-based approach towards protecting and ensuring the security of information, whereas the proposed framework appears to place a greater focus on a traditional compliance model, emphasising the need for – and offering solutions that are based on – compliance. OVIC has invested considerable resources to educate regulated entities on how to work with risk-based standards and has concerns that working with a compliance-focused model as well would only serve to confuse regulated entities.

13. OVIC also queries whether the intent of the proposed framework – to develop a more consistent approach towards managing risk across critical infrastructure sectors – can be fully realised where multiple sector regulators are involved and, moreover, where those regulators are proposed to co-design sector-specific standards across each sector. Achieving consistency within this context seems likely to be challenging, where different sets of standards apply to entities in different sectors.

Compulsive powers

14. The proposed framework includes compulsive powers to enable the Commonwealth Government, in certain circumstances, to provide protective or mitigative directions to critical infrastructure entities, or take direct action, in order to protect critical infrastructure or systems. Notwithstanding that this capability is intended to be primarily discharged on a voluntary basis as noted in the paper, given the significance of these powers, OVIC believes a greater evidence-base is required to support the need for such powers. For example, OVIC queries whether any relevant entity (either public or private) has ever refused the assistance of cybersecurity expertise, to drive or warrant the

[7] As noted on page 12 of the paper.

need for such powers. Currently, the paper does not provide sufficient explanation or evidence behind the driver for such a significant and powerful instrument.

Existing Commonwealth frameworks

15. OVIC also queries the need for an enhanced regulatory framework in light of existing national mechanisms such as the Protective Security Policy Framework (**PSPF**) and Information Security Manual (**ISM**)[8], schemes in which the Commonwealth Government has already heavily invested. The Victorian model was developed to closely align with international and national security frameworks and standards, complementing the requirements and controls set out at the Commonwealth level under the PSPF and ISM.

16. OVIC suggests these mechanisms could be given legislative backing and expanded in scope to include private entities that own or operate critical infrastructure and systems of national significance. The PSPF and ISM already scale in operation, promote a risk-based approach, and are already familiar to stakeholders. In particular, the ISM is regularly updated to reflect current threats to Australian organisations, based on threat intelligence from the Australian Cyber Security Centre. Leveraging from, and investing in, these existing models may be less resource-intensive and would avoid the potential for duplication of security requirements.

<u>Suggested carve-out</u>

17. In light of the above, OVIC strongly advocates for the inclusion of a carve-out in the proposed framework, to the extent that VPS entities are already regulated by OVIC under the VPDSF and VPDSS. For example, such a carve-out 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. In similar fashion, a carve-out inserted into section 16 of the *Security of Critical Infrastructure Act 2018* could uphold the information security obligations and regulatory roles that already exist at State or Territory level over public sector data and information technology systems, including over functions that are constitutionally under State purview.

18. In OVIC's view, such a provision would minimise the risk of constitutional conflict and avoid duplication and potential for confusion, placing VPS regulated entities in the best position to continue to build and enhance their information security risk management capability and maturity. OVIC is well placed to support this endeavour, having developed effective relationships with its regulated entities since the PDP Act came into effect in 2014, and investing considerable resources into the Victorian model to produce, administer, and refine a framework and standards that understand and reflect the needs of those stakeholders, and which has their support and buy-in.

19. In particular, the VPDSS has an established risk-based model for the development and implementation of controls proportionate to the information security risks and environment of different organisations and sectors: these standards articulate high level requirements which can then be applied with sector-specific controls that map back to the VPDSS. This approach ensures consistency while also allowing for local customisation tailored to the unique operating environments of different entities.

20. Further, Parts 4 and 5 of the PDP Act provide the Information Commissioner with the power to issue, respectively, protective data security standards in relation to public sector data (section 86), and law enforcement data security standards in relation to law enforcement and crime statistics data (section 92).[9] In particular, section 86(2)(b) provides for the issuance of *customised* protective

[8] https://www.cyber.gov.au/acsc/view-all-content/guidance/executive-summary
[9] 'Law enforcement data' (including 'crime statistics data') are defined in section 3 of the PDP Act.

data security standards that can apply to specified agencies or bodies,[10] and any specified information or activity, or class of information or activity, of those entities. OVIC may therefore still be able to meet the needs of the Commonwealth, within the bounds of the PDP Act, by establishing, if necessary, customised requirements specific to critical infrastructure owners or operators (where they are covered by the VPDSF). This would be akin to the development of sector-specific standards (as it relates to information security), as outlined in the proposed framework.

21. The second element of the proposed framework – enhanced cyber security obligations – proposes providing the Australian Government with the ability to request information to contribute to a near real-time threat picture. Under the Victorian model, specifically OVIC's Information Security Incident Notification Scheme, OVIC already receives notification of incidents that have an adverse impact on the confidentiality, integrity or availability of public sector information with at least a 'limited' business impact on government operations, organisations or individuals. This scheme is an element of Standard 9 of the VPDSS (Information security reporting to OVIC). It assists OVIC with developing a comprehensive security risk profile of the Victorian Government, which can be used for trend analysis and understanding of the threat environment. This scheme requires organisations to report an information security incident to OVIC as soon as practical, and no later than 30 days once an incident has been identified.[11]

22. VPS regulated entities are also required to develop a Protective Data Security Plan (**PDSP**) and submit a copy to OVIC. Reviewed every two years (or upon significant change),[12] a PDSP is a reporting tool used by entities to inform OVIC of their maturity level and implementation status of the VPDSS. As such, PDSPs are a primary source of information for OVIC, enabling us to assess the state of information security across the VPS. Additionally, OVIC's regulatory powers under the PDP Act allow for (but are not limited to) the conduct of audits (of potential breaches of the VPDSS), and the undertaking of preliminary inquiries where a theme or issue is identified (including an information security breach or inadequate information security practice).[13] These activities also assist to provide OVIC with visibility over implementation of the VPDSS, and the broader information security threat environment to Victorian Government.

Concluding remarks

23. We would welcome the opportunity to discuss our comments above in further detail and to hear the Department's views on our suggested approaches for the proposed framework.

24. OVIC understands that legislation for the proposed framework will be introduced to the Australian Parliament in the next month. Given our remit and the information security implications of the proposed framework, we would greatly appreciate receiving a copy of the draft Bill for review in advance of its introduction, as well as the opportunity to be involved in any consultations that may occur in the future.

My office will closely follow the progress of the Department's proposed framework with interest. I have no objection to this submission being published by the Department 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 to allow the Department to collate and publish submission proactively.

[10] That is, an agency or body referred to in section 84(1) of the PDP Act.
[11] For more information about OVIC's Information Security Incident Notification Scheme, see https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/.
[12] Or alternatively, where there is a significant change in the regulated entity's operating environment or security risks – section 89 of the PDP Act.
[13] OVIC's Regulatory Action Policy outlines how OVIC uses its regulatory powers, available at https://ovic.vic.gov.au/regulatory-action-policy/.

If you have any questions regarding any of the above, please contact me directly or alternatively, my colleague Anthony Corso, Assistant Commissioner – Information Security, at [redacted].

Yours sincerely

Sven Bluemmel
Information Commissioner