Submission No 20

INQUIRY INTO THE ADEQUACY OF THE LEGISLATIVE FRAMEWORK FOR THE INDEPENDENT BROAD-BASED ANTI-CORRUPTION COMMISSION

Organisation: Office of the Victorian Information Commissioner

Date Received: 14 July 2025

Office of the Victorian Information Commissioner

Phone: 1300 00 6842
Email: enquiries@ovic.vic.gov.au
PO Box 24274
Melbourne Victoria 3001

14 July 2025

Tim Read MP
Chair, Integrity and Oversight Committee
Parliament of Victoria

By email only: inquiryibac@parliament.vic.gov.au

Dear Chair,

Inquiry into the adequacy of the legislative framework for the Independent Broad-based Anti-Corruption Commission

Thank you for the opportunity to make a submission to the Integrity and Oversight Committee's (**Committee**) inquiry into the adequacy of the Independent Broad-based Anti-Corruption Commission (**IBAC**) legislative framework.

The Office of the Victorian Information Commissioner has combined oversight of information privacy, information security and information access, administering both the *Freedom of Information Act 1982* (Vic) and the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**).

Given OVIC's remit, this submission will address term of reference 4 by discussing the information security framework in the PDP Act and obligations for Victorian public sector (**VPS**) organisations. This submission will not specifically comment on IBAC's legislative framework or on IBAC's systems and practices as OVIC has not had reason to audit IBAC to gain insight into its information security environment.

Overview of the information security legislative framework

Part 4 of the PDP Act establishes the authority for OVIC to develop the Victorian Protective Data Security Framework (**the Framework**).[1] The Framework provides a model to monitor and assure the security of public sector information[2] and information systems across the VPS.

[1] *Privacy and Data Protection Act 2014* (Vic), section 85. The Victorian Protective Data Security Framework is available at: https://ovic.vic.gov.au/wp-content/uploads/2023/10/Victorian-Protective-Data-Security-Framework-V2.1.pdf.
[2] Public sector information is defined in section 3 of the PDP Act.

The Framework is supported by the Victorian Protective Data Security Standards (**the Standards**).[3] The Standards are 12 high-level mandatory requirements to protect the confidentiality, integrity and availability of public sector information and systems across all security areas: governance, information, personnel, ICT and physical security.

The Standards take a risk-based approach to information security and reflect national and international best practice, tailored to the VPS environment. Each Standard is underpinned by a suite of elements (or controls) that describe the security measures an organisation can take to modify risk. It is open to an organisation to determine which elements are applicable, informed by the organisation's particular circumstances, risk acceptance criteria and risk treatment options. Organisations can design their own controls as required or identify them from any source that has at least functional equiveillance to, or is better than, the element identified by OVIC.

The monitoring and assurance activities in the Framework are designed to help organisations mitigate information security risks, and to provide OVIC with insight into information security practices across the VPS. The activities are based on:

- the legislative obligations[4] of VPS organisations subject to Part 4 of the PDP Act[5]
- OVIC's responsibilities, powers,[6] and functions.[7]

Organisational monitoring and assurance activities

To demonstrate compliance with the PDP Act, the public sector body heads of regulated organisations are required to undertake specific monitoring and assurance activities. This includes ensuring a security risk profile assessment (**SRPA**) is undertaken for the organisation and a protective data security plan (**PDSP**) is developed.

A SRPA is designed to effectively identify, analyse, evaluate and treat an organisation's information security risks, including cyber security risks. A PDSP is a reporting tool that supports an organisation's assessment of its information security program, provides a template to summarise its progress towards implementing the Standards, and offers a means by which the organisation can provide a form of assurance to OVIC that they are making progress towards improving information security. In accordance with the PDP Act, a PDSP should be reviewed and submitted to OVIC every two years, or sooner in the event of a significant change in the organisation's operating environment or security risks.[8]

[3] *Privacy and Data Protection Act 2014* (Vic), section 86. The Victorian Protective Data Security Standards are available at: https://ovic.vic.gov.au/information-security/standards/.
[4] *Privacy and Data Protection Act 2014* (Vic), section 88 and 89.
[5] Organisations subject to Part 4 are listed in section 84 of the Act.
[6] *Privacy and Data Protection Act 2014* (Vic), Part 6.
[7] *Privacy and Data Protection Act 2014* (Vic), section 8D.
[8] *Privacy and Data Protection Act 2014* (Vic), section 89.

PDSPs submitted to OVIC enable OVIC to analyse the state of information security across the VPS. OVIC publishes reports with statistics and general insights drawn from PDSPs.[9] The insights include general trends and themes and a comparative analysis of whole of Victorian Government versus portfolio reporting.

OVIC also conducts targeted one-on-one sessions with some organisations to discuss their PDSPs and enhance their understanding of the requirements of the Standards.

Organisations are also expected to monitor for information security incidents and report eligible incidents to OVIC under the Information Security Incident Notification Scheme (**ISINS**).[10]

Risk-based approach to information security

The Victorian information security framework uses a risk-based approach to implementing the elements in the Standards. Organisations can adapt the elements to suit their contexts, and to implement controls most relevant to their circumstances. This enables organisations to build information security programs tailored to their specific operating environments.

Further, the PDP Act provides for the issuance of customised Standards that can apply to specified agencies or bodies, and any specified information or activity (or class of information or activity) of those agencies or bodies.[11]

Thus, OVIC would caution against amendments being made to an organisation's enabling legislation to build in specific information security provisions. This may add an unnecessary level of complexity to an organisation's capacity to understand and comply with its information security obligations.

Further, the PDP Act specifically regulates information security across the VPS and should remain the primary avenue through which public sector information and information systems are protected. Among other outcomes, OVIC's monitoring and assurance activities are designed to:

- support organisations' compliance with information security obligations
- uplift organisations' information security capability and maturity
- promote accountability and continuous improvement with the VPS in relation to information security
- build confidence in the information security practices of the Victorian Government.

[9] See OVIC website: https://ovic.vic.gov.au/information-security/information-security-resources/protective-data-security-plan-insights/.
[10] Detailed guidance on the ISINS is available on the OVIC website here: https://ovic.vic.gov.au/information-security/ovic-information-security-incident-notification-scheme/.
[11] *Privacy and Data Protection Act 2014* (Vic), section 86(2)(b).

Should there be any gaps identified in an organisation's information security practices, these can be addressed by existing mechanisms in the PDP Act.

Mandatory information security incident notification scheme

While OVIC expects organisations to report eligible information security incidents under the ISINS, incident notification is not mandatory under the PDP Act. In addition, organisations are not required to notify individuals whose information has been compromised following an incident. This places Victoria far behind other Australian jurisdictions including New South Wales, Queensland, Western Australia and the Commonwealth.

In OVIC's view, it would be prudent for Victoria to have a mandatory ISINS under which organisations would be obligated to report incidents of a certain threshold to OVIC. OVIC should also have powers to require an organisation to notify individuals affected by an incident. A mandatory scheme would enable OVIC to gain a more comprehensive security risk profile of the Victorian Government, identify security and privacy trends and themes, and have a fulsome understanding of the threat environment as it relates to the protection of public sector information and systems.

OVIC has previously raised this view in submissions to other Parliamentary inquiries, and would be happy to provide the Committee with further information on how a mandatory ISINS could work, if required.[12]

If the Committee has any questions about this submission, please contact OVIC through [redacted]

Yours Sincerely

[redacted]

Sean Morrison
Victorian Information Commissioner

[12] For example, see OVIC's submission to the Public Accounts and Estimates Committee's inquiry into fraud and corruption control in local government: https://ovic.vic.gov.au/wp-content/uploads/2025/05/Submission-to-the-Inquiry-into-fraud-and-corruption-control-in-local-government.pdf.