1. **OVIC updated its Regulatory Action Policy in October 2022. What impact has this updated policy had so far, and how will the new regulatory approaches (noted at the public hearing on 25 November 2024) build on the current policy?**

The objective of OVIC's Regulatory Action Policy is to express OVIC's regulatory strategy and how it reflects existing and emerging issues affecting the information rights of Victorians. The primary changes to OVIC's Regulatory Action Policy made in 2022 were designed to:

- enable OVIC to communicate its regulatory actions more clearly, particularly in specifying that OVIC will publish reports of its regulatory action except where there are compelling reasons not to
- reflect that OVIC's approach to regulatory action takes account of the published regulatory priorities
- consolidate privacy, freedom of information and information security into a single set of factors OVIC considers when deciding whether to undertake regulatory action
- amend the guiding principles to include a principle that ensures all regulatory action is effective and targeted, and make the principle of proportionality more prominent
- clarify the actions OVIC takes when following up recommendations made during regulatory action.

As a result of the 2022 Regulatory Action Policy, OVIC's Investigations team has implemented changes to its practices and approaches to regulatory action. The following excerpt from OVIC's 2023-24 annual report outlines the impact of the Policy:

> *On this year's theme of Changes, the Investigations team has made greater use of preliminary inquiries as a regulatory tool. One function of preliminary inquiries is to gain further information to assess the need for more formal action, however the Investigations team also uses these to identify cases where it can work with an agency to bring about improvements to ensure compliance without resorting to more formal action.*
>
> *A greater reliance on preliminary inquiries has allowed the Investigations team to have increased contact with more organisations. In appropriate cases, it has also allowed for the achievement of regulatory outcomes in a more flexible and efficient way.*
>
> *A further change this year has been the reporting of compliance monitoring activities in the annual report… Updates have been provided on whether or not organisations have implemented recommendations that OVIC has issued through previous regulatory action, and how these recommendations were implemented.*

OVIC plans to make further amendments to the Regulatory Action Policy in 2025. These amendments will build on regulatory actions implemented throughout 2022-2024 and reflect necessary adaptations in OVIC's regulatory strategy as it responds to developments in technology, resourcing, and societal and cultural attitudes.

2. As stated in the Information Commissioner's opening remarks at the public hearing, please provide details and possible timelines on OVIC's current review of internal processes if available.

The Information Commissioner's opening remarks at the public hearing noted that OVIC is undertaking a review of its processes and has recently updated its Strategic Plan. Enclosed is OVIC's new strategic plan represented on a page format.

OVIC's 2024-2027 vision is:

a public sector culture that supports access to information and ensures its proper use and security.

This vision speaks to the co-regulatory model noted in question 3 and expresses the purpose of OVIC's current review of internal processes: to make the regulatory mechanism more accessible and navigable.

There are a range of internal process reviews happening across OVIC currently, which includes reviews to OVIC's guidance material and OVIC-issued standards. Details of these reviews are included in OVIC's response to this question, as they speak to the way OVIC interprets the legislation it administers and the processes within that OVIC itself must follow.

Public Access processes

OVIC's Public Access process and guidance documents include information on its approach to reviews and complaints under the *Freedom of Information Act 1982* (FOI Act), promotion of proactive and informal release of information, informal resolution, and other supporting documentation for the completion of work.

As part of ongoing improvement efforts, a thorough review of the freedom of information (FOI) reviews procedure will be completed by the end of the 2025 calendar year. This review will align with recent changes to the FOI Act and OVIC's FOI Guidelines, and will refine OVIC's internal processes to enhance efficiency and accessibility. One significant recent change is increased power for the Information Commissioner to resolve an FOI review informally. This change was introduced by the *Justice Legislation Amendment (Integrity, Defamation and Other Matters) Act 2024*. OVIC is reviewing, updating and implementing processes that align with these changes, including procedures for preliminary inquiries and a process for determining whether a matter can be resolved informally.

OVIC has also been refining its approach to providing access to the information it holds, with a formal policy to be published in early 2025.

Process improvements implemented since 2022-23 with respect to OVIC's FOI operations, include:

- enhancing the usability of correspondence templates by adopting a plain language approach
- reviewing and updating OVIC's Notice of Decision template
- shortening timeframes for agencies to respond to review matters

- reviewing how agencies provide information to applicants to encourage agencies to provide all information upfront rather than incrementally
- making 'short form' decisions on FOI reviews, where appropriate
- increasing functionality in OVIC's case management system.

FOI Professional Standards

As required under section 6X(1) of the FOI Act, a review of the FOI Professional Standards (**Standards**) was recently completed. The review was conducted by KPMG, whose report is available on OVIC's website. OVIC supports the majority of the 27 recommendations made in the report. OVIC's response to the recommendations is also available on OVIC's website. OVIC will be updating the Standards based on the recommendations. As required by section 6U(4) of the FOI Act, OVIC will consult on the updated draft Standards and agencies and interested parties will have the opportunity to provide feedback and comments. This consultation will occur in early 2025, with an aim to have updated Standards in place for 2025-26.

Victorian Protective Data Security Framework and Standards

OVIC is also reviewing and updating the Victorian Protective Data Security Framework (**VPDSF**) and Victorian Protective Data Security Standards (**VPDSS**). The VPDSF provides direction to the Victorian Public Sector (VPS) on its information security obligations. The VPDSS establish 12 high-level mandatory requirements to protect public sector information across all security domains, including governance, information, personnel, Information Communications Technology and physical security.

The last update to the VPDSS occurred in 2019. The purpose of OVIC's current review is to identify opportunities to simplify the VPDSS, make them less technical where possible, and account for any changes in best practice since the last update. The review will involve extensive consultation with stakeholders. Updating the VPDSS will entail a broader review of internal processes such as evaluation and analytics of agencies that report to OVIC under the VPDSS. OVIC intends for the updated VPDSF, VPDSS and implementation guidance material to be published by the end of 2025.

Guidelines to the Information Privacy Principles

OVIC continues to update the Guidelines to the Information Privacy Principles (**IPPs**) to ensure they are clear, and to assist organisations to interpret and apply the IPPs consistently. Public consultation was finalised in 2023-24, with work continuing on the re-drafting of the Guidelines. This includes developing new scenarios to support the practical application of the IPPs to trending scenarios, and ensuring emerging trends and key issues such as Artificial Intelligence (**AI**) are included.

3. **How will the co-regulatory approach as described at the public hearing improve and build on OVIC's current practice? How, if at all, is this approach connected with OVIC's development of a new evaluation and assessment framework for its education and prevention program? When will that framework be finalised?**

A co-regulatory model for OVIC means that regulated agencies are empowered to proactively implement information handling practices, policies and procedures based on the requirements of the

FOI Act and the *Privacy and Data Protection Act 2014* (**PDP Act**), and OVIC's expectations of best practice. Part of this co-regulatory approach has always been within OVIC's regulatory strategy. For example, it is clear to agencies how OVIC performs its functions and makes decisions about its regulatory action. This allows agencies to align their practices accordingly, and effectively partner with OVIC to regulate information privacy, information security and access to information.

Privacy, FOI and information security span across various industries within the VPS. Different agencies have different needs and uses for the information they collect and hold. A co-regulatory model recognises this complexity and provides regulated entities with flexible solutions to often industry-specific problems. Critically, this flexibility must be underpinned by clear legislative obligations and OVIC's regulatory and enforcement powers.

This is why one of OVIC's strategic priorities in its 2024-2027 Strategic Plan is to continue to create regulatory certainty to the agencies it regulates and the Victorian public. OVIC aims to achieve this through:

- updating internal processes and existing guidance materials that reflect recent shifts in technology and information management
- convening events with stakeholders such as the Victorian Privacy Network, International Access to Information Day, Privacy Awareness Week and Victorian Information Security Network
- identifying trends in international privacy, freedom of information and information security practice through participation in inter-agency practice groups
- developing policy options for legislative reform.

OVIC's ongoing regulatory strategy acknowledges that when agencies know what to expect from a regulator, they can take actions that are more aligned with best practice. This extends to the public when lodging privacy or FOI complaints or applying for review of an agency decision.

OVIC has a small budgetary and staffing presence as an integrity body and, to continue its demonstrated effectiveness, it needs to encourage, assist and educate agencies on how to implement best practice in information management. Incident prevention relies on collaborating constructively with agencies and fostering relationships where they feel comfortable acting or otherwise seeking OVIC's guidance.

The co-regulatory model does not mean that OVIC seeks to limit regulatory action to ensure compliance with the FOI and PDP Acts. A key priority of OVIC's Strategic Plan is to "Identify and address regulatory trends, issues and risks" and OVIC will continue to use its powers to address regulatory concerns in efficient, effective and proportionate ways. The co-regulatory approach recognises that it is not possible for OVIC to act on all instances of non-compliance. Rather, supporting the uplift of practices within agencies is the most efficient way of meeting the objects of the FOI and PDP Acts.

Consultations with agencies are increasing

Organisations frequently consult OVIC on initiatives and reforms that intersect with privacy, information security and FOI. Consultations involve providing guidance and feedback on proposed government projects, initiatives, policies, procedures, guidelines, and legislative proposals. Some of the key themes raised in consultations with OVIC included proposed government policy reforms, AI, information sharing, digital identity, and access to information.

Many of these consultations are led by OVIC's Policy team with input from other teams. In 2023-24, OVIC's Policy team was involved in 80 consultations with organisations. This is up from 67 consultations in 2022-23. Additionally, other program areas of OVIC regularly interface with VPS agencies in informal consultations which include following up on new policies and programs, legislated reporting obligations, and preliminary inquiries. This increase in agency-initiated consultations is reflective of how a co-regulatory approach can drive positive change in information management practice and culture. Organisations see value in consulting with OVIC, as it helps them to improve their practices.

Evaluation and assessment framework

Critical to the success of a co-regulatory approach is education. OVIC has a responsibility to assist public sector employees at all levels to understand their roles in cultivating safe information practices. Developing an evaluation and assessment framework is part of this responsibility. In April 2022, the Committee recommended that OVIC, and other integrity agencies, develop an evaluation and assessment framework for its education and prevention initiatives as part of its Inquiry into the education and prevention functions of Victoria's integrity agencies.[1]

The framework will aim to understand how OVIC is providing its stakeholders with the skills they need to meet their obligations, and will complement the co-regulatory approach by further ensuring that agencies are better able to adhere to the requirements of the FOI and PDP Acts. The framework is intended as a more rigorous evidence base of the effectiveness of OVIC's educational initiatives. It will inform future educational programs and identify new or preferred educational methodologies. OVIC's framework is expected to be delivered in late 2025.

4. **Could you elaborate on OVIC's initiatives to understand the causes and impacts of agency data breaches in Victoria and how they might be prevented or mitigated (for example, breaches in hospitals, courts and tribunals). Are there any legislative reforms, or other measures, that would improve the oversight of, and agency transparency and accountability for, data breaches?**

Currently, there is no legislated requirement for VPS agencies to report information privacy or information security incidents to OVIC or to individuals whose information may be compromised.

[1] The Integrity and Oversight Committee's report is available at https://www.parliament.vic.gov.au/4af99d/contentassets/4cd6614380794503b5fa2c2200e4beed/ioc_59-04_education_and_prevention_functions_victorian_integrity_agencies_2.pdf.

Despite this, OVIC has implemented a raft of initiatives that aim to understand the causes and impact of data incidents in Victoria, including:

- OVIC's Information Security Incident Notification Scheme
- running the Victorian Information Security Network, Victorian Privacy Network and Privacy Roundtable, which encourage agencies to share insights with OVIC and one another
- publishing risk statements based on security incident insights reports
- other stakeholder engagement activities and relationships that allow OVIC to understand the causes of agencies' incidents
- OVIC's regulatory action, which provides comprehensive insights into the causes of incidents that have led to the regulatory action.

Incident notification through the VPDSS

While the Committee's question mentions data breaches, this term may not capture the full range of incidents that the Committee is referring to. A serious incident may occur which does not constitute a data breach. An incident refers to a compromise of either confidentiality, integrity or availability of information whereas a data breach is an incident that results in the confirmed disclosure – not just potential exposure – of data. For example, a cyber-attack on an agency which shuts down their systems would be a significant incident but would not be a data breach – unless the agency's data is copied, transferred, retrieved or accessed by the perpetrator.

OVIC has implemented an Information Security Incident Notification Scheme through the VPDSS. Each of the 12 standards include suggested actions that agencies should take to adhere to the intent of the Standards, called elements. While each of the Standards is mandatory, the elements are strongly advised but not mandatory. One such element under Standard 9 is that all entities notify OVIC of 'incidents that have an adverse impact on the confidentiality, integrity, or availability of public sector information with a business impact level of 2 (limited) or higher.'

OVIC has provided an incident notification form and guidance on how to report to OVIC, what to report and when to report. These incident notifications assist OVIC in gaining insight into the current security risk profile of the Victorian public sector. This can be used for trend analysis and understanding of the threat environment as it relates to the protection of public sector information.

Since 2020, OVIC has published twice-yearly security incident insight reports that provide an overview and analysis of incidents notified via this scheme. VPS agencies can use these insights to inform their own information security risk assessments.

While there has been wide acceptance and use of this scheme by agencies, it is subject to several limitations:

- as this scheme is established as an element under Standard 9 it is not mandatory, despite OVIC having an expectation that agencies will comply

- due to the limited scope of public sector organisations subject to Part 4 of the PDP Act, the scheme does not apply to the local government, health services, courts or the higher education sector[2]
- the scheme does not create an obligation to notify individuals impacted by a breach or incident
- there are no penalties or consequences for failing to notify OVIC of a breach or incident.

While the Information Security Incident Notification Scheme does not apply to entities not captured by Part 4, OVIC still encourages these entities to report any incidents. This enables OVIC to assist those entities to minimise harm occurring from an incident and to implement better information security practices in the future.

Victoria needs a mandatory incident notification scheme

Victoria does not have a mandatory incident notification scheme where all VPS agencies are required to notify the regulator and individuals whose information has been compromised following an incident. This puts Victoria far behind other Australian jurisdictions, including New South Wales, Queensland, Western Australia and the Commonwealth.[3]

OVIC holds a strong view that a mandatory incident notification scheme is required for Victoria.

A mandatory incident notification scheme must apply to both information privacy and information security incidents. Victoria is unique in the Australian context in that the PDP Act provides for a specific protective data security scheme, which is not the case in other Australian jurisdictions. This recognises that all public sector information (not just personal information) is of value and must be subject to protections. An incident notification scheme must therefore apply to all incidents involving public sector information that meet a certain threshold.

Mandatory notification of impacted individuals is critical in safeguarding individuals' personal information and encouraging enhanced information security measures. According to a 2017 study by the Office of the Australian Information Commissioner, 95% of Australians believe that if a government agency loses their personal information, they should be told about it.[4] Individuals are empowered to take remedial action to protect their personal information, and in extreme cases, their safety. For example, individuals may move house if subject to domestic violence, change passwords, cancel credit cards, and update identity documents.

[2] Section 84(2) lists the organisations that are not subject to Part 4 of the PDP Act.
[3] The Commonwealth and New South Wales have established privacy incident notification schemes. Queensland's scheme will come into effect in July 2026, and Western Australia's recently passed *Privacy and Responsible Information Sharing Act 2024* contains a notifiable information breaches scheme.
[4] Australian Community Attitudes to Privacy Survey 2017 report, https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2017-report#figure16.

OVIC is also of the view that under an incident notification scheme, OVIC should have powers to require an agency to notify individuals affected by a breach and in some cases, make a public statement about the incident.

OVIC has undertaken extensive research on how an incident notification scheme could work in Victoria and would be pleased to share further details on this issue with the Committee.

All agencies should be subject to Part 4 of the PDP Act

Currently, local councils, universities, courts and tribunals, and public health service providers are expressly excluded from having to comply with information security obligations under Part 4 of the PDP Act.[5] Each of these sectors is responsible for delivering a range of critical functions and services to the Victorian community, and in doing so generates, holds, and handles significant amounts of public sector information (including personal information) necessary to carry out those functions and services.

The evidence shows that threat actors are increasingly targeting these sectors, with data breaches, cyber-attacks, and ransomware attacks now considered an expectation rather than a mere possibility.

For example, OVIC are aware that incidents are occurring in entities such as courts and tribunals.[6] These entities are exempt under section 10 of the PDP Act from the IPPs and VPDSS in relation to their judicial or quasi-judicial functions. Essentially, this places courts and tribunals beyond the oversight of OVIC and renders that sector completely opaque in terms of incidents that are occurring, unless the entity self-reports. Not knowing what kind of incidents are occurring and when they are occurring means harm caused by these incidents cannot be minimised effectively and vulnerable Victorians' information cannot be protected.

Broadening the application of the information security measures established under Part 4 of the PDP Act will assist these sectors to identify and mitigate risks, and protect information, assets, and services against a range of threats they now face. It will also extend OVIC's remit, creating regulatory certainty and assuring the Victorian community that a regulator has oversight of these sectors.

OVIC should have regulatory oversight of health information privacy

In its report on the Inquiry into the operation of the *Freedom of Information Act 1982* (Vic), the Committee recommended that the Health Privacy Principles (**HPPs**) under the *Health Records Act 2001* and the IPPs be consolidated, under the regulation of OVIC.[7] This legislative change is one that OVIC strongly supports. From the perspective of understanding the causes and impacts of incidents, and agencies being able to respond appropriately, it is logical to have a single regulator. OVIC has the experience and expertise to take on this role, and coupled with the expansion of Part 4 of the PDP Act

[5] That is, unless that body is performing a function on behalf of an entity that is subject to Part 4, in which case that body will have obligations under Part 4.
[6] OVIC's recent investigation into the use of ChatGPT by a Child Protection Worker, Court Services Cyber Incident Information, https://courts.vic.gov.au/news/court-services-victoria-cyber-incident
[7] See recommendation 96 of the Committee's report, https://www.parliament.vic.gov.au/4ae880/contentassets/6522402fb4ba4ae4b65de621f953f874/ioc-60-04-the-operation-of-the-foi-act-1982-vic.pdf.

to agencies not currently covered, consolidating the HPPs and the IPPs would streamline expectations for agencies and the public.

5. How does OVIC oversight the FOI, information security and privacy dimensions of outsourced government operations? What lessons has OVIC learnt from these oversight activities? Are there any legislative reforms, or other measures, that would improve the oversight, and transparency and accountability, of outsourced operations?

Freedom of information

The FOI Act applies to 'documents of an agency'. This includes a document in both the physical and constructive possession of an agency. Where an agency contracts out a task or function to a contracted service provider (CSP), issues can arise regarding access to documents created by the CSP for the purpose of performing their role under the contract, but which are not in the physical possession of the agency. In those circumstances, whether the agency has constructive possession of the document must be considered. This is a complex task, open to interpretation by an agency or third party.

This issue arose in 'EC3' and Department of Jobs, Precincts and Regions (Freedom of Information) [2022] VICmr 47 (27 June 2022). The applicant sought access to a behavioural interview tool assessment they undertook as part of a recruitment process that the agency had outsourced. The former Information Commissioner decided the agency did not have constructive possession of the document, having considered the contractual relationship between the various parties involved and the ability of the agency to access or request the document. However, the matter was later referred to the Victorian Civil and Administrative Tribunal where the former Information Commissioner's decision was overturned. VCAT ruled that the agency did have constructive possession of the document.

The opacity of constructive possession is why it is OVIC's view that a State contract between an agency and a CSP should always stipulate that the agency has a right to access information held by the CSP for the purposes of the contract and that any documents created by a third party will be subject to the FOI Act. This will ensure proper accountability and transparency of outsourced government functions and services.

Information privacy and information security obligations when outsourcing

Section 17 of the PDP Act applies to outsourcing arrangements between VPS agencies and CSPs, in respect of information privacy. Section 17(2) notes that a State contract may provide for the CSP to be bound by the IPPs for the purposes of the State contract, in the same way as the outsourcing party would be. Where this is the case, and where the applicable IPP is capable of being enforced against the CSP in accordance with the procedures in the PDP Act, privacy complaints can be made against the CSP. OVIC regularly considers whether it is the CSP or outsourcing party who is liable for a complaint, for example, if contractual provisions don't bind the CSP to the IPPs. In some cases, the contractual terms agencies use are lacking, meaning that their CSPs are not bound by the IPPs, resulting in the outsourcing party being liable for privacy complaints or incidents.

In relation to information security, section 88(2) of the PDP Act places the obligation on the agency head to ensure that a CSP does not contravene the VPDSS in respect of public sector information it handles. This means that VPS agencies will always be liable for the actions of their CSPs in relation to information security under Part 4 of the PDP Act.

Standard 8 of the VPDSS requires agencies to ensure that third parties securely collect, hold, manage, use, disclose or transfer public sector information. Agencies are required to include information pertaining to their compliance with Standard 8 in their Protective Data Security Plan (**PDSP**). The PDSP is submitted to OVIC every two years and is attested to in alternate years.

Despite this, anecdotal evidence suggests that agencies don't necessarily understand that they are accountable for third party arrangements and that, even when they are aware, they do not always conduct assurance processes to validate the controls in those arrangements. In the 2024 PDSP submissions received by OVIC, approximately 33% of agencies identified the management of third parties as a challenge. In response, OVIC has been liaising with VPS agencies on how they can uphold their obligations under the VPDSS, particularly in ensuring that third parties are able to implement best practice information security measures. OVIC is currently updating its guidance on outsourcing arrangements, which aim to help agencies understand their obligations when entering these arrangements.[8]

Oversight of outsourcing arrangements

Under section 8D(2)(b) of the PDP Act, the Information Commissioner and Privacy and Data Protection Deputy Commissioner have a function to conduct monitoring and assurance activities, including audits, to ascertain agencies' compliance with data security standards. In 2022, OVIC conducted an audit of four organisations to establish whether they had appropriate practices and procedures in place to ensure third parties are handling public sector information securely. The findings of the audit are published in the Audit of information security in third-party arrangements under section 8D(2)(b) of the *Privacy and Data Protection Act 2014* (Vic) report. Further insights on agencies' adherence to Standard 8 are also gained from OVIC's incident notification scheme.

The Information Commissioner and Privacy and Data Protection Deputy Commissioner also have a function under section 8C(2)(e) of the PDP Act to carry out investigations and issue compliance notices in relation to information privacy. Where CSPs are bound by the PDP Act, OVIC can take regulatory action where there has been a flagrant or serious contravention of the IPPs.

For example, in July 2023 OVIC published a report about an investigation into misuse of Department of Health (Department) information by CSP employees during the pandemic response. While the Department was the subject of the investigation, rather than the CSP, a central aspect of the investigation's findings and recommendations was the Department's oversight of compliance with contractual obligations relating to information handling.

[8] A copy of the draft updated guidance, on which OVIC conducted public consultation in late 2024, is available on OVIC's website at https://ovic.vic.gov.au/public-consultation-on-outsourcing-in-the-victorian-public-sector-resource/.

Additionally, in 2023 OVIC launched an investigation into the Datatime Services Pty Ltd (**Datatime**) data breach. Datatime was a company that provided document scanning and data entry services, and was a CSP to VPS agencies. The investigation exposed deficiencies in Datatime's understanding of critical information security and privacy concepts, such as destruction of data and cybersecurity controls. Datatime was voluntarily wound up in October 2023, which meant it was not possible to formally determine compliance with the IPPs.

However, there were several key lessons from this incident for VPS agencies that engage CSPs. These lessons include that agencies should:

- conduct appropriate due diligence in relation to a prospective CSP's information security and privacy posture, to assess it will be capable of appropriately handling personal information
- seek specific advice from a CSP on the cybersecurity resources and controls it has in place
- ensure that any clauses in a State contract relating to information handling are clear, unambiguous and understood by all parties
- actively monitor a CSP's compliance with the IPPs and any contractual obligations relating to information handling, which may include attestations, surveys, reports, site visits or audits.

Further, OVIC regularly conducts preliminary inquiries under its Regulatory Action Policy into issues of regulatory concern involving CSPs. These have been used to gain information to assess the need for formal investigation, gain assurances about steps taken to remediate information security incidents, and/or bring about changes to information handling practices without the need for more formal regulatory action.

These preliminary inquiries have included issues such as a council's use of audio recording services provided by a CSP in the context of noise complaints, allegations of unauthorised access to sensitive departmental systems by CSP staff, a cyber-attack on a CSP to a department, and a council's use of a CSP's AI services to monitor swimming pool users.

Proposed reforms to the PDP Act

There are a range of recommendations OVIC has for improving oversight of CSPs:

- **Mandatory incident notification scheme**: as discussed in response to question 4, a mandatory incident notification scheme for Victoria would provide greater transparency of incidents occurring by CSPs. Subjecting agencies to this scheme would enable them to pass on these obligations in contracts with CSPs, requiring them to report incidents to OVIC directly. The scheme should also require CSPs to notify affected persons of an incident, enhancing transparency and accountability.
- **Expanding the application of Part 4 of the PDP Act**: sections 88-89 of the PDP Act and Standard 8 of the VPDSS are subject to the same limitations as the incident notification scheme discussed in the response to question 4 — primarily that Part 4 of the PDP Act has a limited application and excludes health services, courts and tribunals, higher education organisations

and local councils. Expanding the application of Part 4 would place an obligation on these excluded agencies to ensure that third parties are responsibly handling public sector information.

- **Amending the wording in Part 4 of the PDP Act to include public sector data systems**: section 88(1) of the PDP Act requires an agency to not do an act or engage in a practice that contravenes a protective data security standard, in respect of public sector data and *public sector data systems*. However, sections 88(2), 89(2) and 89(3) only refer to public sector data and exclude public sector data systems. Despite this, there are instances where a CSP may have access to or use of a public sector data system such as outsourcing for ICT provisions and support. The PDP Act should be amended to include public sector data systems in these provisions.

6. **How many of the outstanding information security and privacy recommendations relating to Victoria Police by OVIC and its predecessors is OVIC aiming to resolve in 2025 and thereafter? What, in general terms, do these recommendations relate to? And how much progress, overall, has Victoria Police made in implementing them?**

OVIC is aiming to resolve the remaining recommendations over the next two years. This is dependent on timely replies from Victoria Police so OVIC can assess its responses. Victoria Police has now submitted 15 responses to the outstanding 16 recommendations and OVIC is now in the process of assessing those responses.

The recommendations mainly relate to identified gaps between the practices of Victoria Police and what was required under the Standards issued by the former Commissioner for Law Enforcement Data Security (**CLEDS**), the former Commissioner for Privacy and Data Protection, and OVIC. The recommendations remaining span from 2008 to 2022.

Since the initial establishment of CLEDS in 2005, there have been 271 recommendations made to Victoria Police. Whilst progress has been slow, approximately 94% of recommendations have been closed.

In addition to the formal recommendations made to Victoria Police relating to information security, in August 2022 OVIC made recommendations to Victoria Police under its information privacy functions, as part of its examination of Victoria Police's privacy and information handling training. OVIC's compliance monitoring activities in respect of the three recommendations made were addressed in OVIC's 2023-24 annual report.[9] The report noted that Victoria Police had met one recommendation, with the other two being partly met at that stage.

[9] See page 64 of the annual report for more detail on the implementation of the recommendations.

7. **Has OVIC been able to support agencies to process FOI requests in a timelier way as well as improve its own timeliness of reviews within the 2022-23 period? What lessons have you learnt from that period in relation to timeliness and delays? How will OVIC endeavour to improve both agencies' and its own timeliness in the future?**

Delays in decision making remain a significant issue for several agencies and are continuing to generate a large volume of complaints made to OVIC. Ongoing high volumes of incoming FOI requests, backlogs of existing FOI requests and resourcing issues are significant factors impacting agencies' ability to meet statutory timeframes under the FOI Act.

When OVIC receives a complaint about an FOI request where a decision is significantly delayed, OVIC's approach is to seek an explanation from the agency for the delay or the way it handled the FOI request. OVIC then monitors progress on the FOI request until a decision is made. However, OVIC does not have the power to compel an agency to make a decision, and a complainant is advised of their right to apply to the Victorian Civil and Administrative Tribunal on the basis of the agency's deemed refusal of the request.

There are several ways that OVIC works to support agencies to improve their timeliness in processing FOI requests. These include through:

- the publication of guidance, such as the comprehensive FOI Guidelines that step agencies through decision making under the FOI Act, practice notes and published review decisions
- FOI training sessions and eLearning modules, OVIC's ASKFOI agency information service, and regular stakeholder engagement, including through the Public Access Agency Reference Group
- OVIC's promotion of access to government information outside the FOI Act with its proactive and informal release policy template and guidance
- advocacy for legislative change to the FOI Act, emphasising the proactive release of information.

In 2022-23, OVIC saw an increase in the time taken to complete reviews and complaints from the previous financial year. In this period, the average time taken by OVIC to finalise an FOI complaint was 111.1 days. Overall, the average time to finalise a complaint increased by 15 days (15.6%) in comparison with 2021-22. The increase in time to complete complaints is attributable to increased delays in agencies responding to those complaints. OVIC does not have the power to compel an agency to make a decision and these complaints remain open with that agency until the decision is made.

In 2022-23, OVIC completed 60% of review applications within the 30-day statutory timeframe or as agreed by the review applicant. This was the same result as in 2021-22. However, the average time to complete a review increased from 110 days to 120 days. The increase in time taken to complete FOI reviews was due to the complexity of reviews and demands on OVIC's services.

Across 2022-23 and 2023-24, OVIC has made adverse findings against several agencies with respect to their compliance with the FOI Act and the FOI Professional Standards, arising from complaints and

reviews. As part of this process, OVIC met with those agencies to discuss the findings and prepared Continuous Improvement Plans, with a view to assisting the agencies to become compliant with the FOI Act and the Professional Standards, which OVIC believes is key to ensuring that FOI requests are processed in a timely fashion.

Formal adverse findings are addressed to the relevant agency's Principal Officer, who is responsible for their agency's FOI functions. Formal findings raise awareness of the issues faced by their FOI team and places responsibility on the Principal Officer to improve their agency's compliance with the FOI Act, including timeliness.

In 2025, OVIC is planning additional training and updates to its guidance on proactive and informal release as recommended by the Culture of implementing Freedom of Information in Australia report. A greater focus by agencies on proactively and informally releasing information will reduce the number of formal FOI requests they receive, allowing them to improve their timeliness in decision making.

OVIC will also continue to collaborate with the Public Record Office Victoria to harmonise guidance around recordkeeping and FOI, to strengthen agency knowledge and improve records management practices within the public sector.

OVIC's current focus is on improving its own timeliness and efficiency in finalising reviews, while continuing to conduct a thorough assessment of the documents and provide comprehensive reasons for decision. OVIC aims to do this by:

- streamlining its internal processes, where possible, including further refining its recommendation and correspondence templates
- focusing on prompt initial assessment of new applications to ensure necessary prioritisation and identify opportunities for informal resolution
- seeking tailored submissions from agencies on points in dispute only, to reduce time impost both on agencies and on OVIC
- exploring technology and automation options, budget permitting, that may reduce the burden of manual administrative tasks
- undertaking ongoing stakeholder engagement and training, including around adherence to the Professional Standards, and in particular, response timeframes to OVIC and the quality of initial decision letters
- skills development for OVIC staff.

8. Does OVIC consider that it receives sufficient funding for the following:
    a. audits to be proactive on information security
    b. capacity to undertake an independent review of the FOI Professional Standards?

OVIC's information security unit oversees approximately 2,500 Victorian Government agencies and its investigation team is limited in its ability to conduct audits. With its current funding, OVIC is an effective regulator, but with additional funding, OVIC could:

- devote more resources to its proactive audit function, enabling OVIC to pursue a range of matters that warrant examination
- expand its educational capabilities for online and in person activities and events.

In 2024, OVIC engaged KPMG to conduct an independent review of the FOI Professional Standards. KPMG's report and OVIC's response is published on the OVIC website.[10] OVIC will be updating the Standards based on KPMG's recommendations. Pursuant to section 6U(4) of the FOI Act, OVIC will consult on the draft updated Standards, and agencies and interested parties will have the opportunity to provide feedback and comments. This public consultation will occur in early 2025.

While OVIC can effectively perform its functions with its current resourcing, it would be extremely difficult for OVIC to continue to effectively oversight the VPS with further reductions to its staffing profile and resourcing.

9. Does OVIC have a view on the new measures introduced in New South Wales through the TD24-12 Charter of Independence for NSW integrity agencies?

OVIC supports the intent of the Charter of Independence for NSW integrity agencies and would welcome the introduction of a similar Charter for Victoria's integrity agencies.

OVIC holds a strong view that OVIC should perform its functions independently of government. In its submission to the Committee's Inquiry into the operation of the *Freedom of Information Act 1982* (Vic), OVIC made a series of recommendations to the Committee that would enhance OVIC's independence. These include:

- OVIC should be solely accountable to the Committee through provision of an annual report
- OVIC should not be required to report to a government department on its performance
- OVIC should receive its annual funding through an independent funding model, rather than through a government department, similar to other integrity agencies
- If funded through the parliament, OVIC should submit budget bids for additional funding directly to the Treasurer via the Department of Treasury and Finance (subject to endorsement by the Committee).

[10] See https://ovic.vic.gov.au/freedom-of-information/review-of-professional-standards-by-kpmg/.

OVIC is the only integrity body that does not receive its funding directly through the Parliament. Even so, the Independent Broad-based Anti-corruption Commission, the Victorian Ombudsman and the Victorian Auditor-General's Office have issued a statement requesting their funding be decided by an independent tribunal rather than the Parliament.[11] A Charter of Independence for Victorian integrity agencies should consider which funding model would best secure OVIC's independence.

A Charter of Independence for Victoria would signal to the Victorian public sector and the community that integrity agencies play a critical role in holding the government to account, and that integrity agencies are not subject to government direction or coercion. This would provide greater certainty to the community that OVIC exists to uphold the public's information rights, and not to act in the interests of the government.

A more independent funding model, such as receiving its budget directly from the Victorian Parliament or through an independent tribunal, would provide for greater transparency to the community in the allocation of OVIC's funding. Further, this model should allow OVIC to submit additional budget bids directly to those that make its budgetary decisions.. This is a critical step in ensuring the important work OVIC does to strengthen the community's information rights is given due consideration.

[11] See https://www.ibac.vic.gov.au/publications-and-resources/article/budget-independence-for-victoria%27s-independent-officers-of-parliament.