Australian Government

Department of Finance

Matt Yannopoulos PSM
Secretary

Our Ref: IS26-000003

Mr Josh Burns MP
Chair
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Chair

I enclose the Department of Finance's submission to the Joint Committee of Public Accounts and Audit *Inquiry into the management of client privacy in the Australian public sector,* addressing relevant matters in the inquiry's terms of reference.

I trust that this information will assist the Committee's inquiry.

Yours sincerely

Matt Yannopoulos PSM
Secretary

14 May 2026

Australian Government
Department of Finance

Department of Finance

Submission to the

Inquiry into the management of client privacy in the Australian public sector

May 2026

Contents

1. Introduction **3**

2. Intersection of the PGPA Act and privacy management **3**

2.1 Reporting on privacy management matters 4

3. Department of Finance's management of privacy matters **5**

3.1 Governance and risk framework 5

3.2 Privacy lifecycle controls and assurance 5

3.3 Data breach preparedness and response 5

3.4 Cyber Security and ongoing management 6

1. Introduction

The Department of Finance (Finance) welcomes the opportunity to contribute to the Joint Committee of Public Accounts and Audit's Inquiry into the management of client privacy in the Australian public sector. The Inquiry will examine public service entities' identification and management of privacy risks, their response strategy to information security breaches and threats, and matters related to the Auditor-General Report No.12 of 2025-26 (ANAO report).

This submission provides information on the intersection of the Public Governance, Performance and Accountability (PGPA) framework with privacy management, existing reporting arrangements, and the management of privacy obligations within Finance.

2. Intersection of the PGPA Act and privacy management

Privacy obligations for Commonwealth entities primarily arise under the *Privacy Act 1988* (Privacy Act).

The *Public Governance, Performance and Accountability Act 2013* (PGPA Act) supports the proper use of public resources by Commonwealth entities, including by requiring high standards of governance, performance and accountability. Under section 15 of the PGPA Act, accountable authorities are responsible for establishing and maintaining appropriate systems of risk management and internal control for their entities. Privacy risks should be considered and managed as part of an entity's broader risk management and internal control arrangements. Consistent with the principles-based nature of the PGPA Act, privacy risk management arrangements should be proportionate to an entity's size, functions, risk profile and the sensitivity of information handled, and comply with specific obligations under the Privacy Act.

Where an entity's functions are delivered through contractual or shared services arrangements, accountable authorities remain responsible under the PGPA Act for ensuring that appropriate risk management and control arrangements – including relating to privacy management – are clearly addressed in contracts and governance arrangements. Finance supports entities in this regard through template clauses for procurement contracts and grant agreements relating to privacy management and notifiable data breach obligations.

In addition, the PGPA Act imposes general duties on the officials of entities that complement obligations under other legislation. These include, for example:

- under section 25, the duty to act with care and diligence (which would include in relation to the collection and use of personal information in the course of official functions), and
- under section 28, the duty not to improperly use information obtained in an official capacity to gain a benefit or cause a detriment.

The PGPA Act reporting and audit arrangements are intended to promote transparency and accountability in entity operations, while ensuring that personal information is not inappropriately disclosed through public reporting. For example:

- section 37 of the PGPA Act provides that accountable authorities must ensure appropriate records relating to the performance of the entity are maintained, and that the

responsible minister and the Finance Minister are entitled to full and free access to this information, *subject to any Commonwealth law that prohibits disclosure of particular information*.

- section 25D of the Public Governance, Performance and Accountability Rule 2014 sets out reporting requirements where a Minister approves a grant in the Minister's electorate for a Commonwealth corporate entity and specifically provides that the Minister must ensure that information is excluded from the public report if disclosure would breach the Privacy Act or other legislation.

Finance supports entities to meet the requirements of the PGPA framework though a number of Resource Management Guides (RMGs) and related resources. This guidance includes:

- Duties of accountable authorities (RMG 200)
- General duties of officials (RMG 203)
- Implementing the Commonwealth Risk Management Policy (RMG 211).

2.1 Reporting on privacy management matters

Existing reporting

Commonwealth entities that are subject to the Privacy Act are required to report Notifiable Data Breaches (NDBs) to the Office of the Australian Information Commissioner (OAIC). The details of individual NDBs are not generally publicly disclosed to prevent further harm to individual privacy. However, the OAIC maintains a 'dashboard' of NDBs received and releases an annual report of NDBs. Both include specific data relating to NDBs disclosed by Australian Government entities.

Entities are separately required under the PGPA Act to disclose a range of relevant matters in their annual reports. These include:

- details about the corporate governance structures and processes that the entity had in place during the reporting period, and
- the particulars of any findings from (among others) the Australian Information Commissioner that have had, or may have, a significant effect on the operations of the entity.

In addition, accountable authorities must notify their responsible minister of 'significant issues', affecting the entity or any of its subsidiaries under section 19 of the PGPA Act. Where the significant issue includes significant non-compliance with the finance law, the Finance Minister must also be notified and the issue reported in the entity's annual report for the period.

Finance publishes detailed guidance for entities to support these reporting obligations, including:

- Annual reports for Commonwealth companies (RMG 137)
- Annual reports for corporate Commonwealth entities (RMG 136)
- Annual reports for non-corporate Commonwealth entities (RMG 135)
- Notification of significant non-compliance with the finance law (RMG 214).

The ANAO's recommendation

The ANAO report included a recommendation (Recommendation 5) that the Attorney-General's Department (AGD), in consultation with Finance, consider advice to Government on options to improve the transparency of entities' compliance with the Privacy Act.

Finance will work closely with AGD to consider the ANAO's recommendation and provide advice to Government. Any additional reporting requirements relating to privacy management would need to be carefully designed to:

- minimise the risk of additional harm to individual privacy and the security of entity systems
- ensure proportionality between the benefits and added administrative burden associated with additional reporting requirements, and
- take account of the existing obligations.

3. Department of Finance's management of privacy matters

3.1 Governance and risk framework

Finance recognises its obligations to maintain robust privacy and cyber controls in relation to its functions, including as a shared service provider. Finance manages security, cyber and privacy risks through established governance, risk and assurance frameworks. These risks are incorporated into Finance's enterprise risk management framework, with a conservative risk tolerance defined by senior leadership, and subject to oversight by existing internal governance structures, including Finance's Audit and Risk Committee.

Finance's privacy risk profile differs from entities that routinely manage high-volume client datasets. Nevertheless, these arrangements support Finance's role in modelling good practice across the Commonwealth and contributing to whole-of-government integrity and accountability.

3.2 Privacy lifecycle controls and assurance

Standardised privacy tools and guidance, developed by Finance's central Privacy team, support proportionate consideration of privacy impacts in projects, policy development and system changes. These arrangements are intended to promote consistent application of the Privacy Act and align with OAIC expectations regarding privacy-by-design and accountability.

3.3 Data breach preparedness and response

Finance maintains a formal data (privacy) breach response framework, including clear escalation pathways, central assessment of incidents and structured decision-making on notification to affected individuals and the OAIC. Finance also maintains mechanisms to capture and review breach information to support organisational learning and continuous improvement via its central Privacy team and regular integrity reporting to Executive Board.

Finance recognises the strong interrelationship between cyber security and privacy and manages these risks in a coordinated way, ensuring that protection of personal information is considered alongside broader information security, system accreditation and incident management arrangements.

No NDB has arisen from Finance's own systems of operations under the NDB Scheme, although certain third-party incidents have been assessed as notifiable in recent years.

3.4 Cyber Security and ongoing management

Finance's governance approach embeds cyber security into its core risk and compliance frameworks. It aligns with national standards such as the Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) and maintains robust internal policies to support secure operations. Regular maturity assessments using the Essential Eight, updated system authorisations, and refreshed policy artefacts ensure risks are actively managed. Governance also extends to third-party and hybrid cloud environments, with strengthened oversight and engagement to ensure external systems meet security expectations. This foundation enables informed decision-making and supports a resilient digital environment. This is further strengthened by the integration of clauses into commercial arrangements with third-party service providers to set expectations in relation to protecting data assets that Finance owns or for which it is responsible. This aligns with relevant legislation and frameworks, including the PGPA Act, Privacy Act and PSPF.