Submission to the Joint Committee of Public Accounts and Audit

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

1. Introduction

I make this submission in my personal capacity.

I welcome the Joint Committee of Public Accounts and Audit's inquiry into the management of client privacy in the Australian public sector. The inquiry concerns public service entities' identification and management of privacy risks, their response strategy to information security breaches and threats and matters related to Auditor-General Report No. 12 of 2025–26, Managing the Privacy of Client Information in Services Australia (Parliament of Australia, 2026; Australian National Audit Office, 2025).

My submission focuses on one core proposition; client privacy in the Australian public sector should be treated as a security engineering, governance and public trust problem, not merely as a compliance problem.

Public-sector privacy deserves a higher standard than ordinary commercial privacy. People can often choose which private companies they deal with. They generally cannot choose whether they need Medicare, Centrelink, child support, tax, immigration, policing, health, education, employment services or identity-related government services. When government requires people to provide personal information to access essential services, government assumes a corresponding duty to protect that information with seriousness, technical discipline and institutional accountability.

This is especially important because government-held personal information can be highly sensitive, persistent and difficult to replace. A compromised email address or password may be changed. A compromised Medicare number, tax file number, address history, family information, health information, identity document, benefit history, immigration information or child support information may have consequences that persist for years, or in some cases, an individual's lifetime.

2. Core position

The Committee should recommend that Australian public-sector entities manage client privacy through an integrated privacy-security framework built around:

- data minimisation;
- clear purpose limitation;
- privacy threat modelling;
- privacy impact assessments for high-risk activities;
- strong access controls;
- secure logging and audit trails;
- retention and destruction discipline;

- third-party risk management;
- breach rehearsals and timely notification;
- public transparency;
- correction and redress pathways;
- measurable assurance rather than policy documents alone.

The existence of a privacy policy, Privacy Officer, Privacy Champion or annual privacy management plan is not enough. Those mechanisms matter but they must be connected to actual operational controls, system design, audit evidence and measurable risk reduction.

3. Public-sector privacy is a trust function

The ANAO report records the OAIC's view that individuals often do not have a choice in providing personal information to government agencies to access services and that government agencies, particularly service-delivery agencies should model best practice and build community trust in their ability to protect personal information (Australian National Audit Office, 2025).

That is the correct starting point. Public-sector privacy is not just an individual-rights issue. It is a trust issue. If people believe government systems cannot protect their information, they may avoid services, provide incomplete information, resist digital services, or lose confidence in public administration.

Trust cannot be rebuilt through reassurance alone. It requires visible, verifiable controls. Public-sector entities should be able to show how they know what personal information they hold, why they hold it, who can access it, how long it is retained, how it is protected, how access is monitored, how breaches are handled and how affected people can seek correction or redress.

4. Privacy risk should be treated as enterprise risk, not a specialist silo

The ANAO found that Services Australia had largely appropriate policies to meet Privacy Act requirements but gaps in arrangements to manage privacy risks at the enterprise level. The ANAO also found that Services Australia did not have a privacy risk management plan or privacy-specific enterprise risk or risk tolerance statement, despite having a high-risk privacy profile (Australian National Audit Office, 2025).

This is a critical distinction. Privacy should not be treated as a specialist compliance issue sitting outside core enterprise risk management. Privacy risk should sit beside cyber security risk, fraud risk, operational risk, legal risk, reputational risk and service-delivery risk.

The Committee should recommend that high-risk public-sector entities be required to maintain an enterprise-level privacy risk management plan that includes:

- a clear privacy risk appetite or tolerance statement;
- data inventories for major systems and services;
- identification of high-risk datasets;
- assessment of cumulative risk across linked systems;
- explicit treatment of third-party and supplier risks;

- privacy-specific control owners;
- measurable control effectiveness indicators;
- board, executive or senior committee reporting;
- regular independent assurance.

This would prevent privacy from becoming a paper framework disconnected from technical and operational reality.

5. Privacy should be engineered into systems from the beginning

The Australian Government Agencies Privacy Code states that APP 1 implicitly promotes a privacy-by-design approach by requiring agencies to take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs and any binding APP code. The Code's objectives include enhancing privacy capability and accountability, promoting good privacy governance and building community trust in agency information handling (OAIC, 2017).

Privacy-by-design should be operationalised as a design discipline. For every major system or service handling client information, agencies should be required to document:

- what personal information is collected;
- the legal authority and purpose for collection;
- whether each field is necessary;
- who has access to the data;
- whether access is role-based and least-privilege;
- whether sensitive fields are segregated or masked;
- where the data is stored and backed up;
- what third parties can access it;
- how long it is retained;
- when it is destroyed or de-identified;
- what audit logs exist;
- how misuse or unusual access is detected;
- what happens if the system is breached.

This should not be reserved only for new projects. Legacy systems often hold the most sensitive data and may have the weakest architecture. High-risk legacy systems should be progressively brought under the same privacy engineering discipline.

6. Data minimisation should be a practical control

Data minimisation is one of the most important privacy controls because information that is not collected, not copied, not retained and not unnecessarily linked cannot later be breached, misused or misinterpreted.

APP 11 requires an APP entity to take active measures to ensure the security of personal information it holds and to actively consider whether it is permitted to retain that information. It also requires reasonable steps to destroy or de-identify personal information once it is no longer needed unless an exception applies (OAIC, 2025a).

The Committee should recommend that agencies treat data minimisation and retention discipline as operational controls. Agencies should be required to review whether high-risk data fields are still necessary, whether copies are being created unnecessarily, whether logs contain excessive personal information, and whether retention periods are justified.

A useful test is; if this dataset were breached tomorrow, could the agency explain why every category of information in it needed to be collected and retained?

7. Privacy impact assessments should be more transparent and more useful

The ANAO found that Services Australia undertakes privacy impact assessments but identified record keeping deficiencies, lack of public consultation and limited public information beyond report dates and titles (Australian National Audit Office, 2025).

Privacy impact assessments should not become internal documents that exist merely to satisfy process. For high-risk activities, they should be practical, evidence-based and capable of being externally scrutinised where security and operational risks allow.

The Committee should recommend that public-sector entities maintain meaningful public PIA registers. At minimum, a PIA register should include:

- the project or system name;
- the date of assessment;
- the type of personal information involved;
- whether sensitive information or government identifiers are involved;
- the broad purpose of the activity;
- the main privacy risks identified;
- the main mitigations adopted;
- whether consultation occurred;
- whether the project proceeded, changed or was stopped because of privacy risk.

Full PIAs may not always be publishable. However, publishing only dates and titles is often insufficient for public accountability. Agencies should publish the maximum useful summary that can be released without creating operational, security or confidentiality risks.

8. Third-party and ecosystem risk must be treated as government risk

Public-sector privacy risk does not stop at the edge of a government agency. Modern public services depend on vendors, cloud providers, identity providers, software platforms, call-centre services, data brokers, contractors, grant recipients and partner agencies.

The ANAO found that third parties were not required to notify Services Australia following a data breach involving government identifiers, creating a risk to the timeliness of assessments of such breaches (Australian National Audit Office, 2025).

That is a serious structural issue. If government identifiers are compromised through a third party, the affected government agency may still be the entity best placed to assess downstream risk, protect the individual and prevent identity fraud. Notification obligations should reflect that reality.

The Committee should recommend that contracts, grants, service agreements and data-sharing arrangements involving personal information or government identifiers include enforceable requirements for:

- timely breach notification to the relevant agency;
- minimum security controls;
- audit rights;
- breach simulation or incident response co-operation;
- restrictions on subcontracting;
- data location and access controls;
- retention and deletion obligations;
- reporting of suspected credential compromise;
- sanctions for failure to notify or protect data.

Government should not outsource privacy risk without retaining visibility and control.

9. Breach response should be rehearsed before a breach occurs

The OAIC explains that a notifiable data breach occurs when personal information is accessed or disclosed without authorisation or is lost and the breach is likely to result in serious harm. Entities covered by the Privacy Act must notify affected individuals and the OAIC in those circumstances (OAIC, 2025b).

The ANAO report noted that business and government reported 1,113 data breaches in 2024, up from 893 in 2023, and that Services Australia recorded 6,042 privacy incidents from 2022–23 to 2024–25. It also recorded 89 notifiable data breaches reported by Services Australia to the OAIC in 2024–25, up from 50 in 2023–24 (Australian National Audit Office, 2025).

Breach response is therefore not a theoretical issue. Public-sector entities should assume that breaches, attempted breaches, credential attacks, phishing, social engineering and third-party compromises will occur.

The Committee should recommend that high-risk agencies maintain rehearsed breach response playbooks covering:

- triage and severity classification;
- legal and privacy assessment;
- technical containment;
- affected-person identification;
- communications;
- third-party and interagency co-ordination;
- identity protection and remediation pathways;
- post-incident review;
- reporting to senior executives and oversight bodies.

Breach notification should be timely, plain-English and practically useful. Affected people should be told what happened, what information was involved, what the agency is doing, what the person should do and what support is readily available.

10. Access controls and audit logs should be treated as civil-liberties safeguards

Access control is not merely an administrative issue. It is a privacy and civil-liberties safeguard.

Public-sector entities should implement least-privilege access to client information. Staff should only access the information needed for their role, for a legitimate purpose and for the minimum period required. Access to highly sensitive datasets should be more tightly controlled, with stronger authentication, approval workflows and monitoring.

Every access to high-risk client information should be logged. Logs should record:

- who accessed the information;
- when they accessed it;
- what record or data category was accessed;
- the system used;
- whether information was exported, printed or disclosed;
- the stated or inferred business purpose;
- whether the access triggered an alert or review.

Audit logs should be protected from tampering and reviewed for unusual patterns. Examples may include repeated access to records outside a staff member's caseload, access to high-profile or sensitive clients, bulk exports, after-hours access, unusual search patterns or access shortly before resignation.

Without auditability, privacy policies rely too heavily on trust. With auditability, agencies can deter misuse, detect misuse and prove appropriate handling.

11. Cyber security and privacy governance should be integrated

The Committee's inquiry expressly concerns public-sector response strategy to information security breaches and threats. Privacy and cyber security should therefore be treated as overlapping disciplines.

The Australian Signals Directorate reported that the OAIC received 595 notifiable data breach notifications between July and December 2024, a 15 per cent increase on the previous six months and that 2024 marked the highest number of notifications in a year since the Notifiable Data Breaches scheme commenced in 2018 (Australian Signals Directorate, 2025).

The Committee should recommend that privacy governance be integrated with cyber security governance. This should include:

- mapping critical personal information assets;
- applying appropriate Essential Eight maturity targets;
- testing restore capability for systems holding personal information;
- phishing-resistant authentication for privileged access where possible;
- privileged access management;
- vulnerability management;
- logging and detection for data access anomalies;

- incident response exercises that include privacy notification and client remediation;
- joint reporting to security, privacy and executive governance committees.

Privacy teams should understand technical risk. Security teams should understand privacy impact. Executive governance should receive a combined picture.

12. Public reporting should be clearer and more comparable

The ANAO recommended enhanced reporting on privacy and identified transparency issues around privacy management. It also noted opportunities to publish more information about privacy management (Australian National Audit Office, 2025).

The Committee should recommend standardised public privacy reporting for high-risk public-sector entities. This could include:

- number of privacy incidents;
- number of notifiable data breaches;
- number of affected individuals;
- main causes of incidents;
- average time to detect incidents;
- average time to assess incidents;
- average time to notify affected individuals;
- number of PIAs completed;
- number of high-risk projects changed because of privacy findings;
- number of access misuse investigations;
- number of substantiated staff misuse cases;
- privacy training completion rates;
- progress against privacy maturity targets.

This reporting should be aggregated and de-identified where necessary. The purpose is not to punish agencies for detecting and reporting incidents. The purpose is to create comparable, public accountability for maturity, timeliness and improvement.

13. Privacy assurance should be evidence-based

The ANAO recommended that Services Australia implement a privacy assurance strategy to assess compliance with its privacy obligations, and Services Australia agreed (Australian National Audit Office, 2025).

This should be treated as a broader lesson for the public sector. A privacy assurance strategy should not merely ask whether policy documents exist. It should test whether controls work.

Evidence-based assurance should include:

- sampling access logs;
- reviewing whether staff access matches business need;
- testing whether deletion and retention rules operate in practice;
- reviewing breach response timeliness;
- checking whether PIAs are completed before decisions are locked in;
- testing whether third-party controls are enforceable;

- reviewing whether privacy risks are escalated to enterprise governance;
- checking whether public privacy notices match actual data flows;
- assessing whether corrective actions are implemented.

The Committee should recommend that high-risk entities periodically include privacy handling in internal audit programmes, as the ANAO suggested for Services Australia's Centrelink, Medicare and Child Support programmes (Australian National Audit Office, 2025).

14. Correction, redress and client-facing pathways matter

Privacy protection should include a practical route for affected people to act when something goes wrong. If a person's government-held information is wrong, misused, breached, disclosed to the wrong party, used in an automated decision, linked incorrectly or retained beyond necessity, the person should have a clear pathway to seek correction, explanation or review.

The Committee should recommend that agencies provide plain-English client pathways for:

- accessing personal information;
- correcting inaccurate information;
- reporting suspected misuse;
- receiving breach support;
- requesting review of high-impact data use;
- escalating unresolved privacy concerns;
- understanding when personal information has been shared with another agency or third party.

A privacy system that is incomprehensible to the public is not functioning properly, even if it is internally documented.

15. Digital service design should include privacy by default

The Digital Service Standard states that Australian Government digital services should be user-friendly, inclusive, adaptable and measurable, and should support simple, secure and connected public services. Its criteria include "Build trust in design" and "Do no harm" (Digital Transformation Agency, 2024).

Those principles should apply directly to client privacy. Digital government services should avoid dark patterns, unnecessary consent bundling, confusing notices, excessive identity checks, unnecessary data sharing and forced use of high-risk channels where safer alternatives are available.

Privacy should be part of service quality. A service that is fast but overcollects data is not a good service. A service that is convenient but cannot explain how information is used is not transparent. A service that is digital-only but leaves vulnerable people unable to manage privacy risk is not inclusive.

16. Recommendations

I recommend that the Committee consider the following recommendations.

1. Require high-risk public-sector entities to maintain enterprise-level privacy risk management plans, including privacy risk appetite or tolerance statements.
2. Require major systems and services handling client information to maintain data inventories, purpose maps and access-control models.
3. Treat privacy-by-design as an engineering and governance obligation, not merely a compliance slogan.
4. Require meaningful privacy impact assessment registers, including public summaries of risks and mitigations where publication would not create security or operational risk.
5. Require third-party contracts and data-sharing arrangements involving personal information or government identifiers to include enforceable breach notification, audit, retention, deletion and security obligations.
6. Require high-risk entities to maintain rehearsed breach response playbooks, including client notification and remediation processes.
7. Require strong access logging and audit review for systems holding sensitive client information.
8. Integrate privacy governance with cyber security governance, including joint reporting on data assets, incidents, control maturity and breach response readiness.
9. Establish standardised public reporting for privacy incidents, notifiable data breaches, PIA activity, correction activity, access misuse investigations and assurance outcomes.
10. Require privacy assurance strategies to test operational control effectiveness, not merely the existence of policies.
11. Include handling of personal information in internal audit programmes for high-risk service-delivery agencies.
12. Ensure people have plain-English pathways to access, correct, challenge and seek review of government-held personal information.
13. Require agencies to review whether high-risk data fields remain necessary and whether retention periods are justified.
14. Ensure government digital service design applies privacy-by-default, data minimisation and “do no harm” principles.
15. Encourage JCPAA follow-up on implementation of ANAO recommendations and broader whole-of-government lessons from Auditor-General Report No. 12 of 2025–26.

17. Closing

The Australian Government holds some of the most sensitive information a person will ever provide. That information is often provided because people need essential public services, not because they have freely chosen a commercial relationship.

For that reason, public-sector privacy should be treated as a core function of public administration. It should be governed with the same seriousness as cyber security, fraud control, financial management and service delivery.

The Committee should recommend a model of public-sector privacy that is practical, technical and accountable; collect less, retain less, protect more, audit access, notify quickly, correct errors, manage third parties, test controls and report publicly.

That approach would not only reduce privacy harm. It would strengthen public trust in Australian Government services and the Australian Government as a whole.

REFERENCES

Australian National Audit Office (2025) Managing the Privacy of Client Information in Services Australia, Auditor-General Report No. 12 of 2025–26. Available at: https://www.anao.gov.au/sites/default/files/2025-12/Auditor-General_Report_2025-26_12.pdf

Australian Signals Directorate (2025) Annual Cyber Threat Report 2024–2025. Available at: https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025

Digital Transformation Agency (2024) Digital Service Standard. Available at: https://www.digital.gov.au/policy/digital-experience/digital-service-standard

Office of the Australian Information Commissioner (2017) Privacy (Australian Government Agencies – Governance) APP Code 2017. Available at: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/government-agencies/australian-government-agencies-privacy-code/privacy-australian-government-agencies-governance-app-code-2017

Office of the Australian Information Commissioner (2025a) Chapter 11: APP 11 Security of personal information. Available at: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information

Office of the Australian Information Commissioner (2025b) Notifiable data breaches. Available at: https://www.oaic.gov.au/privacy/notifiable-data-breaches

Parliament of Australia (2026) Inquiry into the management of client privacy in the Australian public sector. Available at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/ClientprivacyintheAPS