Australian Government
Services Australia

Our Ref: IS26-000003

Acting Chief Executive Officer
Charles McHardie AM

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

Email: jcpaa@aph.gov.au

Dear Mr Burns

Joint Committee of Public Accounts and Audit Inquiry

Services Australia welcomes the opportunity to contribute to the Joint Committee of Public Accounts and Audit (the Committee) inquiry into the management of client privacy in the Australian public sector and our submission can be found at Attachment A to this letter.

Services Australia is a large service delivery agency and a custodian of Australians' personal information. We take our responsibility to protect that information seriously, as public trust in government services depends on it. We hold and use personal information in order to deliver payments and services safely, lawfully and with integrity. We recognise that strong privacy practices are fundamental to maintaining community confidence in our services.

The Committee's inquiry provides an important opportunity to reflect on how government entities manage privacy risk in a complex and evolving threat environment. Services Australia acknowledges the findings of the Australian National Audit Office performance audit *Managing the Privacy of Client Information in Services Australia* and accepts that further work is required to strengthen enterprise-level risk management, transparency and assurance.

In response to these findings, Services Australia has adopted a practical, phased approach to improvement that focuses on embedding stronger privacy practices into business as usual. This includes strengthening enterprise-wide privacy risk management, improving transparency and record keeping, enhancing the use of complaints data as risk intelligence, and implementing a privacy assurance framework to support sustained oversight and accountability.

Our submission also sets out the privacy governance frameworks that underpin Services Australia's management of personal information, including how these frameworks are being strengthened in response to the Australian National Audit Office's findings.

Services Australia is also progressing broader, Agency-wide initiatives that support privacy outcomes and help prevent harm before it occurs. This includes work to strengthen authentication, reduce account compromise risk and improve end-to-end support for customers affected by identity crime. These initiatives reflect our commitment to protecting personal information while continuing to deliver services at scale in a high-risk environment.

Services Australia welcomes the Committee's role in examining these issues and will continue to engage constructively throughout the inquiry. We value the opportunity to work together with Government, regulators and whole-of-government partners to strengthen privacy protections, maintain public trust and support confident, transparent government service delivery.

Thank you for the opportunity to make this submission. Services Australia stands ready to provide further information and to assist the Committee as the inquiry progresses.

Yours sincerely

Charles McHardie
05 May 2026

Australian Government

Services Australia

Submission to the Joint Committee of Public Accounts and Audit Inquiry into the management of client privacy in the Australian public sector

Introduction

Services Australia (the agency) welcomes the opportunity to lodge a submission to the Joint Committee of Public Accounts and Audit inquiry into the management of client privacy in the Australian public sector.

The agency is one of the Australian Government's largest service delivery agencies and a significant custodian of Australian's personal information. The agency collects, uses and discloses personal information to deliver payments and services safely, lawfully and with integrity to millions of people. Protecting personal information is fundamental to maintaining public trust and confidence in government services, particularly with increasing digital service delivery that must operate in an environment of growing cyber threats and scams.

This submission addresses the Committee's terms of reference by setting out:

- the privacy governance and risk management frameworks used by the agency to meet its obligations under the Privacy Act 1988;
- the agency's capability to respond to privacy incidents, data breaches, cyber threats and malicious actors; and
- matters arising from Auditor General Report No. 12 of 2025–26: Managing the Privacy of Client Information in Services Australia, and the actions underway in response.

Privacy frameworks used by the agency to identify and manage privacy risks

Legislative and policy framework

The agency manages the privacy of client information within a comprehensive legislative and policy framework established by the *Privacy Act 1988*, the Australian Privacy Principles and the *Privacy (Australian Government Agencies – Governance) APP Code 2017*. These obligations are supported by whole-of-government frameworks including the Commonwealth Risk Management Policy and the Protective Security Policy Framework.

This framework recognises that the agency operates in a high-risk privacy environment. The agency holds personal information relating to most Australians, including sensitive information, and delivers services at scale to many vulnerable customers. This risk profile is further heightened by sustained malicious activity targeting government systems, online services and credentials.

Privacy Management Plan

In accordance with the Australian Privacy Principles (APPs) Code, the agency maintains and annually reviews a Privacy Management Plan (PMP). The PMP is the agency's primary framework for governing privacy risk and progressively strengthening privacy capability.

The PMP:

- assesses privacy maturity across core components of governance, culture, risk management, incident response, assurance, training and transparency;
- sets defined privacy goals and maturity targets informed by the Office of the Australian Information Commissioner guidance;
- identifies priority activities to address known risks and uplift capability over time; and
- supports structured monitoring and reporting to executive governance forums.

The Australian National Audit Office (ANAO) recognised the agency has existing privacy governance arrangements in place, while also identifying the need for stronger enterprise-level visibility and prioritisation of privacy risk. The agency has accepted this assessment and is strengthening the way PMP outcomes are integrated into broader enterprise risk and assurance processes.

Operational privacy policy and internal guidance

The Agency maintains an internal Operational Privacy Policy, supported by operational blueprints and guidance materials across service delivery, program design, data exchange and corporate functions.

These materials:

- translate legislative and regulatory obligations into practical, role-based guidance for staff;
- support consistent handling of personal information in high-volume operational environments;
- reinforce accountability through clearly defined responsibilities and mandatory training; and
- promote a culture of privacy awareness and lawful information handling.

The Operational Privacy Policy is reviewed regularly and forms a core component of first-line privacy risk management across the agency.

To support the consistent application of privacy obligations and early identification of risk, the agency also maintains an internal Privacy Contact Officer Network coordinated by the Privacy and Personal Information Release Branch. The network brings together representatives from business areas with significant privacy risk exposure to support dissemination of guidance, escalation of incidents and emerging issues, and sharing of operational insights to strengthen privacy capability and risk management across the agency.

Privacy incident and data breach response framework

The agency has an established Privacy Incident and Data Breach Response Plan, aligned with legislative requirements and Office of the Australian Information Commissioner guidance.

The framework sets out:

- mechanisms for identifying and escalating suspected privacy incidents;
- processes for assessing incidents and determining whether a notifiable data breach has occurred;
- statutory assessment and notification arrangements;
- defined roles and responsibilities across operational areas, legal functions and executive oversight; and
- reporting arrangements to senior executive committees.

Integration with enterprise risk management

Privacy is recognised within the agency's enterprise risk management framework as a specialised risk, with privacy impacts embedded across enterprise risks relating to data, cybersecurity, fraud and integrity.

Privacy risks are identified and managed through:

- group-level risk management plans aligned to enterprise risks;
- defined controls recorded in the Agency Control Library; and
- oversight through executive security, risk and audit committees.

In response to the ANAO findings, the agency is strengthening the consolidation, visibility and escalation of privacy risks to ensure privacy risk management is clearly articulated and monitored at an enterprise level.

Capability to respond to data breaches, cyber threats and malicious actors

The agency operates in an environment of sustained privacy and security threat, particularly from phishing, impersonation-based scams and third-party data breaches involving government-related identifiers. The agency's response capability is designed to manage both the likelihood of incidents occurring and the potential harm to individuals, particularly vulnerable customers.

Detection, response and escalation

The agency has established arrangements to support the early identification, escalation and management of privacy incidents and potential data breaches. Privacy incidents may be identified through staff reporting, customer complaints, third-party notifications and intelligence received from partner organisations.

Incidents are assessed centrally to determine severity, risk of harm and reporting obligations, with defined escalation pathways in place. These arrangements operate within existing executive governance structures and involve coordinated input from service delivery, technology, security, fraud, legal and corporate functions.

Regular reporting to senior executives supports visibility of emerging trends, systemic issues and response effectiveness, and informs ongoing risk management and capability uplift.

Notifiable data breaches

The agency complies with the Notifiable Data Breaches scheme under the Privacy Act 1988. The ANAO identified historical challenges in consistently meeting assessment and notification timeframes, reflecting the complexity and volume of incidents and the vulnerability of affected customers.

The agency accepted the ANAO's findings and recommendations and is implementing improvements to strengthen the consistency, timeliness, monitoring, record-keeping and enterprise-level assurance of notifiable data breach assessment and notification processes. These improvements build on existing incident response arrangements and are aligned to broader executive oversight and assurance mechanisms.

Malicious activity and third-party threats

A significant proportion of privacy incidents arise from malicious activity external to the agency, including third-party data breaches and impersonation-based scams. The agency, works closely with regulators, law enforcement, cyber security agencies and other government entities, as well as internal operational and technology stakeholders, to detect, assess and respond to these threats in a coordinated manner.

Where government-issued identifiers are exposed through third-party breaches, the agency undertakes risk assessment and harm-mitigation actions, which may include account protections, targeted customer support and public guidance. The agency supports whole-of-government reforms to improve the timeliness and reliability of third-party breach notifications to enable earlier and more effective intervention.

Matters arising from Auditor-General Report No. 12 of 2025–26

The ANAO performance audit Managing the Privacy of Client Information in Services Australia examined whether the agency is effectively managing the privacy of client information in accordance with legislative and policy requirements.

ANAO findings

The ANAO concluded that the agency is partly effective in managing the privacy of client information. The audit recognised that the agency has strong foundational arrangements in place, including defined governance roles, privacy policies and guidance, staff training, privacy incident and data breach response arrangements, and internal reporting mechanisms.

The ANAO also identified areas requiring further uplift, particularly:

- enterprise-level visibility and prioritisation of privacy risks;
- transparency and record-keeping for privacy impact assessments;
- transparency of data-matching activities;
- improved use of privacy complaints as risk intelligence; and
- the absence of a clearly articulated, enterprise-level privacy assurance strategy.

Agency response

The agency has agreed, or agreed in principle, to all recommendations directed to the agency and has adopted a phased approach to embed improvements into business as usual, consistent with existing governance and risk management arrangements.

The agency's response has been developed and prioritised through established executive governance forums, with input from operational, technology, security, fraud, legal and corporate stakeholders across the agency.

Enterprise-level privacy risk management (Recommendation 1 – agreed in principle)

A central theme in the ANAO's findings was the need for stronger enterprise-level visibility and prioritisation of privacy risk. The agency is strengthening this through a consolidated enterprise view of privacy risk, drawing together privacy risks identified through group-level plans and aligning them to existing enterprise risk management arrangements.

The agency is also strengthening clarity around privacy risk ownership and escalation obligations and is developing clearer risk tolerance settings to support consistent identification of systemic risks requiring executive oversight. This work is being integrated with the agency's Privacy Management Plan and monitored through existing governance reporting.

Transparency of data-matching activities (Recommendation 3 – agreed)

The ANAO identified the need for improved transparency of data-matching activities. The agency is strengthening its processes for publishing data-matching program protocols, including clearer information about program purpose, dates of operation and current status.

Arrangements are also being implemented to ensure published protocols are reviewed and kept current. Where necessary, exemptions are applied on a risk-based basis to balance transparency with legislative, privacy and security obligations.

Privacy impact assessment governance (Recommendation 6 – agreed)

The agency is strengthening the conduct and transparency of privacy impact assessments. This includes improved record-keeping for Privacy Threshold Assessments and Privacy Impact Assessments, ensuring threshold assessment requirements are applied consistently, and improving the timeliness and quality of entries on the public Privacy Impact Assessment register.

Where appropriate, register entries will include more meaningful descriptions commensurate with privacy and security risk, and stakeholder consultation will be considered to support transparency and confidence in privacy decision-making.

Use of privacy complaints as risk intelligence (Recommendation 7 – agreed)

The ANAO identified opportunities to strengthen the analysis and reporting of privacy complaints. The agency is enhancing categorisation, analysis and reporting, including regular trend and root-cause analysis to identify recurring or systemic issues.

Insights from complaint analysis are reported through governance forums and used to inform enterprise privacy risk management and assurance activities.

Privacy assurance (Recommendation 8 – agreed)

To strengthen enterprise-level assurance, the agency is developing a documented privacy assurance strategy. The strategy will define assurance scope, methodology and review cycles, including control effectiveness testing, review of privacy incident handling and notifiable data breach assessment and notification processes, and analysis of complaint trends.

The strategy is being aligned to the privacy risk register and embedded within the Privacy Management Plan to support sustained executive oversight and accountability.

Other initiatives supporting privacy outcomes

In addition to implementing the ANAO recommendations, the agency is progressing a range of agency-wide initiatives that reduce privacy risk and support customer privacy, harm prevention and remediation. These initiatives complement governance and assurance uplift by addressing practical privacy risk drivers in a large, high-volume service delivery environment, particularly risks associated with identity compromise, unauthorised access and malicious activity.

Identity theft and customer remediation

The Identity Theft Resolution project will commence from mid 2026 and will be implemented through a phased rollout. The project will establish an end-to-end Identity Theft Resolution Service for agency customers who experience identity compromise.

The service is designed to:

- provide a single point of entry for affected customers;
- reduce the need for customers to repeatedly tell their circumstances;
- enable coordinated containment, remediation and ongoing protection actions;
- improve coordination across programs; and
- support restoration of customer record integrity.

This initiative directly supports privacy harm mitigation by enabling faster, more coordinated responses when personal information or credentials are compromised.

Strengthening customer authentication

The agency is further strengthening authentication controls to reduce the risk of unauthorised access to personal information.

The Enterprise Customer Authentication Tool (ECAT) project supports a guided, technology-enabled authentication process and introduces additional authentication methods, including one-time passcodes and wider use of the Document Verification Service. This supports more consistent and robust application of authentication controls across service delivery channels.

Since the pilot commenced in October 2025 with a select cohort of staff, more than 71,000 customers have been authenticated using ECAT.

The Uplift Agency Linking Processes (UALP) project

UALP is delivering actions in response to the Commonwealth Ombudsman's Keeping myGov secure report. This includes implementing mandatory multi-factor authentication and strengthened fraud controls when linking Centrelink, Medicare and Child Support accounts to myGov.

The agency is also strengthening policy settings that support the myGov ecosystem to better prevent, detect and respond to any unauthorised access. These changes, endorsed through the myGov Strategic Committee, reflect the risk environment associated with shared digital platforms.

Scams, fraud and third-party risk management

A number of ongoing and established activities further support privacy outcomes:

- the Scams and Identity Theft Helpdesk (SAITH) continue to provide advice and education to staff, customers and members of the public about scams, identity security and containment actions following credential compromise. Demand for SAITH assistance has increased over the past few years, and matters are becoming increasingly complex;
- completed the first phase of the myGov security review, prompting users to strengthen account security, including reducing reliance on secret questions and answers. Inactive myGov accounts have been closed to reduce the risk of misuse without the individual's knowledge;
- is continuing to strengthen myGov fraud intelligence capabilities, including improving audit log quality, enhancing the myGov Incident Response System, and strengthening analysis and data-sharing arrangements;
- continues to work closely with intelligence partners, stakeholders (including the National Office of Cyber Security) and external organisations to respond to third-party data breaches and the broader global threat environment; and
- also operates a scams response model designed to detect, analyse and respond to impersonation scams, where offenders use agency impersonation and personal information exposed in third-party data breaches to target customer accounts. The Counter-scams Strategy builds on existing capability and recognises that addressing scams is a collective effort across government and industry.

Integration with fraud and integrity functions

The agency's fraud and corruption operational functions play an important role in identifying suspicious activity and potential misuse of credentials or personal information through the agency's long-standing fraud detection and investigative capability.

Where fraud activity or anomalous behaviour indicates a suspected privacy incident, this information is referred through established pathways for assessment by the agency's privacy function, in accordance with the Privacy Incident and Data Breach Response framework. This separation of roles ensures that fraud detection, privacy incident assessment and determination of notifiable data breaches are undertaken by the appropriate functions.

Together, these arrangements support early identification of privacy-related risks, enable timely escalation and assessment, and complement the agency's privacy governance and assurance framework by addressing operational drivers of privacy risk and reducing the likelihood and impact of harm to customers.

Whole-of-government considerations

The ANAO identified that some privacy risks arise from whole-of-government arrangements rather than the actions of individual agencies.

The agency supports:

- improved whole-of-government arrangements for timely notification of third-party data breaches involving government-related identifiers;
- clearer and more contemporary guidance on data-matching practices; and
- increased transparency of Privacy Act compliance at a whole-of-government level.

In relation to the ANAO Recommendation 2, directed to Government, the agency notes that timely notification of third-party data breaches involving government-related identifiers may require legislative and policy reform.

The agency will continue to work constructively with relevant policy owners and regulators, including the Attorney-General's Department, to support reforms such as potential changes to the Notifiable Data Breaches scheme that strengthen privacy outcomes across the Australian public sector.

Conclusion

The agency recognises that strong privacy governance is essential to maintaining public trust and confidence in government services.

The agency has established comprehensive privacy frameworks, including a Privacy Management Plan, operational privacy policies, incident and data breach response arrangements, and integration with enterprise risk management. The actions outlined in this submission demonstrate the agency's commitment to strengthening enterprise-level privacy risk management, improving transparency and assurance, and continuously uplifting how personal information is managed in a complex and evolving threat environment.

The agency welcomes the Committee's examination of these matters and will continue to engage constructively as the inquiry progresses.