

Managing the Privacy of Client Information in Services Australia

Services Australia

© Commonwealth of Australia 2025

ISSN 1036–7632 (Print)

ISSN 2203–0352 (Online)

ISBN 978-1-923405-79-0 (Print)

ISBN 978-1-923405-80-6 (Online)

Except for the content in this document supplied by third parties, the Australian National Audit Office logo, the Commonwealth Coat of Arms, and any material protected by a trade mark, this document is licensed by the Australian National Audit Office for use under the terms of a Creative Commons Attribution-NonCommercial-NoDerivatives 3.0 Australia licence. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.

You are free to copy and communicate the document in its current form for non-commercial purposes, as long as you attribute the document to the Australian National Audit Office and abide by the other licence terms. You may not alter or adapt the work in any way.

Permission to use material for which the copyright is owned by a third party must be sought from the relevant copyright owner. As far as practicable, such material will be clearly labelled.

For terms of use of the Commonwealth Coat of Arms, visit the *Australian honours system* website at <https://www.pmc.gov.au/honours-and-symbols/australian-honours-system>.

Requests and inquiries concerning reproduction and rights should be addressed to:

Chief Operating Officer
Corporate Management Group
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Or via email:

communication@anao.gov.au.



Canberra ACT
9 December 2025

Dear President
Dear Mr Speaker

In accordance with the authority contained in the *Auditor-General Act 1997*, I have undertaken an independent performance audit in Services Australia. The report is titled *Managing the Privacy of Client Information in Services Australia*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit to the Parliament.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website — <http://www.anao.gov.au>.

Yours sincerely



Dr Caralee McLiesh PSM
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out their duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7300
Email: ag1@anao.gov.au

Auditor-General reports and information about the ANAO are available on our website:
<http://www.anao.gov.au>

Audit team

Jason Millward
Carina Moeller
Ewan McPherson
Tatenda Zembe
Nathan Callaway

Contents

Summary and recommendations.....	7
Background	7
Conclusion	8
Supporting findings	9
Recommendations	10
Summary of entity responses	12
Key messages from this audit for all Australian Government entities	14
Audit findings.....	15
1. Background	16
Introduction	16
Rationale for undertaking the audit	19
Audit approach	19
2. Arrangements to manage privacy	21
Has Services Australia established appropriate governance and oversight arrangements for managing the privacy of client information?	21
Does Services Australia appropriately assess risks to the privacy of client information under its enterprise risk management framework?	25
Has Services Australia developed appropriate policies to manage the privacy of client information consistent with the <i>Privacy Act 1988</i> ?	32
Do Services Australia's data-matching activities comply with legislation and guidelines?	36
Has Services Australia implemented appropriate education and training arrangements to promote compliance with policy requirements?	42
Has Services Australia established effective arrangements to monitor and report on privacy arrangements?	44
3. Implementation of arrangements to manage the privacy of client information.....	48
Has Services Australia undertaken privacy impact assessments appropriately?	48
Has Services Australia complied with the <i>Privacy Act 1988</i> requirements in relation to privacy complaints and notifiable data breaches?	56
Does Services Australia have appropriate assurance arrangements over its management of the privacy of client information?	63
Has Services Australia implemented recommendations from the Office of the Australian Information Commissioner?	69
Appendices	73
Appendix 1 Entity responses	74
Appendix 2 Improvements observed by the ANAO	82
Appendix 3 Services Australia privacy management plan attribute maturity targets and assessments	83
Appendix 4 Complaints made to the Office of the Australian Information Commissioner	85
Appendix 5 Implementation of OAIC recommendations	86



Audit snapshot

Auditor-General Report No.12 2025–26

Managing the Privacy of Client Information in Services Australia



Why did we do this audit?

- ▶ Australians expect government entities to manage their personal information appropriately.
- ▶ Services Australia collects, stores and uses the personal information of more than 27 million people to deliver services and payments.
- ▶ This audit provides assurance to Parliament about whether Services Australia is effectively managing the privacy of client information.



Key facts

- ▶ The *Privacy Act 1988* provides the legal framework under which Australian Government entities must operate to protect personal information.
- ▶ Government entities must also adhere to the Privacy (Australian Government Agencies — Governance) APP Code 2017.
- ▶ Business and government reported 1,113 data breaches in 2024, up from 893 notifications in 2023.
- ▶ The Australian Government sector was the second highest for privacy complaints and third highest for notifiable data breaches.



What did we find?

- ▶ Services Australia is partly effective in managing the privacy of client information.
- ▶ There were partly appropriate arrangements to manage privacy.
- ▶ Services Australia was partly effective with implementing arrangements.
- ▶ There were deficiencies with risk management, data matching, record-keeping, privacy impact assessments, transparency and reporting.



What did we recommend?

- ▶ Five recommendations to Services Australia to improve risk management, data-matching practices, privacy impact assessments, complaints assessment and privacy assurance arrangements.
- ▶ Services Australia agreed in principle to one and agreed to four.
- ▶ Three recommendations to regulators to review data-matching arrangements, share third-party data breach information and enhanced reporting on privacy. Three were agreed, wholly or in principle.

57

privacy impact assessments completed by Services Australia from 2022–23 to 2024–25.

6,042

privacy incidents in Services Australia from 2022–23 to 2024–25.

89

notifiable data breaches reported by Services Australia to the OAIC in 2024–25 (50 in 2023–24).

Summary and recommendations

Background

1. The *Privacy Act 1988* (the Privacy Act) provides the legal framework under which entities and the government must operate to protect personal information. The Office of the Australian Information Commissioner (OAIC), the national privacy regulator, has stated that:

While individuals can generally choose the private sector organisations with which they share their personal information, they often do not have a choice in providing their personal information to government agencies to access their services. It is essential that government agencies, especially those with service delivery functions, model best practice and build community trust in their ability to protect the security of personal information they hold.¹

Rationale for undertaking the audit

2. The Australian community expects that government entities manage personal information appropriately and in accordance with the Privacy Act and other legislative requirements. Consistent with community expectations, the Privacy (Australian Government Agencies — Governance) APP Code 2017² (the APP Code) requires ‘all agencies to strive for best practice in privacy governance so they’re all managing personal information to a consistent high standard’. This ‘helps build public trust and confidence in personal information handling practices and new uses of data proposed by agencies’.

3. In 2023–24, the OAIC reported that the Australian Government sector was the second highest sector for privacy complaints and third highest for notifiable data breaches. In May 2025, the Privacy Commissioner advised that business and government reported 1,113 data breaches in 2024, up from 893 in 2023, noting:

The trends we are observing suggest the threat of data breaches, especially through the efforts of malicious actors, is unlikely to diminish, and the risks to Australians are only likely to increase. Businesses and government agencies need to step up privacy and security measures to keep pace.

4. Services Australia holds data and information on approximately 27.5 million Australians through Medicare, Centrelink and child support services and other programs it delivers on behalf of government. Prior ANAO audits³ and the Royal Commission into the Robodebt Scheme raised

1 Office of the Australian Information Commissioner (OAIC), *Notifiable Data Breaches Report: January to June 2024*, OAIC, Canberra, 16 September 2024, available from <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2024> [accessed 27 June 2025].

2 OAIC, *Privacy (Australian Government Agencies — Governance) APP Code 2017*, 2017, available from <https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes/privacy-australian-government-agencies-governance-app-code-2017> [accessed 27 June 2025].

3 Auditor-General Report No.38 *Management of Cyber Security Incidents*, ANAO, Canberra, 2024, available from <https://www.anao.gov.au/work/performance-audit/management-cyber-security-incidents> [accessed 17 June 2025].

Auditor-General Report No.42 *Interim Report on Key Financial Controls of Major Entities*, ANAO, Canberra, 2024, section 3.23, available from <https://www.anao.gov.au/work/financial-statement-audit/interim-report-key-financial-controls-major-entities-2023-24> [accessed 17 June 2025].

concerns about Services Australia's management of client information and compliance with the Privacy Act.

The Commission's findings about the possible breaches of the APPs in the Privacy Act in the Data-matching and exchanges chapter are significant and arise in the context of repeated and voluminous exchanges of personal information and data matches conducted by DHS and the ATO under the Scheme.⁴

5. This audit was conducted to provide assurance to the Parliament about whether Services Australia is effectively managing the privacy of client information in accordance with the Privacy Act, the APP Code and other legislative requirements.

Audit objective and criteria

6. The objective of the audit was to assess the effectiveness of Services Australia's management of the privacy of client information.

7. To form a conclusion against the objective, the ANAO adopted the following two high-level audit criteria.

- Has Services Australia developed appropriate arrangements to manage the privacy of client information consistent with the *Privacy Act 1988* and other legislative requirements?
- Has Services Australia effectively implemented arrangements to manage the privacy of client information?

Conclusion

8. Services Australia is partly effective in managing the privacy of client information. It has developed governance arrangements and processes for managing growing privacy risks such as increasing data breaches and cyber-attacks by malicious actors. Within the context of its high-risk privacy environment, its arrangements for managing privacy fall short of its risk profile and emerging risks.

9. Services Australia has developed partly appropriate arrangements to manage the privacy of client information. It has largely appropriate policies in place to meet the requirements of the Privacy Act, however, there are gaps in arrangements to manage privacy risks at the enterprise level. It did not document a rationale or seek legal advice when it decided to no longer undertake data matching under the *Data-matching Program (Assistance and Tax) Act 1990*.

10. Services Australia is partly effective in implementing its arrangements to manage the privacy of client information. It undertakes privacy impact assessments (PIAs), however, there were record keeping deficiencies, it does not conduct public consultation and does not provide information to the public on its PIAs beyond report dates and titles. There were other gaps with respect to implementation of arrangements including that it: does not analyse data on privacy incidents and complaints to assess risk; has not always been timely in making notifications of

4 Royal Commission into the Robodebt Scheme, *Report, Royal Commission into the Robodebt Scheme*, 7 July 2023, p. 627, section 8, Conclusion and p. 461, section 5.7 Possible Privacy Breaches, available from <https://robodebt.royalcommission.gov.au/publications/report> [accessed 6 January 2025].

notifiable data breaches (NDBs); and has not established an overarching assurance framework setting out how it assures itself that it is effectively managing the privacy of client information.

Supporting findings

Arrangements to manage privacy

11. Services Australia has established largely appropriate governance and oversight arrangements. To meet the requirements established in the APP Code, Services Australia has a Privacy Champion and two Privacy Officers. It has also established a Privacy Contact Officer Network to support the management of the privacy of client information. Reporting on privacy matters is provided to Services Australia's Security Committee. The Privacy and Personal Information and Release branch assists with processing privacy matters. Services Australia's privacy management plans include performance measures for the self-assessment of privacy-related activities and have been reviewed annually. Services Australia has a high-risk privacy profile. It has identified that it needs to mature its arrangements to be commensurate with this risk profile, with it not meeting 12 of 21 target maturity ratings for 2024–25. (See paragraphs 2.2 to 2.15)

12. Services Australia's enterprise-level Risk Management Policy and Framework categorises privacy as a 'specialist risk'. It does not have a privacy risk management plan or privacy specific enterprise risk or risk tolerance statement. Privacy related risks are incorporated in the group risk management plans of the seven service groups. There has been an increase in the volume of data breaches in Services Australia, largely caused by malicious actors. Third parties are not required to notify Services Australia following a data breach involving government identifiers, creating a risk to the timeliness of assessments of these breaches. Services Australia has not developed a technology security risk management plan as required by PSPF Direction 002-2024. (See paragraphs 2.16 to 2.58)

13. Services Australia publishes a privacy policy and privacy notices that largely comply with the requirements of Australian Privacy Principles 1 and 5. Services Australia does not regularly review its public privacy policy and privacy notices. Review of these products would benefit from client input. Services Australia maintains an internal operational privacy policy and 'operational blueprints' that provide guidance to staff. The operational privacy policy was reviewed in 2023–24. Services Australia has policies to support individuals access their own information, and to support appropriate data destruction. (See paragraphs 2.59 to 2.78)

14. Services Australia no longer undertakes data matching under the *Data-matching Program (Assistance and Tax) Act 1990* and instead follows the voluntary guidelines on data matching in Australian Government administration. This approach reduces transparency and accountability to Parliament. There was no documented rationale or legal advice to underpin this change. Services Australia has not fully implemented Robodebt Royal Commission recommendations relating to data matching. Services Australia has published 13 of 32 data-matching protocols. (See paragraphs 2.79 to 2.109)

15. Services Australia has implemented mandatory induction and refresher training programs for staff on their privacy responsibilities. Training completion rates met the 95 per cent target in 2024. (See paragraphs 2.110 to 2.116)

16. Services Australia produces a monthly executive report and a quarterly privacy dashboard report for its Security Committee and regular reporting to its Audit and Risk Committee. Services Australia does not publicly report on privacy incidents, complaints and notifiable data breaches. (See paragraphs 2.117 to 2.129)

Implementation of arrangements to manage the privacy of client information

17. Services Australia undertakes privacy threshold assessments (PTAs) for projects involving new or changed information arrangements. Higher risk projects are subject to privacy assurance advice or a privacy impact assessment (PIA). Services Australia appropriately undertakes PIAs, except that none included public consultation. Record keeping of PTAs and PIAs was deficient. Services Australia maintains a public PIA register. It does not publish PIAs. One of the 18 Freedom of Information requests for PIAs since 2020 was successful; 14 were refused on the basis of legal professional privilege. (See paragraphs 3.2 to 3.28)

18. Services Australia accepts privacy-related complaints through its complaint's mechanism. It does not analyse or report on privacy complaints, nor does it use data from privacy complaints to inform its risk assessments. Services Australia did not meet the legislated 30-day requirement for assessing potential NDBs in 2022–23 or 2023–24. It met this requirement in 2024–25. Services Australia did not notify affected individuals and the OAIC in accordance with its internal target timeframes, although performance improved in the first quarter of 2025–26. Services Australia has not documented its approach to assuring that its handling of NDBs complies with the Privacy Act. (See paragraphs 3.33 to 3.60)

19. Services Australia does not have a privacy assurance strategy. There are a range of internal controls and assurance processes, including user access monitoring, quality monitoring of calls and internal audit, that provide assurance over the management of personal information. Services Australia has unresolved ANAO user access controls audit findings which are not being addressed at a pace commensurate with the increasing risks to privacy. (See paragraphs 3.62 to 3.87)

20. Of the 13 recommendations made by the OAIC in three privacy assessments between 2020 and 2023, Services Australia has implemented nine, partially implemented two, and two recommendations were superseded by events. (See paragraphs 3.88 to 3.91)

Recommendations

Recommendation no. 1 Services Australia improve the identification, assessment and management of privacy risks by implementing an enterprise-wide privacy risk management plan.
Paragraph 2.34

Services Australia response: *Agreed in principle.*

Recommendation no. 2
Paragraph 2.53

The Australian Government consider implementing arrangements to support Services Australia being provided with timely notification of third-party data breaches involving government-related identifiers such as Medicare numbers and Centrelink reference numbers.

Attorney-General's Department response: *Agreed.*

Office of the Australian Information Commissioner response: *Agreed.*

Recommendation no. 3
Paragraph 2.98

Services Australia publish all data-matching program protocols on its website, including dates of operation, and regularly review the currency of the information published, except where an exemption has been sought in accordance with the Office of the Australian Information Commissioner's voluntary data-matching guidelines.

Services Australia response: *Agreed.*

Recommendation no. 4
Paragraph 2.104

The Australian Government review existing data-matching activities undertaken by Services Australia and other government entities to assess whether the current frameworks — the *Privacy Act 1988*, the *Data-matching Program (Assistance and Tax) Act 1990*, and the voluntary Guidelines on data matching in Australian Government administration — are appropriate for use with contemporary data-matching and information-sharing practices and provide sufficient transparency and accountability.

Department of Social Services response: *Agreed in principle.*

Attorney-General's Department response: *Noted.*

Office of the Australian Information Commissioner response: *Agreed.*

Recommendation no. 5
Paragraph 2.127

There is limited reporting to the Australian Parliament by Australian Government entities on their compliance with the *Privacy Act 1988*. Entities are not required to report in annual reports on their management of privacy. The Attorney-General's Department, in consultation with the Department of Finance as required, consider advice to the Australian Government on options to improve the transparency of entities' compliance with the *Privacy Act 1988*.

Attorney-General's Department response: *Agreed.*

Department of Finance response: *Agreed.*

Recommendation no. 6 Services Australia improves the conduct and transparency of its privacy impact assessment (PIA) processes by:
Paragraph 3.27

- (a) implementing external consultation arrangements for PIAs;
- (b) publishing a description of each PIA on its PIA register;
- (c) implementing arrangements to ensure PIAs are added to its public register in a timely manner;
- (d) reviewing the appropriateness using of legal professional privilege Freedom of Information requests for PIAs; and
- (e) publishing PIA reports to the extent that this does not exacerbate privacy or other risks.

Services Australia response: *Agreed.*

Recommendation no. 7 Services Australia undertake analysis and reporting of privacy complaints to understand trends, identify emerging risks and promote continuous improvement in its management of privacy.
Paragraph 3.47

Services Australia response: *Agreed.*

Recommendation no. 8 Services Australia implements a privacy assurance strategy to assess compliance with its privacy obligations.
Paragraph 3.86

Services Australia response: *Agreed.*

Summary of entity responses

21. The proposed audit report was provided to the Services Australia and extracts were provided to the Attorney General's Department, the Department of Finance, the Department of Social Services and the Office of the Australian Information Commissioner. Summary responses are reproduced below and full responses are at Appendix 1. Improvements observed by the ANAO during the course of this audit are listed in Appendix 2.

Services Australia

The Agency welcomes the report and notes the report recommendations aimed at further strengthening the Agency's management of privacy. Protecting privacy is a key part of the Agency's core business and promotes trust and confidence in the Agency to deliver government services to all Australians. The Agency actively promotes a culture of valuing and protecting information.

Attorney-General's Department

The department appreciates the important opportunity afforded by this audit to consider the potential for improvements to the legal frameworks and processes governing the handling of Australians' personal information, in particular, government-related identifiers and Tax File Numbers.

The department supports the Attorney-General to administer the *Privacy Act 1988* (Privacy Act), and notes the importance of all regulated entities maintaining strong protections for Australians' personal information in accordance with the Privacy Act. The department also notes that Government agencies such as Services Australia are subject to the Australian Government

Agencies Privacy Code, which has a key objective of enhancing the privacy capability and accountability of agencies.

The department has responded to the three recommendations that pertain to the department's responsibility for the Privacy Act, including the Notifiable Data Breaches scheme.

Department of Finance

The Department of Finance notes the findings in the report extract.

Department of Social Services

The Department of Social Services (the Department) appreciates and acknowledges the insights and opportunities for improvement outlined in the Australian National Audit Office (ANAO) report on Managing the privacy of client information in Services Australia.

The Department agrees in principle with Recommendation 4.

The Department is supportive of an independent review to assess the effectiveness of the *Data-matching Program (Assistance and Tax) Act 1990* to determine if it remains fit for purpose for contemporary data-matching and information sharing. The Department is ready to provide support to the review should it go ahead.

An independent review would ensure an arm's length and publicly transparent evaluation of data-matching activities conducted by Services Australia and other government entities to inform any potential legislative change.

The Department would assume the responsibility of and is committed to, progressing any suggestions that may result from an independent review, including amendments to, or a repeal of, the *Data-matching Program (Assistance and Tax) Act 1990*.

Office of the Australian Information Commissioner

The OAIC agrees in principle it would be beneficial for Services Australia to be notified of relevant third-party data breaches to enable it to act to prevent future breaches and carry out its functions. Such arrangements could require legislative reform, which is a matter for Government.

If a new reporting obligation is to be imposed it will be necessary to specify the entities to which the requirement applies and the threshold for notification. For example, consideration should be given to whether the obligation rests with third parties to directly notify Services Australia. The OAIC is not notified of all data breaches involving Services Australia or individual identifiers. The Notifiable Data Breaches scheme only requires entities regulated under the Privacy Act to notify the OAIC if a data breach is likely to result in serious harm to an individual.

Data matching activities potentially create significant privacy impacts for individuals. It is important that these activities are conducted in compliance with privacy obligations, and that agencies conducting data matching programs consider and manage privacy impacts during program development.

The OAIC is currently reviewing the voluntary *Guidelines on data matching in Australian Government administration*. The OAIC will consult relevant agencies during this process.

Key messages from this audit for all Australian Government entities

22. Below is a summary of key messages, including instances of good practice, which have been identified in this audit and may be relevant for the operations of other Australian Government entities.

Governance and risk management

- Good privacy practices are essential to ensure citizens trust the government to collect and use their personal information appropriately. In an environment of increasing data breaches, cyber threats and malicious actors, entities should regularly assess privacy risks to inform reviews of their privacy management plans and implementation of governance, policies, ICT controls, training, audit and assurance arrangements.
- Entities with specific or higher privacy risks should implement additional arrangements, such as those implemented by Services Australia with the privacy contact officer network, privacy assurance advice processes and data breach response plan. Arrangements could include a dedicated privacy risk management plan, privacy assurance strategy and scenario-based privacy training.

Transparency and accountability

- Building and maintaining public trust can be achieved by entities being transparent about their privacy management practices and responses to emerging privacy issues. Entities should publish data on privacy incidents and data breaches and engage with clients to review privacy policies and notices to ensure that these are easily understood.
- Privacy impact assessments (PIAs) are required for all high-risk projects and should, where possible, be informed by stakeholder consultation. External PIA registers should contain useful information about the assessments, and — to the extent that operational or security risks are not created — PIAs should be published.

Audit findings

1. Background

Introduction

1.1 The Australian Government collects, stores and uses personal information on every Australian citizen, resident and visitor. Strong privacy practices and policies are important as they influence how Australians think about, and perceive, the trustworthiness of government entities and other organisations.

1.2 The Office of the Australian Information Commissioner (OAIC) has stated that:

While individuals can generally choose the private sector organisations with which they share their personal information, they often do not have a choice in providing their personal information to government agencies to access their services. It is essential that government agencies, especially those with service delivery functions, model best practice and build community trust in their ability to protect the security of personal information they hold.⁵

Privacy framework

1.3 The *Privacy Act 1988* (the Privacy Act) provides the legal framework under which Australian Government entities, private organisations and businesses, and other specified entities⁶ must operate to protect personal information. The Privacy Act defines ‘personal information’ as:

Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- a) whether the information or opinion is true or not; and
- b) whether the information or opinion is recorded in a material form or not.

1.4 Certain types of information constitute personal information under the Privacy Act:

- sensitive information, where this information otherwise meets the definition of personal information, including: health information; information on an individual’s racial or ethnic origin, sexuality, or criminal record; and personal beliefs such as political opinions or religious beliefs;
- credit information, employee record information; and
- tax file number information.⁷

1.5 The Privacy Act sets out 13 Australian Privacy Principles (APPs) which govern standards, rights and obligations around:

- the collection, use and disclosure of personal information;

5 OAIC, *Notifiable Data Breaches Report: January to June 2024*, 16 September 2024, available from <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2024> [accessed 27 June 2025].

6 OAIC, ‘Rights and responsibilities’, available from <https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/rights-and-responsibilities> [accessed 28 July 2025]. Whether a private organisation of business is required to adhere to responsibilities under the Privacy Act is determined, in some cases, by the annual turnover of the organisation, and/or the type of organisation and what activities it undertakes.

7 OAIC, ‘What is personal information’, 5 May 2017, available from <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/what-is-personal-information> [accessed 6 July 2025].

- an organisation or agency's governance and accountability;
- integrity and correction of personal information; and
- the rights of individuals to access their personal information.⁸

1.6 Australian Government entities are required to handle personal information in accordance with the Privacy Act.⁹ All entities covered by the Privacy Act are subject to the Notifiable Data Breaches scheme, which requires entities to notify affected individuals and the OAIC when a data breach occurs that is likely to result in serious harm to an individual whose personal information is involved.¹⁰

1.7 Australian Government entities must also adhere to the Privacy (Australian Government Agencies — Governance) APP Code 2017 (the APP Code).¹¹ The APP Code is a legislative instrument issued under section 26G of the Privacy Act that requires entities to:

- have a privacy management plan;
- appoint a Privacy Officer, or Privacy Officers, and ensure that the Privacy Officer functions are undertaken;
- appoint a senior official as a Privacy Champion to provide cultural leadership and promote the value of personal information, and ensure that the Privacy Champion functions are undertaken;
- undertake a privacy impact assessment (PIA) for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information and which are likely to have a significant impact on the privacy of individuals;
- maintain a register of all PIAs conducted and publish this register, or a version of the register, on their websites; and
- take steps to enhance internal privacy capability, including by providing appropriate privacy education or training in staff induction programs, and annually to all staff who have access to personal information.

8 OAIC, *Australian Privacy Principles*, OAIC, December 2022, available from <https://www.oaic.gov.au/privacy/australian-privacy-principles> [accessed 7 January 2025].

9 The *Privacy Act 1988* applies to Australian Government entities, and to private sector and community organisations with an annual turnover of more than \$3 million.

10 Part IIIC of the *Privacy Act 1988* sets out requirements for notification of eligible data breaches. Serious harm can include identity theft, financial loss through fraud, a likely risk of physical harm, family violence, physical harm or intimidation, serious psychological harm and serious harm to an individual's reputation. See OAIC, 'Part 1: Data breaches and the Australian Privacy Act', 'Consequences of a data breach', 5 June 2024, available from <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/> [accessed 28 June 2025].

11 OAIC, Privacy (Australian Government Agencies — Governance) APP Code 2017, available from <https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes/privacy-australian-government-agencies-governance-app-code-2017> [accessed 22 January 2025].

Privacy Act review

1.8 The Attorney-General's Department completed a review of the Privacy Act in 2022, and the Australian Government response was published in September 2023.¹² The *Privacy and Other Legislation Amendment Act 2024* (Amendment Act) implemented proposals from the government response to the review. These included expanding the Australian Information Commissioner's powers, facilitating information sharing in emergency situations or following eligible data breaches, development of a Children's Online Privacy Code, enhancing protections for certain overseas disclosures of personal information, introducing new tiers of civil penalties, and increasing transparency about automated decisions which use personal information.

National regulator for privacy

1.9 The OAIC is the national regulator for privacy and an independent statutory agency established under the *Australian Information Commissioner Act 2010*. The OAIC's functions relate to the protection of the privacy of individuals in accordance with the Privacy Act, resolving privacy complaints and investigating potential data breaches, the provision of guidance on how to handle personal information and the promotion of privacy awareness. Alongside receiving notifications of eligible data breaches (see paragraph 1.6), the OAIC also has a range of regulatory powers, including 'to work with entities to facilitate legal compliance and best privacy practice, as well as investigative and enforcement powers to use in cases where a privacy breach has occurred'.¹³

Services Australia

1.10 Services Australia aims to 'support Australians by efficiently delivering high-quality, accessible services and payments on behalf of government'.¹⁴ It collects, stores and uses the personal information of over 27 million clients¹⁵ to support the delivery of 'services and payments related to social security, child support, students, families, aged care and health programs'. Services Australia shares data with the Australian Taxation Office and other entities across the Commonwealth, state and territory jurisdictions, and internationally, to support its own and their functions. At 30 June 2024, Services Australia employed 33,554 people.

1.11 The Australian Public Service Commission's 2024 Capability Review of Services Australia stated that:

Services Australia has the most frequent and direct interactions with the Australian public compared with any other Australian Government entity. Staff access to population-level personal citizen data is unmatched by any other Commonwealth agency. Staff adherence to the APS

12 Attorney-General's Department (AGD), *Privacy Act Review — Report 2022*, AGD, 2022, available from <https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report> [accessed 18 June 2025].

Australian Government, *Government response to the Privacy Act Review Report*, AGD 28 September 2023, available from <https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report> [accessed 18 June 2025].

13 OAIC, *Guide to privacy regulatory action*, (n.d.), available from <https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action> [accessed 23 June 2025].

14 Services Australia, *Corporate Plan 2025–26*, available from <https://www.servicesaustralia.gov.au/sites/default/files/2025-08/12637-2507-corporate-plan-25-26.pdf> [accessed 10 October 2025].

15 This report uses the term 'client' to refer to people who engage with Services Australia to receive a service or payment. The report includes quotes that use the term 'customer'. Both terms can be read interchangeably.

frameworks and policies, the *Privacy Act 1988* and other legislation protecting privacy and governing sharing and use of citizen data, is integral to upholding integrity in the programs and services they deliver, and helps to build trust with the Australian public.¹⁶

Rationale for undertaking the audit

1.12 The Australian community expects that government entities manage personal information appropriately and in accordance with the Privacy Act and other legislative requirements. Consistent with community expectations, the APP Code requires ‘all agencies to strive for best practice in privacy governance so they’re all managing personal information to a consistent high standard’. This ‘helps build public trust and confidence in personal information handling practices and new uses of data proposed by agencies’.

1.13 In 2023–24, the OAIC reported that the Australian Government sector was the second highest sector for privacy complaints and third highest for notifiable data breaches. In May 2025, the Privacy Commissioner advised that business and government reported 1,113 data breaches in 2024, up from 893 notifications in 2023, noting:

The trends we are observing suggest the threat of data breaches, especially through the efforts of malicious actors, is unlikely to diminish, and the risks to Australians are only likely to increase. Businesses and government agencies need to step up privacy and security measures to keep pace.

1.14 Services Australia holds data and information on approximately 27.5 million Australians through Medicare, Centrelink and child support services and other programs it delivers on behalf of government. Prior ANAO audits¹⁷ and the Royal Commission into the Robodebt Scheme raised concerns about Services Australia’s management of client information and compliance with the Privacy Act.

The Commission’s findings about the possible breaches of the APPs in the Privacy Act in the Data-matching and exchanges chapter are significant and arise in the context of repeated and voluminous exchanges of personal information and data matches conducted by DHS and the ATO under the Scheme.¹⁸

1.15 This audit was conducted to provide assurance to the Parliament about whether Services Australia is effectively managing the privacy of client information in accordance with the Privacy Act, the APP Code and other legislative requirements.

Audit approach

Audit objective, criteria and scope

1.16 The objective of the audit was to assess the effectiveness of Services Australia’s management of the privacy of client information.

16 Australian Public Service Commission, *Capability review: Services Australia*, 28 January 2025, p. 22, available from <https://www.apsc.gov.au/initiatives-and-programs/workforce-information/research-analysis-and-publications/capability-review-program/capability-review-services-australia> [accessed 31 January 2025].

17 Auditor-General Report No.38 of 2023–24 *Management of Cyber Security Incidents*.
Auditor-General Report No.42 of 2023–24 *Interim Report on Key Financial Controls of Major Entities*, ANAO, Canberra, 2024, section 3.23.

18 Royal Commission into the Robodebt Scheme, *Report, Royal Commission into the Robodebt Scheme*, 7 July 2023, p. 627, section 8, Conclusion, and p. 461, section 5.7 Possible Privacy Breaches.

1.17 To form a conclusion against the objective, the ANAO adopted the following two high-level audit criteria.

- Has Services Australia developed appropriate arrangements to manage the privacy of client information consistent with the *Privacy Act 1988* and other legislative requirements?
- Has Services Australia effectively implemented arrangements to manage the privacy of client information?

1.18 The audit scope focussed on whether Services Australia's frameworks and practices comply with the requirements and intent of the Privacy Act, including the APP Code between 2022–23 to 2024–25.

1.19 An assessment of the effectiveness of the OAIC as the national regulator for privacy was outside the scope of this audit. The audit did not consider the management of employees' personal information.

Audit methodology

1.20 The audit methodology included:

- reviewing Services Australia's records and data;
- meeting with officers from Services Australia, the OAIC, the Attorney-General's Department, the Australian Taxation Office, and the Department of Social Services; and
- site visits to Services Australia's service centres in Woden (ACT) and Tweed Heads (NSW).

1.21 Australian Government entities largely give the ANAO electronic access to records through cooperation, in a form useful for audit purposes.

- Services Australia advised the ANAO in January 2025 that it could not voluntarily provide access to certain record-keeping systems requested by the ANAO due to concerns about its obligations under protected information provisions in legislation, including the *Health Insurance Act 1973* and the *Migration Act 1958*. Services Australia advised that it could not be certain, in providing information access through electronic means, that all legal secrecy provisions could be maintained. The ANAO and Services Australia agreed that ANAO access to those systems would occur on Services Australia premises pursuant to the access provisions of section 33 of the *Auditor-General Act 1997*.
- The OAIC advised the ANAO that it could not voluntarily provide certain information requested by the ANAO due to concerns about its obligations under section 29 of the *Australian Information Commissioner Act 2010*. On 21 March 2025 the Auditor-General issued the Australian Information Commissioner with a notice to provide information and produce documents pursuant to section 32 of the *Auditor-General Act 1997*. Under this notice, the Australian Information Commissioner provided the requested information and documents.

1.22 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of approximately \$622,108.

1.23 The team members for this audit were Jason Millward, Carina Moeller, Ewan McPherson, Tatenda Zembe and Nathan Callaway.

2. Arrangements to manage privacy

Areas examined

This chapter examines whether Services Australia has developed appropriate arrangements to manage the privacy of client information consistent with the *Privacy Act 1988* (the Privacy Act), the Privacy (Australian Government Agencies — Governance) APP Code 2017 (the APP Code) and other legislative requirements.

Conclusion

Services Australia has developed partly appropriate arrangements to manage the privacy of client information. It has largely appropriate policies in place to meet the requirements of the Privacy Act, however, there are gaps in arrangements to manage privacy risks at the enterprise level. It did not document a rationale or seek legal advice when it decided to no longer undertake data matching under the *Data-matching Program (Assistance and Tax) Act 1990*.

Areas for improvement

The ANAO made two recommendations to Services Australia aimed at: improving privacy risk management; and publishing data-matching protocols. There are three recommendations to other entities to: improve notification to Services Australia of third-party data breaches involving government identifiers; review data-matching arrangements; and enhancing the transparency of Australian Government entities' management of privacy.

The ANAO also suggested that Services Australia could: engage clients to review its privacy policy and notices; link its operational blueprints to privacy legislation and guidelines; and publish more information about its management of privacy.

2.1 The APP Code requires entities to implement governance arrangements 'to move towards a best practice approach to privacy governance to help build a consistent, high standard of personal information management across all Australian Government agencies'.¹⁹

Has Services Australia established appropriate governance and oversight arrangements for managing the privacy of client information?

Services Australia has established largely appropriate governance and oversight arrangements. To meet the requirements established in the APP Code, Services Australia has a Privacy Champion and two Privacy Officers. It has also established a Privacy Contact Officer Network to support the management of the privacy of client information. Reporting on privacy matters is provided to Services Australia's Security Committee. The Privacy and Personal Information and Release branch assists with processing privacy matters. Services Australia's privacy management plans include performance measures for the self-assessment of privacy-related activities and have been reviewed annually. Services Australia has a high-risk privacy profile. It

¹⁹ Office of the Australian Information Commissioner (OAIC), Privacy (Australian Government Agencies — Governance) APP Code 2017, OAIC, Canberra, 26 October 2017, available from <https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes/privacy-australian-government-agencies-governance-app-code-2017> [accessed 22 January 2025].

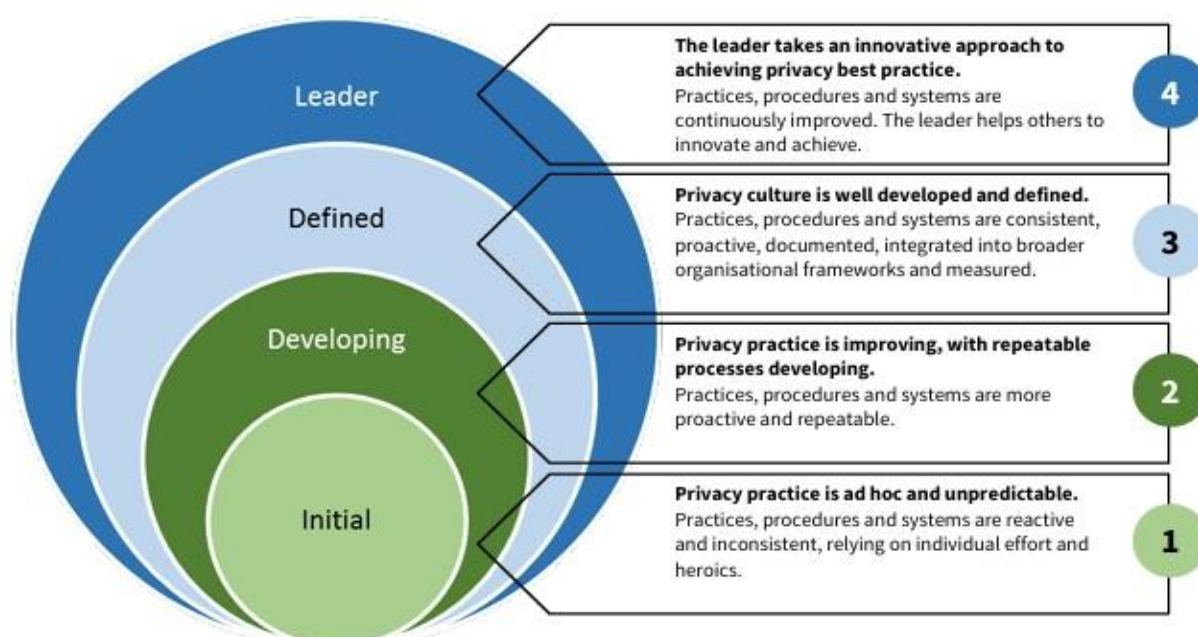
has identified that it needs to mature its arrangements commensurate with this risk profile, with it not meeting 12 of 21 target maturity ratings for 2024–25.

Privacy management plans

2.2 Section 9 of the APP code requires agencies to have a privacy management plan (PMP), and to measure and document performance against the PMP at least annually. The PMP is required to identify 'specific, measurable privacy goals and targets', and set out how an agency will meet its compliance obligations under Australian Privacy Principle (APP) 1.2.

2.3 The Office of the Australian Information Commissioner (OAIC) provides guidance for developing PMPs, including a framework against which entities can assess their privacy maturity across a set of criteria.²⁰ Figure 2.1 describes the maturity levels from the OAIC's Privacy Program Maturity Assessment Framework (Maturity Framework).

Figure 2.1: Privacy Program Maturity Assessment Framework maturity levels



Source: OAIC, *Interactive PMP Explained*, July 2018, p. 25.

2.4 Services Australia developed a PMP each year as required by the APP Code. PMPs were informed by OAIC guidance. In PMPs, Services Australia: assesses the current state of its privacy practices; sets privacy goals and targets; and sets out plans to measure its performance regarding the compliance obligations under the Privacy Act. The 2025–26 PMP outlines that '[p]rotecting privacy is part of the agency's core business and promotes trust and confidence in the agency to deliver government services to all Australians'. It also states that it:

20 OAIC, *Privacy management plan template*, May 2016, and *Interactive PMP Explained*, July 2018, available from <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/government-agencies/australian-government-agencies-privacy-code/interactive-privacy-management-plan> [accessed 22 January 2025].

[A]dvances Services Australia's 2030 Vision by strengthening our commitment to delivering simple, helpful, respectful and transparent services through clearly defined, measurable privacy goals that enhance customer trust and service excellence.

2.5 Services Australia uses the OAIC's template for PMPs. This PMP template is designed to support entities to assess their overall privacy risk maturity profile. Entities are to measure their privacy maturity across five elements: governance and culture; privacy strategy; privacy processes; risk and assurance; and data breach responses. To measure across these five elements, entities assess maturity across 21 'attributes'.²¹

2.6 Services Australia annually self-assesses its prior-year maturity (see Figure 2.1) against the 21 attributes. It uses these assessments to inform subsequent targets and to define activities to be used to achieve PMP outcomes. Appendix 3 shows Services Australia's self-assessment against each of the 21 attributes in PMPs developed between 2022–23 and 2025–26.

- Against its targets for 2021–22, Services Australia did not meet target maturity ratings for 10 out of 21 attributes.
- Against its 2022–23 targets, it did not meet target maturity for seven of 21 attributes.
- Against its 2023–24 targets, it did not meet target maturity for 20 of 21 attributes.
- Against its 2024–25 targets, it did not meet target maturity for 12 of 21 attributes.

2.7 As defined in its 2025–26 PMP, Services Australia is aiming to improve its maturity to the rating of 'leader' across 13 attributes, sustaining its maturity of 'defined' across five attributes, and sustaining its maturity of 'leader' for three attributes. The decline in target completion from 2021–22 has reflected a change in target maturity levels and changes to self-assessment.

2.8 As Services Australia has noted in its 2025–26 PMP, it has a high-risk privacy profile due to it providing complex public services and handling a significant amount of personal information. Services Australia is aiming for higher levels of privacy maturity so that it has arrangements which are commensurate with this risk profile.

2.9 The attributes in the PMP are taken from those provided in the OAIC template. Services Australia's uses these OAIC-provided attributes and adapts them to its own operational context, such as in the 2025–26 PMP where the OAIC-provided attribute of 'Privacy Values' is discussed by with specific reference to its internally-developed operational privacy policy.

2.10 Services Australia is required by subsection 9(3) of the APP Code to measure performance against the PMP at least annually. In accordance with this requirement, quarterly reporting of PMP activities has been provided to relevant executive officers within Services Australia and the Security Committee.

Privacy Officers and Privacy Champion

2.11 The APP Code requires an entity to have:

21 Attributes are groups of specific activities or functions the entity undertakes to assess and manage its overall risk maturity profile in relation to privacy.

OAIC, *Privacy management plan template*, May 2016, pp. 5–24, available from

https://www.oaic.gov.au/data/assets/pdf_file/0023/250439/OAIC-Privacy-Management-Plan-FY-24-25.pdf

[accessed 16 September 2025].

- a Privacy Officer to be the ‘primary point of contact for advice on privacy matters’ (section 10); and
- a Privacy Champion who is a senior official in the entity (section 11).

2.12 Services Australia has two Privacy Officers (General Counsel, Privacy and Personal Information Release branch and General Counsel, Digital Delivery and Privacy Legal branch) and a Privacy Champion (the Chief Counsel also has the role of Privacy Champion) whose roles are defined by those functions required by sections 10 and 11 of the APP Code.

2.13 The Privacy Officers are responsible for the management of privacy complaints and enquiries, maintaining a record of personal information holdings in the entity, overseeing the conduct of privacy impact assessments (chapter 3, from paragraph 3.19), and maintaining a register of these assessments.

2.14 The Privacy Champion promotes a positive privacy culture and privacy values, provides leadership on privacy matters, reviews and approves the PMPs, and advises and reports to Service Australia’s executive bodies on privacy issues.

2.15 In February 2023, Services Australia established the Privacy Contact Officer Network (PCON) to share information about privacy requirements and initiatives throughout the agency, and to ‘ensure the agency’s compliance with the Australia Privacy Principles’ (see case study 1).

Case study 1. Privacy Contact Officer Network (PCON)

Services Australia established a pilot PCON in February 2023 to enhance privacy awareness across the agency, and to consolidate ‘privacy management practices throughout the agency by capitalising on shared skills, knowledge, and experience’. As of May 2025, PCON had 88 contact officers. Contact officers are Executive Level (EL) 1 or EL2 employees and are provided with additional education on Services Australia’s privacy processes, governance arrangements, and the legal obligations related to privacy.

PCON acts as a community of practice, meeting monthly with the Privacy Officers and the Privacy Champion. Key activities include:

- raising and escalating any significant or systemic issues noted by officers, or management, to the Privacy team and other PCON members;
- supporting the Privacy team in raising awareness on privacy matters across the agency;
- reviewing the efficacy, appropriateness, and design of privacy processes used by staff to drive improvement;
- analysis of privacy incidents and identification of trends in incidents across teams, branches, and the agency;
- promoting and maintaining communication between operational and executive staff on privacy incidents and risks; and
- assisting in the remediation of substantiated privacy incidents and socialising any key learning amongst Services Australia staff.

A 2023 evaluation of the PCON pilot found that it had ‘improved privacy awareness in the agency’ and had enhanced the capability of staff in managing privacy incidents and risks.

Does Services Australia appropriately assess risks to the privacy of client information under its enterprise risk management framework?

Services Australia's enterprise-level Risk Management Policy and Framework categorises privacy as a 'specialist risk'. It does not have a privacy risk management plan or privacy specific enterprise risk or risk tolerance statement. Privacy related risks are incorporated in the group risk management plans of the seven service groups. There has been an increase in the volume of data breaches in Services Australia, largely caused by malicious actors. Third parties are not required to notify Services Australia following a data breach involving government identifiers, creating a risk to the timeliness of assessments of these breaches. Services Australia has not developed a technology security risk management plan as required by PSPF Direction 002-2024.

2.16 Section 16 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) requires entities to establish and maintain appropriate systems and internal controls for the oversight and management of risk.

Enterprise risk management

2.17 Services Australia's Risk Management Policy and Framework (RMPF) is 'the set of components and arrangements that articulate the direction and approach for managing risk in the agency'. The October 2024 RMPF is aligned with the requirements of the Commonwealth Risk Management Policy and outlines the hierarchy of risk management arrangements and roles and responsibilities. As of October 2025, Services Australia has 10 enterprise risks, each led by a deputy Chief Executive Officer (CEO) in their role as risk stewards.²²

2.18 None of the 10 enterprise risks explicitly refer to privacy. Enterprise risks 8 and 9 are related to privacy as these refer to risks to data, which in Services Australia is largely personal information.

Data: We fail to ensure the appropriate governance, curation, and use of data [enterprise risk 8].

Cybersecurity: We fail to detect and protect our systems and data holdings from internal or external malicious or unintentional activity [enterprise risk 9].

2.19 While Services Australia has not set a specific risk appetite statement or risk tolerances for privacy, its risk tolerance for privacy is referenced under the following themes from its RMPF: 'security information and systems' (low tolerance); and 'fraud and integrity' (medium tolerance, although low tolerance for unethical or illegal conduct).

Group risk management plans

2.20 Rather than having a single enterprise-level or agency-wide risk management plan, Services Australia's seven service groups each identify group risks that could impact the delivery of group objectives and align these risks to the 10 enterprise risks. Deputy CEOs are responsible for managing enterprise risks through group risk plans, which inform the development of a 'quarterly Enterprise Risk Profile' for Executive Committee discussion and endorsement'.

²² These enterprise risks are also outlined in Services Australia's 2025–26 corporate plan. Services Australia, *Corporate Plan 2025–26*, Services Australia, Canberra, 2025, p. 18, available from <https://www.servicesaustralia.gov.au/sites/default/files/2025-08/12637-2507-corporate-plan-25-26.pdf> [accessed 10 October 2025].

2.21 Group risk management plans (GRMPs) are reviewed and approved by the relevant deputy CEO and individual group risks are administered by group risk owners.²³ The GRMPs contain ‘aggregated risk information for the group’ and do not assess operational risks, which are ‘day-to-day risks [that] all staff are expected to identify, control and escalate’. They include a risk register, a risk rating summary, controls, and the risk decision by the risk owner, including notes to accept where a risk is outside of tolerance.

2.22 ANAO analysis of GRMPs for the first quarter of 2024–25 found that privacy-relevant risks were incorporated into the GRMPs of the seven service groups, and aligned primarily to enterprise risks 8 and enterprise risk 9 (see paragraph 2.18).

2.23 In quarter 1, 2024–25, four service groups covered privacy risks under group risks mapped to enterprise risk 8: Data, one group under enterprise risk 9: Cyber Security, and one group under both 8: Data and 9: Cyber Security, and one group under enterprise risk 1: Future Readiness. For example, the Corporate Enabling Group had the following privacy relevant group risk linked to enterprise risk 8: Data:

The workforce and systems do not protect sensitive personal, personnel, financial and government, data and information (and customer data where the group is responsible).

2.24 Services Australia has developed the Agency Control Library (ACL) to document the suite of 252 controls available to mitigate the range of group risks.²⁴ ANAO analysis of the quarter 1, 2024–25 GRMPs identified 11 privacy-specific ACL controls related to privacy governance and policies, privacy education and training, information release and exchange, scams and identity theft. Privacy-related ACL controls targeted the specialist risks of fraud and corruption, cyber and data security.

2.25 The GRMPs map ACL controls to risk causes and consequences. Controls to mitigate privacy risks and the risk causes and consequences are aligned. For example, the quarter 1, 2024–25 GRMP of the Corporate Enabling Group contains the privacy-relevant risk cause:

Inappropriate handling (collection /storage / transmission / disposal) of sensitive data and information, including personal and protected information.

2.26 Controls to mitigate this risk include the operational privacy policy; information security policy and procedures; the protective security plan 2023–25; protective security incident management; and security classifications and dissemination limiting markers.

Specialist risks

2.27 Services Australia has ‘specialist’ risk areas to ‘provide agency-wide direction on risks’ and ‘report independently through relevant committees’. In the October 2024 RMPF, there were 11 specialist risk areas, including for legal, financial, fraud, security, cyber security and privacy. While the RMPF does not define the term ‘specialist risk’, it states that:

23 As of June 2025, Services Australia is structured around seven service groups: Strategy and Performance; Service Delivery Excellence; Program Design; Customer Service Delivery; Payments and Integrity; Corporate Enabling; and Technology and Digital Programmes.

24 Services Australia’s RMPF defines a control as ‘Any process, policy, device, practice or other actions that is put in place to regulate or modify the likelihood or consequence of a risk. They can be preventative, detective or corrective in nature’.

- Under the direction of their Deputy CEOs, specialist risk areas ... assist to strengthen, integrate and support specialist risks, providing direction to agency officials on the management of their risk discipline in line with relevant Commonwealth legislation and policies.
- These areas monitor and report on the impact of their risk discipline on the agency to their line management and relevant enterprise governance committees.

2.28 Services Australia has risk management plans for the specialist risks of fraud and corruption, and security. These incorporate privacy risks.

- The Fraud and Corruption Control Plan 2025–2026 explains Services Australia’s approach to managing privacy and related legal obligations and summarises strategic alignment with privacy-related strategies and plans.
- The Protective Security Plan 2023–25 explains governance arrangements for privacy and related legal obligations and lists security requirements and actions relevant to privacy.

2.29 Services Australia does not have a separate privacy risk management plan. Paragraph 2.32 outlines the benefits that such a plan could provide.

Privacy management plan — risk identification and assessment

2.30 Services Australia self-assessed its performance against the attribute of ‘privacy risk identification and assessment’ in its 2024–25 PMP as ‘defined’ (see paragraph 2.3), meaning that ‘Strong, clear and consistent processes exist for identifying and assessing privacy risks’ and that privacy risks have been ‘integrated into agency’s wider risk management framework’.

2.31 In this self-assessment, Services Australia outlined that it operates a ‘three lines of defence’ model with ‘strong privacy officer involvement’ — these measures are defined as:

First line — operational privacy risks are identified and recorded in risk register and control activities are documented.

Second line — the Privacy Officer collaborates with information security, data governance and risk functions to provide oversight of privacy risk management.

Third line — internal audit (or independent assessors) conduct regular privacy-related assurance activities.

2.32 Despite being categorised as a ‘specialist’ risk, Services Australia does not have an enterprise-wide risk management plan for privacy (a privacy risk management plan). A privacy risk management plan could:

- underpin the first line of defence described above;
- complement the annual review and development of PMPs;
- assist with the identification, assessment and management of privacy risks across the seven service groups;
- provide an enterprise-wide view on privacy risk tolerances at a more specific level; and
- assist to better manage the potential harm to individuals resulting from privacy breaches.

2.33 Establishing these risk management arrangements at the enterprise-level for privacy would better reflect that Services Australia has a high-risk profile for privacy.

Recommendation no. 1

2.34 Services Australia improve the identification, assessment and management of privacy risks by implementing an enterprise-wide privacy risk management plan.

Services Australia response: *Agreed in principle.*

2.35 *The Agency agrees in principle with this recommendation and will explore opportunities to improve the identification, assessment and management of privacy risk. Effective management of privacy risk is critically important to the Agency as part of our commitment to building public trust.*

2.36 *The Agency's risk management policy and framework establishes that all risks, including privacy risks, are managed within group risk management plans that are overseen by deputy CEOs. This means that risks are assessed, accepted, treated, monitored and reported alongside other risks using a consistent methodology. This approach also ensures accountability for acceptance, assessment, treatment and monitoring of risk resides within the operational areas best placed to manage those risks.*

2.37 *The Agency's Executive Committee provides oversight and guidance for each of the Agency's 10 enterprise risks which cover elements of privacy risk.*

2.38 *The recommendation currently prescribes only one solution to improving the identification, assessment and management of privacy risks, through the introduction of a standalone enterprise-wide risk management plan.*

2.39 *The Agency will address the intent of the recommendation through a targeted and integrated approach in alignment with the current risk management policy and framework. This will include:*

- *improving how privacy risks are embedded into group risk management plans;*
- *stronger emphasis and integration of privacy risks into the Agency's enterprise risk framework;*
- *enhancing the reporting and visibility of privacy risk trends to the Security and Audit and Risk Committees; and*
- *aligning privacy risk oversight with existing documents, such as the Privacy Management Plan.*

Reporting and review

2.40 Services Australia's Executive Committee, chaired by the CEO, receives quarterly risk reports on enterprise risks. Reports focus on enterprise-risks that exceed levels of risk tolerance (see from paragraph 2.118 for reporting and monitoring arrangements).

2.41 The Chief Counsel provides updates to Services Australia's audit and risk committee on privacy matters, such as notifiable data breaches.

2.42 Services Australia advised the ANAO on 29 January 2025 that:

The Chief Operating Officer gives a weekly operational briefing on [Notifiable Data Breaches] and privacy incidents to the CEO and Agency Executive through Executive Stand-Up. Specific incidents

are escalated for visibility of key senior executives, in accordance with the Privacy Incident and Data Breach Response plan.

Management of specific privacy risks

Privacy risks arising from technology risks

2.43 Vulnerabilities in information management and computer systems present interrelated risks to the privacy of individuals and fraud and corruption and may be exploited for malicious purposes which could impact individuals as well as entities. The Protective Security Policy Framework (PSPF) Direction 002-2024 requires entities ‘to identify and actively manage the risks associated with vulnerable technologies they manage, including those they manage for other entities’.²⁵

2.44 Services Australia relies on ‘multiple ageing legacy ICT systems to deliver services and payment’, which creates risks to privacy. PSPF Direction 002-2024 urges Australian Government entities to ‘proactively seek out vulnerabilities that may be present on Australian Government networks’.²⁶ The number of notifiable data breaches (NDBs) (see paragraph 3.50) attributed to malicious or criminal attacks on Services Australia systems or client access credentials has increased from three in 2019–20 to 82 in 2024–25. Services Australia advised the ANAO in November 2025 that these NDBs primarily involve incidents where customers have inadvertently provided personal information and myGov sign-in credentials to parties impersonating the agency.

2.45 Services Australia’s Protective Security Plan 2023–25 outlines the protective security environment, including high level risks, governance and responsibilities. Services Australia had not developed a technology security risk management plan²⁷ by 30 June 2025, as required by PSPF Direction 002-2024. Services Australia produced a technology asset stocktake, as required by that direction. It advised the ANAO on 6 November 2025 that it planned to provide a draft technology security risk management plan for approval to its Security Committee in December 2025.

Privacy risks arising from third-party data breaches

2.46 APP 9 covers the adoption, use and disclosure of ‘government related identifiers’, such as Medicare numbers and Centrelink reference numbers, by third-party organisations.

2.47 In 2022, Services Australia developed a third-party compromise response plan (TPCRP) in response to data breaches (Optus²⁸, Medibank²⁹, and Medlab³⁰) that involved government-related identifiers. The TPCR describes Services Australia’s approach to monitoring, assessing, and

25 Department of Home Affairs, *PSPF Direction 002-2024, Technology Asset Stocktake*, 5 July 2024, available from <https://www.protectivesecurity.gov.au/protective-security-directions-under-pspf> [accessed 1 April 2025].

26 *ibid.*

27 A technology security risk management plan is to be developed for all internet-facing systems or services, as part of the entity’s overall security plan.

28 OAIC, *OAIC opens investigation into Optus over data breach*, 11 October 2022, available from <https://www.oaic.gov.au/news/media-centre/oaic-opens-investigation-into-optus-over-data-breach> [accessed 7 October 2025].

29 OAIC, *OAIC opens investigation into Medibank over data breach*, 1 December 2022, available from <https://www.oaic.gov.au/news/media-centre/oaic-opens-investigation-into-medibank-over-data-breach> [accessed 7 October 2025].

30 OAIC, *OAIC opens investigation into Medlab over data breach*, 5 December 2022, available from <https://www.oaic.gov.au/news/media-centre/oaic-opens-investigation-into-medlab-over-data-breach> [accessed 7 October 2025].

responding to third-party compromises to prevent and mitigate fraud against the agency and its clients, resulting from the compromise of sensitive information held by an external third party. It outlines the roles and responsibilities for managing the response to a third-party compromise, including determining what credentials have been exposed and the information impacted. The TPCRP was updated on 15 August 2024. It is not identified as a control in the Agency Control Library.

2.48 Two groups within Services Australia (the Technology and Digital Program Group and the Payments Integrity Group) include third-party data breaches as causes of group risks in their GRMPs. Services Australia advised the ANAO on 4 April 2025 that it becomes aware of third-party compromises through the OAIC and the Australian Cyber Security Centre, media monitoring, or advice from affected individuals.

2.49 The TPCRP states that Services Australia ‘does not have legislated authority to compel third parties to share information about a data breach or compromise event where agency issued credentials are impacted’ and instead ‘seeks and obtains information from third parties in compliance with section 86E of the *Crimes Act 1914* (Cth)’, and under guidance from the *Crimes Legislation Amendments (Powers, Offences and Other Measures) Act 2018* (Cth), which states that ‘a release of information for ‘integrity purposes’ is permissible under Australian Privacy Principle 6 in the *Privacy Act 1988*’.

2.50 Requests for voluntary provision of information from third parties occur when there has been exposure of ‘agency issued credentials’ such as Medicare details or Centrelink customer numbers and ‘personally identifiable information’ that could enable a malicious actor to impersonate a genuine customer, make false claims or redirect payments.

2.51 In contrast, third-party compromises relating to My Health Records must be notified to the OAIC and the system operator, which is the Australian Digital Health Agency, as outlined in the OAIC’s *Guide to mandatory data breach notification in the My Health Record system*.³¹ The OAIC’s data breach action plan for health service providers states ‘you may wish to contact Services Australia [link to external site] to discuss options for protecting customers’ Medicare, Centrelink or Child Support records’.³²

2.52 With multiple notifiable data breaches relating to ‘government related identifiers’ issued by Services Australia since 2022, there is a risk that the personal information of Services Australia’s clients could be further compromised before Services Australia is notified and undertakes a risk assessment. Services Australia does not have formalised arrangements with external entities or parties to facilitate the notification of such breaches. This creates a risk that Services Australia may not be made aware of such breaches in a timely manner, meaning that it may not be able to respond in a timely manner to personal information compromises.

31 OAIC, *Guide to mandatory data breach notification in the My Health Record system*, 10 October 2023, available from <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/health-service-providers/my-health-record/guide-to-mandatory-data-breach-notification-in-the-my-health-record-system> [accessed 15 April 2025].

32 OAIC, *Data breach action plan for health service providers*, 11 February 2020, available from <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/health-service-providers/data-breach-action-plan-for-health-service-providers> [accessed 16 April 2025].

Recommendation no. 2

2.53 The Australian Government consider implementing arrangements to support Services Australia being provided with timely notification of third-party data breaches involving government-related identifiers such as Medicare numbers and Centrelink reference numbers.

Attorney-General's Department response: *Agreed.*

2.54 *The Attorney-General's Department (the department) notes the importance of ensuring that government-related identifiers are appropriately protected in accordance with APP 9, and of taking timely steps to mitigate the risk to Australians when those identifiers are potentially disclosed through a data breach. The department is developing a second tranche of privacy reforms for consideration by the Government, including consideration of reforms to the Notifiable Data Breaches scheme. Alongside that work, the department will give consideration to possible arrangements to facilitate timely notification to Services Australia when a regulated entity has experienced a data breach involving government-related identifiers. Similar to the approach in the My Health Record system, the most appropriate arrangements may be through OAIC guidance, rather than legislative amendment. The department will consult the OAIC in undertaking this work.*

Office of the Australian Information Commissioner response: *Agreed.*

2.55 *The OAIC would support a requirement for entities to notify Services Australia directly following a relevant data breach, however mandating such a requirement would be a matter for Government.*

2.56 Services Australia supports clients affected by third-party data breaches by providing advice regarding the protection of agency-issued credentials.³³ The TPCRP outlines the following.

- The responsibility to notify individuals affected by a breach lies with the third party that incurred the breach, and notification should be done in accordance with OAIC guidelines and the Privacy Act. Services Australia considers communicating with impacted individuals on a case-by-case basis, depending on additional risks due to vulnerabilities.
- Services Australia's response to a third-party data breach can include: applying protective measures to impacted client accounts and monitoring of accounts for suspicious or fraudulent activities; requesting password resets for, and providing email notifications in, MyGov accounts; public messaging on Services Australia's website; and undertaking data-matching activities for certain types of breaches (see paragraph 2.58).

2.57 Services Australia undertakes 'data matching activities for third-party organisation data breaches' to assess and manage the risk of client identity theft and fraud. This type of data matching involves comparing Services Australia's Medicare and Centrelink client records with information from a third-party organisation to identify affected clients.

2.58 As of June 2025, Services Australia has published 14 data-matching program protocols for third-party data breaches (developed between 2022 and February 2024) for data-matching

33 Services Australia, *Protecting your personal information after a data breach*, available from <https://www.servicesaustralia.gov.au/protecting-your-personal-information-after-data-breach?context=60271> [accessed 6 June 2025].

activities that involve over 5,000 individuals. The protocols are published on Services Australia's website³⁴ and in the Australian Government Gazettes³⁵ as recommended in the OAIC's voluntary *Guidelines on data matching in Australian Government administration* (voluntary data matching guidelines) (refer to paragraph 2.93).

Has Services Australia developed appropriate policies to manage the privacy of client information consistent with the *Privacy Act 1988*?

Services Australia publishes a privacy policy and privacy notices that largely comply with the requirements of Australian Privacy Principles 1 and 5. Services Australia does not regularly review its public privacy policy and privacy notices. Review of these products would benefit from client input. Services Australia maintains an internal operational privacy policy and 'operational blueprints' that provide guidance to staff. The operational privacy policy was reviewed in 2023–24. Services Australia has policies to support individuals access their own information, and to support appropriate data destruction.

Public privacy policy and privacy notices

2.59 The Privacy Act sets out the requirements for a privacy policy under APP 1 and privacy notices under APP 5. The *Australian Privacy Principles Guidelines* provide entities with further guidance.³⁶

- Under APP 1, an entity must have a clearly expressed and up-to-date policy about the management of personal information by the entity. It must be readily available.
- Under APP 5, an entity must take steps to notify individuals about the collection of their personal information.

2.60 Services Australia publishes a privacy policy³⁷ on its website, which links to other privacy content including 19 program-specific privacy notices and other documents, such as:

- Child Care Subsidy privacy notice for customers;
- Child Care Personnel and Provider Digital Access (PRODA) privacy notice;
- COVID-19 and influenza (flu) immunisation history statement privacy notice;
- National Redress Scheme privacy notice;
- Centrelink data-matching activities (see from paragraph 2.79);
- Data-matching activities for third-party organisation data breaches (see from paragraph 2.46); and

34 Services Australia, *Data matching activities for third party organisation data breaches*, 2 September 2024, available from <https://www.servicesaustralia.gov.au/data-matching-activities-for-third-party-organisation-data-breaches?context=22> [accessed 05 May 2025].

35 Federal Register of Legislation, *Australian Government Gazettes*, available from [https://www.legislation.gov.au/search/collection\(Gazette\)/status\(InForce\)](https://www.legislation.gov.au/search/collection(Gazette)/status(InForce)) [accessed 12 May 2025].

36 OAIC, *Australian Privacy Principles Guidelines*, December 2022, available from <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines> [accessed 22 January 2025].

37 Services Australia, *Privacy Policy*, available from <https://www.servicesaustralia.gov.au/privacy-policy?context=22> [accessed 12 May 2025].

- CCTV privacy notice.

2.61 Services Australia also includes privacy notices:

- within Services Australia's client forms used for payment applications³⁸;
- on the myGov website; and
- in scripts used by officers during inbound and outbound calls.

2.62 Services Australia's privacy policy satisfies the requirements of APP 1 and privacy notices largely meet the requirements of APP 5, with the exception that not all data-matching programs have been published (see paragraphs 2.96 and 2.97). Privacy notices are updated by individual policy and program owners. Services Australia does not coordinate the review of its privacy notices and privacy policy at an enterprise level. Services Australia does not test the format or content of privacy information with clients, as recommended by the OAIC's *Guide to developing an APP privacy policy*.

Opportunity for improvement

2.63 Services Australia could engage clients to inform regular reviews of its privacy policy and privacy notices to ensure that information is presented in formats that meet client needs.

Operational privacy policy and operational blueprints

2.64 Services Australia maintains an internal operational privacy policy and privacy-related operational blueprints that provide specific guidance to staff.

2.65 The operational privacy policy was first approved in 2018. It was updated in December 2024, with the next review due in December 2025. The purpose of the policy is 'to ensure staff manage personal information of customers and staff in accordance with the agency's obligations under the Privacy Act, and the Privacy Code [the APP Code]'. The policy sets out that all staff are responsible for:

- understanding the obligations that apply to them, including how to manage personal information and potential consequences from breaches of the Privacy Act;
- promoting privacy awareness and compliance, including awareness of the Privacy Officers and Privacy Champion;
- completing mandatory privacy training, reporting and managing a privacy incident, providing guidance on privacy management processes such as privacy threshold and impact assessments; and
- understanding and adhering to this policy.

2.66 As of June 2025, Services Australia has over 5,000 operational blueprints that outline procedures for staff performing various functions. The ANAO identified 39 operational blueprints that provide privacy guidance. The ANAO assessed a sample of 28 operational blueprints (including 12 privacy specific) and found that these provide largely appropriate guidance to staff, with the

38 Services Australia, *Accessing our Services: Forms*, available from <https://www.servicesaustralia.gov.au/forms?context=64107> [accessed 28 August 2025].

exception that the privacy blueprints did not always include references to relevant legislation, OAIC guidance and Services Australia's privacy policies.

Opportunity for improvement

2.67 Services Australia could improve its privacy operational blueprints with the inclusion of references to privacy legislation, privacy policy and OAIC guidance.

Access to personal information

2.68 APP 6 requires that entities must not disclose personal information for a secondary purpose unless an individual has consented. APP 12 sets out requirements for entities to provide individuals with access to their own information.

2.69 Services Australia has policies and processes in place to manage client and third-party requests for information about clients, including requests by individuals, through freedom of information (FOI), by consent, public interest requests and by subpoena.³⁹

Individuals' requests for personal information

2.70 Individuals can access their personal information through myGov, by request to Services Australia or through a freedom of information (FOI) request. Individuals can also consent to third parties requesting their information from Services Australia on their behalf⁴⁰, including through the Customer Information Release Service.⁴¹ Consent requests are processed by a personal information release team who undertakes authorisation verifications in accordance with APP 6. In 2024–25, Services Australia received 45,056 requests for information by consent.

Freedom of information requests for personal information

2.71 Services Australia received 4,469 FOI requests for personal information in 2023–24, and 4,899 requests in 2024–25. In a submission to the Senate Standing Committee on Legal and Constitutional Affairs made in October 2025, Services Australia noted that approximately 95 per cent of all FOI requests it receives are for access to personal information.⁴² See Appendix 2 for discussion on how Services Australia reported these figures to the OAIC.

2.72 In processing these FOIs for personal information, Services Australia can release the information in full, in part, or refuse to release any information. Most FOI requests which Services

39 Services Australia, *Personal information releases*, available from <https://www.servicesaustralia.gov.au/personal-information-releases?context=22> [accessed 2 July 2025].

Services Australia, *Freedom of information*, <https://www.servicesaustralia.gov.au/freedom-information?context=22> [accessed 2 July 2025].

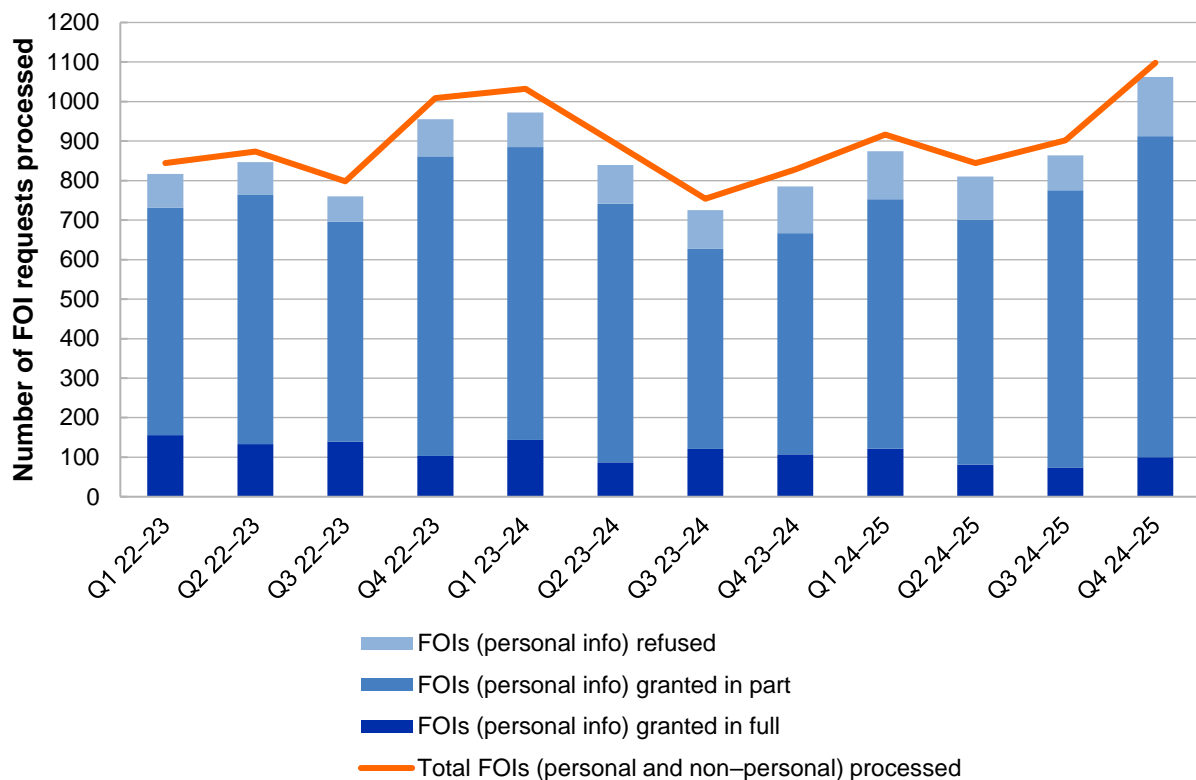
40 Services Australia, *Authority to release personal information — Personal injury, insurance, superannuation or other matter form (SI039)*, June 2024, available from <https://www.servicesaustralia.gov.au/si039> [accessed 2 July 2025].

41 Services Australia, *Customer Information Release service*, available from <https://www.servicesaustralia.gov.au/customer-information-release-service> [accessed 5 September 2025].

42 Services Australia, submission to the Senate Standing Committee on Legal and Constitutional Affairs, 'Freedom of Information Amendment Bill 2025, Services Australia's Submission', p. 3, October 2025, available from https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/FOI_Bill2025/Submissions [accessed 21 October 2025].

Australia receives are for the release of personal information — 94 per cent of all FOI requests in 2023–24, and 95 per cent in 2024–25 (see Figure 2.2).

Figure 2.2: Services Australia FOI request processing, 2022–23 to 2024–25



Source: ANAO analysis of Services Australia FOI request processing data, as reported to the OAIC.

Australian Government freedom of information statistics, 13 January 2025, available from

<https://www.oaic.gov.au/freedom-of-information/australian-government-freedom-of-information-statistics>.

Public interest requests for information and subpoenas

2.73 In some cases, requests for an individual's information may come from a third party who is not acting on behalf of an individual under their authorisation. Services Australia has processes in place to respond to requests to release information requested under public interest grounds and to respond to subpoenas.

2.74 The Social Security (Public Interest Certificate Guidelines) (DSS) Determination 2015 permits Services Australia to issue Public Interest Certificate ss to support the release of information to third parties under paragraph 208(1)(a) of the *Social Security (Administration) Act 1999*.⁴³ This provides for the release of information to police, coroners, state government agencies and other parties for relevant purposes, such as law enforcement, confirmation of housing and educational statuses,

⁴³ Under section 208 of the *Social Security (Administration) Act 1999*, information otherwise protected under sections 204 (Offence—unauthorised making a record of, disclosure of or use of protected information) and 207 (Protection of certain documents etc. from production to court etc.) can be disclosed for certain purposes. Services Australia undertakes disclosures by using Public Interest Certificates, where it documents the reason for release that may otherwise be protected in line with the guidelines as defined in section 209.

child protection matters, and for supporting or investigating the health and welfare of an individual (such as missing persons).

2.75 Services Australia received 23,241 public interest requests for information in 2024–25, and 22,289 in 2023–24. In 2024–25, the largest volume of requests (10,357) were made by police and other law enforcement agencies (for criminal matters and missing persons), followed by 7,753 from government agencies acting on child protection matters, and 2,474 medical related requests (including 1,819 from the Australian Health Practitioner Regulation Agency).

2.76 Services Australia was issued 7,014 subpoenas for personal information in 2024–25. Services Australia advised the ANAO on 19 March 2025 that its processes for managing subpoenas involves ensuring their legitimacy and authority through the courts, and that if Centrelink information has been requested that it is only released if relevant to section 207 of the *Social Security Act 1991*.

Data destruction and disposal

2.77 Services Australia has designated its records management team as responsible for the disposal of records with business areas as needed. To support these activities, and compliance with its obligations under APP 11 (security of personal information), Services Australia has developed four program-specific Records Authorities with the National Archives of Australia to govern the destruction and disposal of data used in support of programs.⁴⁴

2.78 The four Records Authorities operate alongside the Administrative Functions Disposal Authority (AFDA) to guide Services Australia on its obligations as to how and when records pertaining to its service delivery activities can be disposed of.⁴⁵ This includes for core service delivery functions, payment and service delivery management functions, specific Medicare functions, and specific Child Support functions.

Do Services Australia's data-matching activities comply with legislation and guidelines?

Services Australia no longer undertakes data matching under the *Data-matching Program (Assistance and Tax) Act 1990* and instead follows the voluntary guidelines on data matching in Australian Government administration. This approach reduces transparency and accountability to Parliament. There was no documented rationale or legal advice to underpin this change. Services Australia has not fully implemented Robodebt Royal Commission recommendations relating to data matching. Services Australia has published 13 of 32 data-matching protocols.

44 OAIC, *Chapter 11: Australian Privacy Principle 11 — Security of personal information*, OAIC, Canberra, 22 July 2019, <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information#destroying-or-de-identifying-personal-information> [accessed 16 June 2025].

45 See the National Archives of Australia's guidance, *ADFA Express Version 2 Functions*, available from <https://www.naa.gov.au/information-management/records-authorities/types-records-authorities/afda-express-version-2-functions> [accessed 23 June 2025].

2.79 Data matching ‘means the bringing together of at least two data sets that contain personal information, and that come from different sources, and the comparison of those data sets with the intention of producing a match’.⁴⁶

2.80 Entities that carry out data matching must comply with the Privacy Act. The OAIC sets out two frameworks for government data matching.

- Data matching involving tax file numbers (TFNs) to detect incorrect payments is governed by the *Data-matching Program (Assistance and Tax) Act 1990* (the DMP Act) and the Data-matching Program (Assistance and Tax) Rules 2021 (data matching rules)⁴⁷ — see from paragraph 2.83.
- Data matching for other purposes is done under the OAIC’s 2014 voluntary *Guidelines on data matching in Australian Government administration* (voluntary data-matching guidelines)⁴⁸ — see from paragraph 2.93.

2.81 Further requirements are set out in the Privacy (Tax File Number) Rule 2015, issued by the Privacy Commissioner under section 17 of the Privacy Act, which states that:

the *Data-matching Program (Assistance and Tax) Act 1990* provides for, and regulates, the matching of records between the Australian Taxation Office and assistance agencies using the TFN in part of the matching process.⁴⁹

2.82 Additional requirements for data matching involving Medicare and Pharmaceutical Benefits Scheme (PBS) data are set out in the *National Health Act 1953* and the National Health (Privacy) Rules 2025.⁵⁰

Data matching under the *Data-matching Program (Assistance and Tax) Act 1990*

2.83 The DMP Act prescribes how data matching of TFNs is to occur.

- Matching is undertaken by a matching agency (Services Australia) (section 4).

46 OAIC, *Guidelines on data matching in Australian Government administration*, 18 June 2014, available from <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/government-agencies/guidelines-on-data-matching-in-australian-government-administration> [accessed 14 April 2025].

47 Under the Administrative Arrangements Order dated 13 May 2025, the Minister for Social Services is responsible for the *Data-Matching Program (Assistance and Tax) Act 1990*. The Data-matching Program (Assistance and Tax) Rules 2021 were issued on 8 June 2021 and replaced the Data-Matching Program (Assistance and Tax) Act 1990 — Guidelines issued on 31 October 1994.

48 OAIC, *Guidelines on data matching in Australian Government administration*, 18 June 2014, available from <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/government-agencies/guidelines-on-data-matching-in-australian-government-administration> [accessed 14 April 2025].

49 OAIC, *The Privacy (Tax File Number) Rule 2015 and the protection of tax file number information*, available from <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/the-privacy-tax-file-number-rule-2015-and-the-protection-of-tax-file-number-information> [accessed 28 May 2025].

50 This audit did not examine data matching under these pieces of legislation. Data matching of Medicare data was assessed in Auditor-General Audit Report No.27 2013–14, *Integrity of Medicare Customer Data*, ANAO, 2014, available from <https://www.anao.gov.au/work/performance-audit/integrity-medicare-customer-data> [accessed 24 June 2025].

- It specifies application to the Australian Taxation Office (ATO) as well to ‘assistance agencies’ defined as the Education Department, the Social Services Department, the Veterans’ Affairs Department and Services Australia (subsection 3(1)).⁵¹
- There are to be no more than nine data matching cycles in a year (subsection 6(1)(2)).
- Requires entities to report annually to Parliament through the OAIC on the conduct of data matching activities (subsection 12(4)).
- Requires entities to report to Parliament through their responsible Minister every three years ‘including all the details relating to the data-matching program carried out during the period’ that are specified in the data matching rules (subsection 12(5)).

2.84 Services Australia reported on its DMP Act data matching in its annual report until 2015–16. In its 2016–17 Annual Report, Services Australia stated that it was no longer operating under the DMP Act⁵², and that it had commenced data matching under the OAIC voluntary *Guidelines on data-matching in Australian Government administration* (voluntary data-matching guidelines).

2.85 The voluntary data-matching guidelines ‘assist Australian Government agencies to use data matching as an administrative tool in a way that complies with the APPs and the Privacy Act, and is consistent with good privacy practice’. The voluntary data matching guidelines state that:

The Guidelines do not generally apply to data matching where Tax File Numbers are used. The *Data-matching Program (Assistance and Tax) Act 1990* (Cth) regulates the use of Tax File Numbers in comparing personal information held by the Australian Taxation Office and by certain ‘assistance agencies’.⁵³

2.86 Services Australia continues to undertake data matching involving TFNs for child support payments and income data, including for example, ‘near-real-time’ single touch payroll (STP) data, where:

The ATO conducts an identity matching exercise to determine the relevant STP records to send to the Agency. ATO does this by matching the personal information provided by the Agency with the records of the ATO. Personal information includes Centrelink Customer Reference Numbers (CRN) or Tax File Number (TFN) for Child Support customers. The ATO replies to the Agency by providing STP data reported by the employers, for mutual customers.⁵⁴

2.87 The Royal Commission into the Robodebt Scheme (Robodebt Royal Commission) provided insight into the data-matching activities undertaken by Services Australia, and provided recommendations relevant to the legal management of these activities. The Information Commissioner’s evidence to the Robodebt Royal Commission stated:

51 Prior to being renamed, Services Australia was the Department of Human Services. This report uses ‘Services Australia’ to refer to both it and the Department of Human Services.

52 Except for acting as the matching agency for the Department of Veterans’ Affairs.

53 Office of the Australian Information Commissioner, *Guidelines on data matching in Australian Government administration*, 18 June 2014, available from <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/government-agencies/guidelines-on-data-matching-in-australian-government-administration> [accessed 24 June 2025].

54 Services Australia, *Program Protocol Data matching between Australian Taxation Office and Services Australia (Centrelink and Child Support) Single Touch Payroll (STP), Phase 2*, January 2021, page 4, available from <https://www.servicesaustralia.gov.au/centrelink-data-matching-activities?context=22> [accessed 7 July 2025].

In 2019, the OAIC undertook targeted consultation to understand which agencies were undertaking statutory data matching. The OAIC found that only DVA continued to conduct statutory data matching activities under the Data-matching Act and the 1994 Guidelines. Services Australia, however, provide administrative and technical support to assist DVA to carry out its data matching programs.⁵⁵

2.88 Services Australia did not document a rationale or seek legal advice to support the change from using the DMP Act for data matching to using the voluntary data-matching guidelines. While this change allows more frequent data exchanges than the maximum nine cycles per year under the DMP Act, it has reduced transparency and accountability, with Services Australia no longer reporting to Parliament about data-matching activities required by the DMP Act. It is unclear how this change was reconciled with the Privacy (Tax File Number) Rule 2015 and OAIC guidance that data matching involving TFNs is regulated by the DMP Act.

2.89 The ANAO identified a document purported to be internal draft legal advice, relating to the use of TFNs for data matching, in the Robodebt Royal Commission document library.⁵⁶ While the document is not stored in Services Australia's record keeping system for legal advice, Services Australia confirmed that it provided this document to the Robodebt Royal Commission. Services Australia was unable to locate a record of final advice.

2.90 The Robodebt Royal Commission made two recommendations related to the exchange of data between Services Australia and the ATO and data matching programs.

- Recommendation 16.1 Legal advice on end-to-end data exchanges.
- Recommendation 16.2 Review and strengthen governance of data-matching programs.

2.91 The Australian Government accepted both recommendations and reported recommendation 16.1 as implemented and the implementation of 16.2 as ongoing as of November 2024.⁵⁷

2.92 The ANAO reviewed evidence of the implementation of these recommendations and found that neither the legal advice for recommendation 16.1 nor the review of governance for recommendation 16.2 contemplated the DMP Act. In July 2025, Services Australia advised the ANAO that it had instructed its legal advisor to also consider the DMP Act for implementation of the Robodebt recommendations; as at November 2025 this legal advice had not been finalised.

55 *Response to request for information - Angelene Falk, Australian Information Commissioner and Privacy Commissioner — Royal Commission into the Robodebt Scheme*, available from <https://robodebt.royalcommission.gov.au/publications/exhibit-4-6719-rbd999900010454-response-request-information-aic-royal-commission-16-january-2023> [accessed 15 May 2025].

56 Department of Human Services, *Legal Advice, [PLEXID 27436] Using Tax File Numbers (TFNs) for data matching, 30 April 2019*, watermarked 'DRAFT', published as *Exhibit 8456 - CTH.3063.0076.7603 - Draft Legal Advice - using TFN for data matching — 27436*, Robodebt Royal Commission, 5 April 2023, available from <https://robodebt.royalcommission.gov.au/publications/exhibit-8456-cth306300767603-draft-legal-advice-using-tfn-data-matching-27436> [accessed 16 October 2025].

57 Australian Government, *Robodebt Royal Commission Implementation update*, November 2024, available from <https://www.pmc.gov.au/resources/government-response-royal-commission-robodebt-scheme> [accessed 12 May 2025].

Voluntary guidelines on data matching in Australian Government administration

2.93 The OAIC's voluntary data-matching guidelines represent the OAIC's view of best practice, and require the following.

- The primary user agency of the data-matching program should prepare a data-matching program protocol before the commencement of the program.
- Each entity involved in a data-matching program should comply with the program protocol.
- The primary user agency should publish the program protocol on its website and should clearly indicate any amendments.
- Before commencing the program, the data-matching agency should — in consultation with the source entity or entities — develop a technical standards report to govern the conduct of the data-matching program.
- The primary user agency should publish a notice of the proposed data-matching program in the Australian Government Gazettes.
- The primary user agency should undertake an evaluation of the data-matching program in accordance with its original objectives.
- Agencies should enable the OAIC to review their data-matching activities and procedures.
- The recommended content of the data-matching program protocols are at Appendix A of the guidelines, and the content of the Technical Standards Report at Appendix B.

2.94 Services Australia's published information does not clearly articulate the framework under which its data matching, including that involving TFNs, is currently undertaken.

2.95 In June 2025, Services Australia's Centrelink data matching activities webpage informed:

In 1991, we began matching Tax File Numbers (TFNs). We did this under the *Data-matching Program (Assistance and Tax) Act 1990* ... We use these guidelines [OAIC voluntary Guidelines on data matching in Australian Government Administration] when we match data that doesn't involve matching Tax File Numbers (TFNs).⁵⁸

2.96 Services Australia has not published all program protocols for data matching, which is best privacy practice recommended in the OAIC voluntary data-matching guidelines. Services Australia advised the ANAO on 30 July 2025 that it has produced 32 data-matching program protocols between 1991 and 2024, of which 13 are published on its website. The 13 published protocols do not include information on program status (active, ended, or paused pending legal review as part of Services Australia's response to Robodebt Royal Commission recommendation 16.2).

2.97 Services Australia has given notice of 15 of the 32 data-matching programs in the Commonwealth Government Gazette. Seventeen protocols did not meet the requirement of the OAIC voluntary data-matching guidelines to take reasonable steps to notify individuals in accordance with APP 5. The gazetted notifications do not inform the public on the current status of the data-matching programs (active, ended, or paused).

58 Services Australia, *Centrelink data matching activities*, 29 April 2025, available from <https://www.servicesaustralia.gov.au/centrelink-data-matching-activities?context=22> [accessed 13 May 2025].

Recommendation no. 3

2.98 Services Australia publish all data-matching program protocols on its website, including dates of operation, and regularly review the currency of the information published, except where an exemption has been sought in accordance with the Office of the Australian Information Commissioner's voluntary data-matching guidelines.

Services Australia response: *Agreed.*

2.99 *The Agency agrees to publish data-matching program protocols on its website in accordance with the OAIC voluntary data-matching guidelines, ensuring that the information is up-to-date and specifies dates of operation, except where an exemption has been sought under Guideline 10.*

2.100 The ANAO assessed nine of the 13 data-matching program protocols (2016–2025) published on Services Australia's website. Six program protocols include TFNs and three do not.

- The protocols outline that Services Australia undertakes data matching in accordance, or complies, with the OAIC's voluntary data matching guidelines, which state that they do not generally apply to data matching involving TFNs.
- The nine published protocols assessed by the ANAO covered the required contents for data-matching program protocols recommended in the OAIC's voluntary data matching guidelines.

2.101 The data matching program protocol for Single Touch Payroll (STP) Phase 2 specifies that data matched to an individual is retained as national archives and refers to the National Archives of Australia General Disposal Authority 24 (GDA 24) as the source of authority for disposal. GDA 24 was revoked on 17 July 2019. Services Australia has not updated the protocol to clarify retention times or if it creates a permanent register or database for matched data.

2.102 Services Australia advised the ANAO on 30 July 2025 that it is aware that GDA 24 was revoked and is developing a data disposal policy for the STP program. Services Australia's agency-specific 2012 records authority for Payment and Service Delivery Management, not included in the protocol, sets out relevant general requirements for keeping or destroying records in the core areas of payment and service delivery.⁵⁹ There is a need for Services Australia to develop a new disposal authority to cover data matching.

2.103 The audit identified that Services Australia completed privacy impact assessments (PIAs) for data matching in the Centrelink and Medicare program (21 April 2021) and the Child Support Program (9 May 2022). The ANAO did not assess if Services Australia has undertaken PIAs for all data-matching activities.

⁵⁹ National Archives of Australia, *Records Authority 2011/00714998, Department of Human Services, Payment and Services Delivery Management*, December 2012, available from <https://www.naa.gov.au/sites/default/files/2019-12/agency-ra-2011-00714998.pdf> [accessed 4 September 2025].

Recommendation no. 4

2.104 The Australian Government review existing data-matching activities undertaken by Services Australia and other government entities to assess whether the current frameworks — the *Privacy Act 1988*, the *Data-matching Program (Assistance and Tax) Act 1990*, and the voluntary Guidelines on data matching in Australian Government administration — are appropriate for use with contemporary data-matching and information-sharing practices and provide sufficient transparency and accountability.

Attorney General's Department response: *Noted.*

2.105 *The Attorney-General's Department (the department) notes the importance of ensuring that the legal frameworks and processes governing data-matching activities are up to date and appropriate. From 2020 to 2022, the department undertook a comprehensive review of the Privacy Act 1988, including whether its approach to the sharing of personal information provides sufficient transparency and accountability. The department is currently developing a second tranche of privacy reform for consideration by the Government, following the passage of the Privacy and Other Legislation Amendment Act 2024.*

2.106 *While the Privacy Act regulates information sharing generally, the department does not have specific responsibility for data-matching activities, the Data-matching Program (Assistance and Tax) Act 1990 (DMP Act) or the voluntary Guidelines (which are developed by an independent regulator), and considers that the need for a review of this nature would be best determined by the Department of Social Services noting their responsibility for the DMP Act. The department also understands that the OAIC is currently reviewing the voluntary Guidelines. The department notes that any decision for the OAIC to increase its oversight or compliance activities in relation to data matching would have resourcing implications. We understand the OAIC currently prioritises its compliance activities through a risk-based and harm-focused approach, which the department generally considers to be appropriate.*

Office of the Australian Information Commissioner response: *Agreed.*

2.107 *A review of the voluntary Guidelines on data matching in Australian Government administration is underway.*

2.108 *Any review of the Privacy Act 1988 and the Data-matching Program (Assistance and Tax) Act 1990 would be a matter for Government.*

Department of Social Services response: *Agreed in principle.*

2.109 *The Department is ready to provide support to an independent review, should it go ahead.*

Has Services Australia implemented appropriate education and training arrangements to promote compliance with policy requirements?

Services Australia has implemented mandatory induction and refresher training programs for staff on their privacy responsibilities. Training completion rates met the 95 per cent target in 2024.

2.110 Section 16 of the APP Code requires entities provide privacy education or training as part of induction, and to annual training to all staff who have access to personal information.⁶⁰

Induction education and training

2.111 Services Australia has mandatory induction training, which covers the privacy obligations of staff and contractors. The induction training introduces the Privacy Act and APPs, and provides guidance on protocols to meet privacy obligations. This includes guidance on the importance of privacy protection, the handling of personal and sensitive information, and procedures aimed at avoiding or mitigating common privacy incidents. The training also refers to the requirement to follow the operational blueprints (discussed in paragraph 2.66).

2.112 Services Australia monitors the completion of the Induction Mandatory Training Program and reported a 94 per cent completion rate for mandatory induction training in 2023–24, measured against a target of 95 per cent.⁶¹ By the end of the 2024 calendar year, mandatory induction training completion was reported as 97 per cent.

Refresher education and training

2.113 Services Australia has implemented an annual mandatory refresher program that addresses staff privacy obligations and provides guidance on mitigating suspected privacy breaches. The privacy module of the mandatory refresher program refers to the governance arrangements within Services Australia, outlining the appointment of the Privacy Officers and the Privacy Champion.

2.114 Services Australia staff are expected to complete the mandatory refresher program between April and September each year with a target completion rate of 95 per cent. The completion rate was 94 per cent in 2022, 92 per cent in 2023 and 96 per cent in 2024.

Privacy Awareness Week

2.115 Privacy Awareness Week is an annual event run by the OAIC to raise awareness of privacy issues and the importance of protecting personal information.⁶² Services Australia participates in Privacy Awareness Week each year with events such as interviews with OAIC representatives and internal and external executives.

Privacy Contact Officer Network

2.116 The Privacy Champion and Privacy Officers provide ongoing education to the Privacy Contact Officer Network (PCON) — see Case study 1.

60 OAIC, *Privacy (Australian Government Agencies — Governance) APP Code 2017*, available from <https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes/privacy-australian-government-agencies-governance-app-code-2017> [accessed 14 January 2025].

61 A 95 per cent completion target is set out to accommodate staff members who are away on long leave.

62 OAIC, *Privacy Awareness Week*, available from <https://www.oaic.gov.au/engage-with-us/events/privacy-awareness-week> [accessed 17 January 2025].

Has Services Australia established effective arrangements to monitor and report on privacy arrangements?

Services Australia produces a monthly executive report and a quarterly privacy dashboard report for its Security Committee and regular reporting to its Audit and Risk Committee. Services Australia does not publicly report on privacy incidents, complaints and notifiable data breaches.

2.117 Subsection 17(2) of the APP Code requires entities to monitor compliance with its privacy practices, procedures and systems.

Monitoring and reporting

2.118 Services Australia's Security Committee has responsibility for privacy matters. It is chaired by the Chief Operating Officer (COO) and provides advice and support to the CEO and the Executive Committee (comprised of the CEO and deputy CEOs). The Chief Counsel, who is also the Privacy Champion, provides a quarterly privacy report to the Security Committee. These reports include a dashboard with details of the number of privacy incidents reported and substantiated each quarter, broken down by program and main causes. The dashboard includes trend analysis on Family and Domestic Violence (FDV) related privacy incidents and the amount of compensation paid (see case study 2).⁶³ FDV incidents have a heightened privacy risk due to their potential for harm. The reports also include details of NDBs reported to the OAIC. From October 2023, the Chief Counsel also provided a monthly executive privacy report to the Security Committee.

2.119 Services Australia provides regular reports to its Audit and Risk Committee on NDBs and privacy matters, including implementation of OAIC recommendations. In September 2024, further detail was provided in the form of a privacy dashboard report for 2023–24. This included trend and thematic analysis of privacy incidents and NDBs, data on FDV related incidents, OAIC complaints, compensation paid, the number of affected clients and performance data on NDB notifications to OAIC and clients. It also included discussions on key themes in the privacy space, such as 'increased NDBs' and the number of data breaches involving myGov, demonstrating that a strategic view was provided to enable and support strategic monitoring and decision making.

2.120 Table 2.1 provides reporting on key metrics from Services Australia's privacy reports between 2020–21 and 2024–25. Services Australia has attributed the increase in reported privacy incidents in 2024–25 to a combination of increased 'third-party unauthorised access' events, and increased staff awareness and recognition of potential incidents.

⁶³ Compensation may be payable where a complaint is substantiated, and loss or damage is suffered. For further information refer to OAIC, *Guide to privacy regulatory action*, OAIC, Chapter 5: Determinations, available from <https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action> [accessed 24 June 2025].

Table 2.1: Services Australia privacy data by financial year

Financial year	Privacy incidents reported	Privacy incidents substantiated	Substantiated incidents with FDV indicator	Compensation paid (all matters)	Number of compensation cases
2020–21	3,646	2,165	28	\$41,527	7
2021–22	5,485	2,836	71	\$109,139	14
2022–23	4,060	2,041	159	\$163,599	23
2023–24	5,652	2,153	112	\$41,527	7
2024–25	11,413	1,848	73	\$24,500	13
Total	30,103	11,043	443	\$380,292	64

Key: FDV: Family and Domestic Violence.

Source: ANAO analysis of Services Australia quarterly privacy reports provided to executive committees.

Public reporting on privacy performance

2.121 Services Australia does not publicly report on privacy incidents (see paragraph 3.38), complaints (see paragraph 3.34) or NDBs. Until 2018–19, Services Australia reported on the number of substantiated privacy incidents in its annual report.

2.122 The Department of Finance Resource Management Guide 135 sets out requirements for entity annual reports, including:

judicial decisions, or decisions of administrative tribunals or the Australian Information Commissioner, made during the period that have had, or may have, a significant effect on the operations of the entity...⁶⁴

2.123 From 2020–21 to 2023–24, Services Australia’s annual reports included information on one of three privacy determinations made by the Australian Information Commissioner and Privacy Commissioner. Each determination declared that Services Australia had ‘engaged in conduct constituting an interference with the privacy of the complainant’. A fourth determination was made in January 2025, and included in the 2024–25 annual report. Table 2.2 provides details of the four determinations and whether they were included in Services Australia’s annual report. Case study 2 details Services Australia’s response to privacy determination 'WZ' and CEO of Services Australia relating to FDV risks arising from privacy breaches (after paragraph 3.91).

⁶⁴ Department of Finance, *Annual reports for non-corporate Commonwealth entities (RMG 135), Annual report content requirements*, available from <https://www.finance.gov.au/government/managing-commonwealth-resources/annual-reports-non-corporate-commonwealth-entities-rmg-135/annual-report-content-requirements> [accessed 25 June 2025].

Table 2.2: Privacy Commissioner determinations relating to Services Australia

Case name	Date	Summary of requirements imposed by Privacy Commissioner	Included in annual report
'ST' and Chief Executive Officer of Services Australia	30 June 2020	\$3,000 compensation	No
'XA' and CEO of Services Australia	13 April 2021	\$1,000 compensation	No
'WZ' and CEO of Services Australia	13 April 2021	\$19,980 compensation and apology Engage an independent auditor to assess policies, procedures and systems against requirements of APP 11 and report back to the OAIC	Yes
'ATQ' and CEO of Services Australia	23 January 2025	\$10,000 compensation and apology Conduct a review and report back to the OAIC	Yes

Source: ANAO analysis of information from Services Australia and the OAIC.

2.124 As the operator of Healthcare Identifiers Service⁶⁵, Services Australia produces annual reports as required by section 34 of the *Healthcare Identifiers Act 2010*.⁶⁶ These reports provide information about online security and privacy management procedures. The reports confirm that there have been no NDBs for the Healthcare Identifiers Service. The reports do not include information on privacy incidents or complaints.

2.125 In the current environment of increasing privacy risks arising from data breaches and malicious actors, entities should publicly report on privacy incidents, complaints, data breaches and measures to secure the privacy of personal information.

Opportunity for improvement

2.126 As a custodian of data on all Australians, Services Australia could improve the transparency of its management of the privacy of client information by providing additional public information and reporting on privacy complaints, privacy incidents, notifiable data breaches and on responses to privacy issues, such as internal initiatives or strategic plans to reduce impacts or risks.

65 OAIC, *Healthcare identifiers*, available from <https://www.oaic.gov.au/privacy/privacy-legislation/related-legislation/healthcare-identifiers> [accessed 3 March 2025].

66 Services Australia, *Healthcare Identifiers Service annual reports*, available from <https://www.servicesaustralia.gov.au/healthcare-identifiers-service-annual-reports?context=22> [accessed 3 March 2025].

Recommendation no. 5

2.127 There is limited reporting to the Australian Parliament by Australian Government entities on their compliance with the *Privacy Act 1988*. Entities are not required to report in annual reports on their management of privacy. The Attorney-General's Department, in consultation with the Department of Finance as required, consider advice to the Australian Government on options to improve the transparency of entities' compliance with the *Privacy Act 1988*.

Attorney-General's Department response: *Agreed.*

2.128 *The Attorney-General's Department (the department) notes the importance of all entities not only complying with the Privacy Act 1988, but also the transparency of this compliance. The Australian Government Agencies Privacy Code requires all Government agencies to demonstrate best practice in upholding the protection of Australians' personal and sensitive information. The department is developing a second tranche of privacy reforms for consideration by the Government, and alongside that work will consider the most appropriate way to improve transparency of Government agencies' compliance with the Privacy Act. The department will consult with the Department of Finance and the OAIC, noting that the most appropriate arrangements may be through OAIC guidance and reporting, rather than legislative amendment.*

Department of Finance response: *Agreed.*

2.129 *The Department of Finance agrees to the recommendation and welcomes the opportunity to work with the Attorney-General's Department to consider appropriate mechanisms to strengthen the transparency of Commonwealth entities' compliance with the Privacy Act 1988.*

3. Implementation of arrangements to manage the privacy of client information

Areas examined

This chapter examines whether Services Australia has effectively implemented arrangements to manage the privacy of client information.

Conclusion

Services Australia is partly effective in implementing its arrangements to manage the privacy of client information. It undertakes privacy impact assessments (PIAs), however, there were record keeping deficiencies, it does conduct public consultation and does not provide information to the public on its PIAs beyond report dates and titles. There were other gaps with respect to implementation of arrangements including that it: does not analyse data on privacy incidents and complaints to assess risk; has not always been timely in making notifications of notifiable data breaches (NDBs); and has not established an overarching assurance framework setting out how it assures itself that it is effectively managing the privacy of client information.

Areas for improvement

The ANAO made three recommendations to Services Australia aimed at: improving the conduct and transparency of PIAs; undertaking analysis of privacy complaints; and implementing a privacy assurance strategy.

The ANAO also suggested that Services Australia could: review its processes to assure that all aspects of privacy threshold assessments are undertaken and registered; consider implementing a register for tracking and collecting privacy assurance advice; consider implementing an overarching assurance process for NDB processing; and undertake internal audits of privacy within specific programs that it delivers.

3.1 Having established arrangements to manage privacy, entities should ensure that those arrangements operate effectively. This includes ensuring compliance with regulatory requirements for PIAs and NDBs, undertaking assurance activities, and implementing OAIC recommendations.

Has Services Australia undertaken privacy impact assessments appropriately?

Services Australia undertakes privacy threshold assessments (PTAs) for projects involving new or changed information arrangements. Higher risk projects are subject to privacy assurance advice or a privacy impact assessment (PIA). Services Australia appropriately undertakes PIAs, except that none included public consultation. Record keeping of PTAs and PIAs was deficient. Services Australia maintains a public PIA register. It does not publish PIAs. One of the 18 Freedom of Information requests for PIAs since 2020 was successful; 14 were refused on the basis of legal professional privilege.

3.2 The Privacy (Australian Government Agencies — Governance) APP Code 2017 (the APP Code) requires that agencies undertake PIAs ‘for all high privacy risk projects’, where an agency

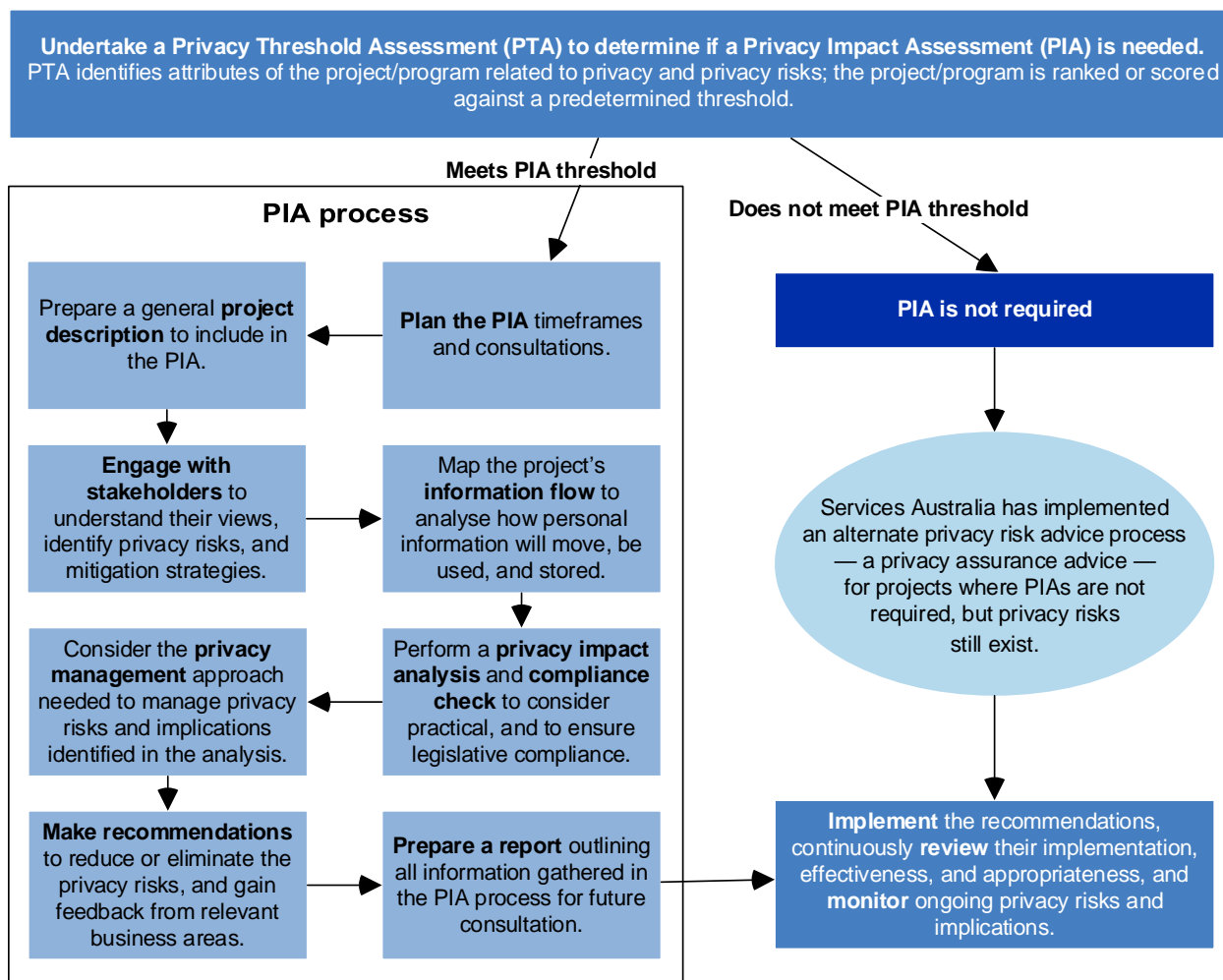
‘reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals’.

3.3 The OAIC defines a PIA as:

a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. PIAs are an important component in the protection of privacy, and should be part of the overall risk management and planning processes of organisations and Australian Government agencies.

3.4 The OAIC’s *Guide to undertaking privacy impact assessments* (PIA Guide)⁶⁷ sets out a 10-step process commencing with a privacy threshold assessment (PTA) to ‘determine whether it will be necessary to undertake the rest of the steps involved in a PIA’.

Figure 3.1: Privacy impact assessment 10-step process



Note: A privacy assurance advice is not a process defined by the OAIC.

Source: ANAO analysis and adaptation of the OAIC *Guide to undertaking privacy impact assessments*.

⁶⁷ OAIC, *Guide to undertaking privacy impact assessments*, 2 September 2021, available from <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessments> [accessed 4 June 2025]

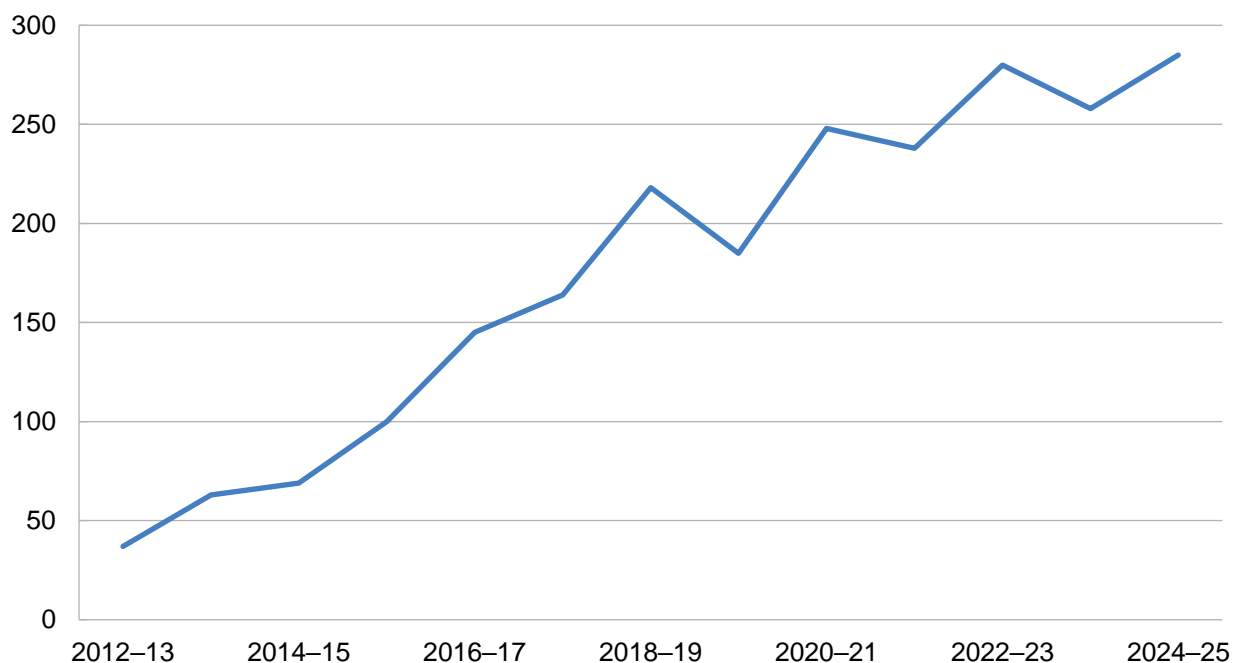
Privacy threshold assessments

3.5 The OAIC recommends undertaking a privacy threshold assessment (PTA) as a preliminary assessment to determine a ‘project’s potential privacy impacts’ and to help entities determine if a project is ‘a “high privacy risk project” requiring a PIA under the APP Code’.

3.6 Services Australia requires a PTA for all new projects and activities which ‘involve changes to the way the agency collects, uses, stores, discloses or handles personal information’. Business leads are required to work with the Privacy and Personal Information Release Branch (PPIR branch) to undertake PTAs, and assess if a PIA or privacy assurance advice (see paragraphs 3.15 to 3.16) is required for the project.⁶⁸ The annual mandatory refresher training (discussed at paragraphs 2.113 and 2.114) reminds all staff of PTA requirements.

3.7 Services Australia has a PTA form. Once completed, it is to be approved by the relevant Senior Executive Service (SES) officer. The PPIR branch determines whether a privacy assurance advice, PIA, or no further action is necessary. The inclusion of a section in the form on client safety represents an adaptation of the OAIC guidance on PTAs for Services Australia’s operational context. Services Australia advised the ANAO on 30 July 2025 that a PIA may be completed without a PTA when there are ‘early indications that a PIA will be required’ for a project. Figure 3.2 charts the number of PTAs completed by Services Australia between 2012–13 and 2024–25.

Figure 3.2: Number of PTAs completed per financial year



Source: ANAO analysis of Services Australia PTA register, provided by Services Australia to the ANAO.

3.8 Services Australia’s PTA form includes a self-assessment matrix with scores informing the subsequent action:

⁶⁸ The PPIR branch ‘manages, coordinates and advises on the agency’s response to privacy incidents and advises on privacy policy and strategy’ and ‘coordinates and manages customer information consent and public interest release as well as responses to subpoenas.’ This branch is led by one of the privacy officers.

- Total below 5 points — No privacy impact assessment or Privacy assurance advice required
- Total between 5 and 11 points — Probably no privacy impact assessment required, but privacy assurance advice may assist you to comply with privacy requirements
- Total over 11 points — the project may require a privacy impact assessment, please provide your completed signed PTA form to [redacted]

3.9 Services Australia has an overarching assurance framework for project management. This framework details different assurance approaches, including self-assurance of legal and policy compliance, independent assurance checks undertaken by third parties, and audits. There is no specific arrangement setting out how Services Australia gains assurance that PTAs are undertaken for all required projects.

3.10 Services Australia maintains a register of all active projects and an internal register for completed PTAs. As at 29 August 2025, all 119 projects requiring a PTA had one on file.

Conduct of PTAs

3.11 The ANAO assessed a random sample of 16 completed PTAs from a total of 1,134 undertaken between July 2020 and October 2024. The 16 PTAs examined contained the following exceptions to the OAIC guidance:

- seven (including three PTAs not filed) did not consider client safety considerations;
- 11 (including three PTAs not filed) did not recognise specific needs of clients from high-risk demographics (i.e. those living with a disability) and how they may have been impacted by the project, as has been included as part of Services Australia's PTA guidance;
- five (including three PTAs not filed) were not finalised with required signoffs;
- six (including three PTAs not filed) did not explicitly define the legislative authority for handling of personal information; and
- five PTAs were not in the appropriate file — of these, two were not able to be located for testing.

3.12 Services Australia advised the ANAO that PIAs may be completed for projects without a prior PTA (see paragraph 3.7). The ANAO selected nine PIAs for assessment (see paragraph 3.20), and found that three of the nine PIAs examined had a PTA on file and that none of these PTAs were finalised or signed appropriately.

3.13 From 2022–23 to 2024–25, 823 PTAs were completed; over the same period Services Australia completed 524 pieces of privacy assurance advice (see paragraph 3.15) and 57 PIAs were added to Services Australia's register (see paragraph 3.20 for discussion of the register⁶⁹, and Figure 3.1 for the relationships between PTAs, PAAs, and PIAs).

69 Services Australia PIA register at: Services Australia, *Privacy Impact Assessment Register*, <https://www.servicesaustralia.gov.au/privacy-impact-assessment-register?context=22> [accessed 8 August 2025].

Opportunity for improvement

3.14 Services Australia could review its processes for assuring that all aspects of PTAs are completed if required, and that PTAs are appropriately logged.

Privacy assurance advice

3.15 Teams undertaking projects can request or be provided internal 'privacy assurance advice' from Services Australia's legal team. Privacy assurance advice is additional to OAIC requirements (see Figure 3.1) and provides assurance over the privacy risk of a project or activity where the privacy risk is below the risk threshold required to complete a PIA. There is no documented process relating to privacy assurance advice and the provision of advice is not standardised. It is generally provided to project owners and teams through emails, which contain privacy and legal advice.

3.16 The ANAO reviewed a random selection of 16 pieces of privacy assurance advice from the 448 produced between July 2022 and November 2024.⁷⁰ There were record-keeping deficiencies with four not on file nor subsequently located by Services Australia. Of the 10 on file, the privacy assurance advice appropriately drew out privacy implications for the relevant projects.

Opportunity for improvement

3.17 Services Australia could consider implementing a register to track and store privacy assurance advice material provided to different projects.

Privacy impact assessments

3.18 The APP Code requires that entities must conduct a PIA for all high-risk projects, maintain a register of PIAs, and publish a version of the register on its website.

Conduct of PIAs

3.19 The OAIC has developed an eLearning course, the PIA Guide, and a toolkit to assist entities undertaking PIAs. The OAIC recommends the use of PIAs 'alongside existing project management and risk management methodologies or as a process in its own right'. The PIA Guide sets out a 10-step process, commencing with a PTA to 'determine whether it will be necessary to undertake the rest of the steps involved in a PIA'. Figure 3.1 shows this process.

3.20 As of February 2025, Services Australia's register of PIAs (see paragraphs 3.25 to 3.26) included 45 PIAs that were added between July 2022 and January 2025. The ANAO selected nine PIAs (20 per cent) to assess against the PIA Guide.⁷¹ The ANAO found the following.

- All were undertaken by contracted legal services providers.⁷²

70 This range as this population was the most-current provided to the ANAO at the time of testing.

71 The ANAO took a targeted sample of nine PIAs as to cover a cross section of Services Australia's activities, including payments, Medicare, fraud, myGov, artificial intelligence and information exchange with an external party (Victorian government).

72 The external firms that undertook the tested PIAs were the Australian Government Solicitor, HWL Ebsworth, Maddocks, and Sparke Helmore.

- The ANAO assessed that seven PIAs largely followed the 10 steps set out in the PIA Guide (see Figure 3.1).
- None included public consultation.
- Two of the sampled PIAs were not added to Services Australia's PIA register in a timely manner, with one added 11 months, and the other two years and nine months after finalisation of the report in August 2020 (not assessed as it predated the PIA guide).

Publication of PIAs

3.21 While the publication of PIAs is not a mandatory requirement under the APP Code, the PIA Guide states that 'ideally, the entity's response to the PIA recommendations will be published together with the PIA report'. Services Australia does not publish its PIAs in part or whole, a summary of the project, details of recommendations, or responses to recommendations on its public register (see paragraphs 3.25 to 3.26).

3.22 Services Australia's PIA register states that copies of PIAs can be sought by making a request under the *Freedom of Information Act 1982* (FOI Act). One of 18 FOI requests for PIAs made between November 2020 and December 2024 was successful. Of the 18 requests made:

- two were withdrawn — one due to the applicant not responding to preliminary charge notices, and the other being a voluntarily withdrawal from the applicant following the charge notices;
- one request from November 2023 — 'Privacy Impact Assessment on the DHS Response to the Independent Review of Health Providers Access to Medicare Numbers', December 2018 — was released with a partial exemption under FOI Act subsections 37(2)(b) disclosure of methods of investigation and 47E(d) adverse effect on operations;
- one request was refused under subsection 24(1) of the FOI Act, on the basis a practical refusal reason existed; and
- 14 requests were refused under the section 42 legal professional privilege exemption of the FOI Act — of these 14 requests, 11 also utilised section 47 exemption powers.⁷³

3.23 The PIA Guide discusses a range of options for undertaking a PIA using internal and external expertise, including with practitioners who have 'a range of expertise' from across 'information security, technology, risk management, law, ethics, operational procedures and industry-specific knowledge'. Services Australia has frequently relied on external legal providers to undertake PIAs on its behalf — see paragraph 3.20.

3.24 The OAIC 'strongly encourages the publication of PIA reports' to project transparency, and to demonstrate to 'stakeholders and the community' that all projects have 'undergone critical privacy analysis, potentially reducing community concerns about privacy'. The use of legal professional privilege exemptions is at odds with the intent of PIAs which includes building community trust, with the OAIC describing PIAs as systematic assessments of projects which identify the impacts which project may have on the privacy of individuals.

⁷³ Three specific *Freedom of Information Act 1982* exemptions were used under section 47 for denial of FOI requests: section 47C (document contains deliberative matter), subsection 47(1)b (document contains commercially valuable information) and section 47E (disclosure of documents would have an adverse effect on agency operations).

Register of PIAs

3.25 Services Australia maintains a register of completed PIAs on its website.⁷⁴ The PIA register includes the PIA title, posted date and reference number. The OAIC recommends that PIA registers also include ‘a summary of the project, the team responsible for undertaking the PIA and the outcome of the PIA or project’. Services Australia’s PIA register does not include sufficient information to inform the reader of the nature of the project or the outcome of the PIA.

3.26 In July 2021, the OAIC assessed agencies within the Social Services portfolio as part of the PIA register assessment program and found Services Australia to be compliant with subsection 15(1) of the APP Code.⁷⁵ This assessment checked that there was a register on Services Australia’s website, and not if the register was complete and accurate. The ANAO identified instances of delays in adding PIAs to the register (see paragraph 3.20).

Recommendation no. 6

3.27 Services Australia improves the conduct and transparency of its privacy impact assessment (PIA) processes by:

- (a) implementing external consultation arrangements for PIAs;
- (b) publishing a description of each PIA on its PIA register;
- (c) implementing arrangements to ensure PIAs are added to its public register in a timely manner;
- (d) reviewing the appropriateness using of legal professional privilege Freedom of Information requests for PIAs; and
- (e) publishing PIA reports to the extent that this does not exacerbate privacy or other risks.

Services Australia response: *Agreed.*

3.28 *Response to Recommendation 6(a):*

Services Australia will identify any internal and external stakeholders who are or might be interested in or affected by a project and consider consultation where appropriate depending on the scale and likely impact of the project, provided such consultation does not increase security risk to customers or Agency systems which may lead to greater risks to customers’ privacy. Services Australia will also work with policy agencies to identify opportunities for public or targeted consultation during policy and program design processes, to consider community attitudes to and expectations of privacy at an early stage of a project which can be considered as part of the PIA.

74 Services Australia, *Privacy Impact Assessment Register*, available from <https://www.servicesaustralia.gov.au/privacy-impact-assessment-register?context=22> [accessed 7 March 2025].

75 OAIC, *Privacy impact assessment register assessment program*, 6 June 2022, available from <https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-assessments/privacy-impact-assessment-register-assessment-program> [accessed 4 November 2024].

The OAIC advised that the ANAO on 11 April 2025 that ‘Services Australia had on its website a PIA register and demonstrated good practice in having updated the register within the last 6 months. The OAIC did not examine whether Services Australia had published on that register all the PIAs it had conducted’.

3.29 Response to Recommendation 6(b):

The legal obligation under the Privacy (Australian Government Agencies – Governance) APP Code 2017 (the Code) is for an agency to maintain and publish a register of the PIAs it has conducted. Services Australia currently meets its obligations under the APP Code. The Agency will publish a description of each new PIA on its register on a case-by-case basis while balancing security and privacy risks. As many of the Agency’s PIAs contain security information, and/or information relevant to its practices, processes and systems that if publicly available, could expose the Agency’s security settings leading to greater risk to customers’ privacy, the Agency must have regard to security and privacy risks when considering publishing a description of a PIA on its register.

3.30 Response to Recommendation 6(c):

Services Australia has improved its arrangements in place to ensure PIAs are added to its public register and guidance material is being developed to support timely publication.

3.31 Response to Recommendation 6(d):

While recommendation 6 refers to FOI, the recommendation more broadly relates to the way the Agency prepares PIAs – improving transparency by publishing those parts of a PIA that are not sensitive. In this way, the FOI approach will not change – FOI will only redact the part/s of the PIA the Agency has already identified as sensitive and not published, with relevant FOI Act exemptions considered holistically and layering applicable exemptions, such as the s 47E(d) conditional exemption (operations of the agency) and the s 42 Legal professional Privilege exemption.

3.32 Response to Recommendation 6(e):

The legal obligation under the Privacy (Australian Government Agencies – Governance) APP Code 2017 (the Code) is for an agency to maintain and publish a register of the PIAs it has conducted. Services Australia currently meets its obligations under the APP Code. The agency will publish a summary of each new PIA on its register on a case-by-case basis while balancing security and privacy risks. As many of the agency’s PIAs contain security information, and/or information relevant to its practices, processes and systems that if publicly available, could expose the agency’s security settings leading to greater risk to customers’ privacy, the agency must have regard to security and privacy risks when considering publishing a description of a PIA on its register.

Has Services Australia complied with the *Privacy Act 1988* requirements in relation to privacy complaints and notifiable data breaches?

Services Australia accepts privacy-related complaints through its complaint's mechanism. It does not analyse or report on privacy complaints, nor does it use data from privacy complaints to inform its risk assessments. Services Australia did not meet the legislated 30-day requirement for assessing potential NDBs in 2022–23 or 2023–24. It met this requirement in 2024–25. Services Australia did not notify affected individuals and the OAIC in accordance with its internal target timeframes, although performance improved in the first quarter of 2025–26. Services Australia has not documented its approach to assuring that its handling of NDBs complies with the Privacy Act.

Privacy complaints

3.33 APP 1 requires entities to take reasonable steps that 'will enable the entity to deal with inquiries or complaints from individuals.'

3.34 Services Australia does not have a distinct complaint's mechanism for privacy-related complaints. Privacy-related complaints are processed using the general management mechanism. Services Australia's privacy policy includes reference to its complaints processes and advises that complainants can contact the OAIC if their complaint is not resolved to their satisfaction.⁷⁶ The privacy policy does not state that Services Australia is bound by the APP Code, meaning clients may be unaware of Services Australia's APP Code responsibilities.

3.35 Services Australia's website informs clients as to how they can submit a complaint about how Services Australia has used, managed, or disclosed their personal information. It also advises that they can contact the OAIC for independent investigations of privacy complaints.

3.36 Services Australia advised the ANAO on 21 March 2025 that where part or all of the content of the complaint made to Services Australia is determined to constitute a privacy incident, a privacy incident is created and treated separately to the initial complaint. The source of these incidents — being internal or external — can provide an indication as to the general trends in complaints being made about privacy, though this data does not indicate which externally-identified privacy incidents were recorded through complaints. In 2021–22, 42 per cent of potential privacy incidents (see paragraph 3.41) reported to Services Australia came from external sources; this increased to 80 per cent in 2024–25.

3.37 As noted in paragraph 3.34, all complaints are dealt with using the general complaint's mechanism. Reporting of privacy incidents (see Table 2.1 and Figure 3.3) does not include data on the number of complaints made directly about privacy. This means that data on privacy complaints cannot inform risk assessments, group risk management plans, or the controls for managing risks (see from paragraph 2.17).

76 Services Australia, *Privacy Policy*, available from <https://www.servicesaustralia.gov.au/privacy-policy?context=22> [accessed 14 November 2024].

Privacy incidents

3.38 Services Australia defines a privacy incident as ‘an event that may amount to a breach of privacy and necessitates action by the agency’. Privacy incidents are identified through complaints, self-reporting by staff, or through any process by which an incident⁷⁷ could be identified.

3.39 Staff are required to report potential privacy incidents to the Privacy and Personal Release (PPIR) branch at the time of identification through use of a privacy incident notification tool. This is to enable the investigation of potential breaches and their reporting (if required). Services Australia’s approach to privacy incidents aligns with the procedures required in the Privacy Act, and the OAIC’s data breach preparation and response guide.

3.40 Services Australia’s operational privacy policy requires that staff involved with a privacy incident ‘support the Privacy Officer [and the PPIR branch] to investigate, manage and remediate privacy incidents’ and to determine if the incident constitutes an NDB — this process begins with the reporting of privacy incidents.

3.41 From 1 July 2022 to 30 June 2025, Services Australia reported the identification of 20,648 potential privacy incidents. In this same period, 14,606 incidents (70.7 per cent) were not substantiated as privacy incidents and 6,042 (29.3 per cent) were substantiated. Of the substantiated privacy incidents, 144 were found to be NDBs.

3.42 The Privacy Act and the OAIC’s Data breach preparation and response guide⁷⁸ require entities to take reasonable steps to assess potential data breaches within 30 days and to notify the OAIC and affected individuals as soon as practicable after assessment. Services Australia’s August 2024 Privacy Incident and Data Breach Response Plan sets key performance indicators after assessment of three business days for notification to the OAIC and 10 business days for notification to individuals. Of 165 NDBs notified to OAIC between 2018–19 and 2024–25, 117 (71 per cent) were reported to the OAIC 50 or more days after Services Australia became aware of the incident.

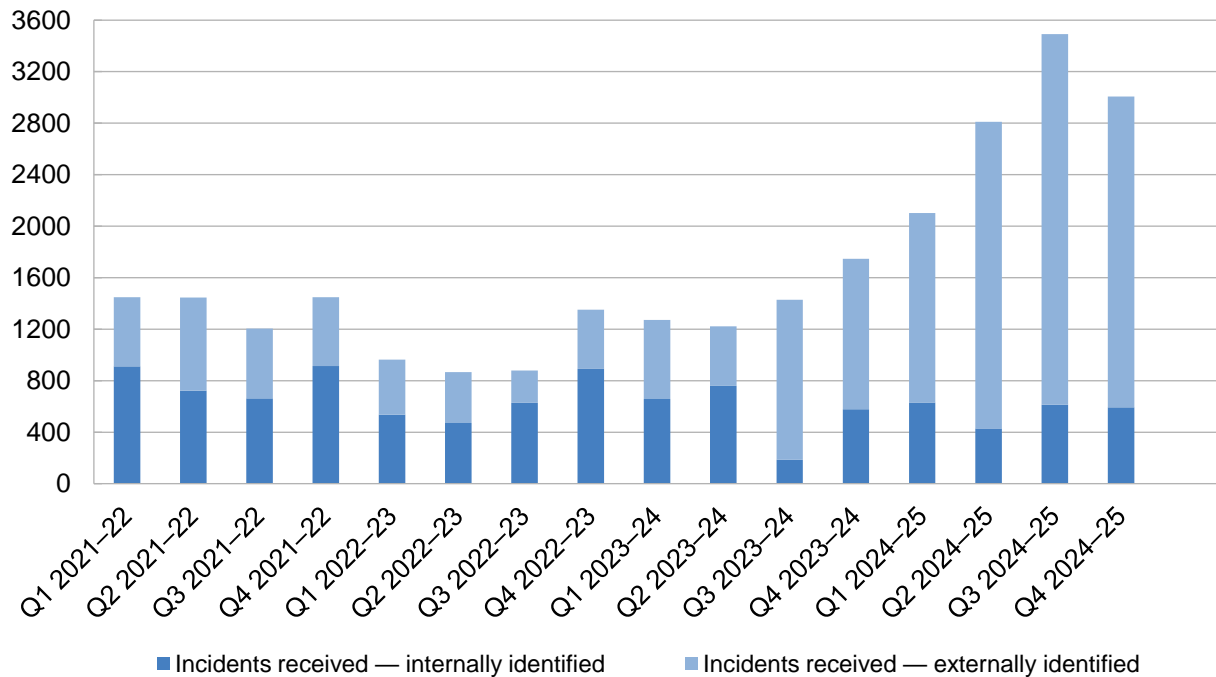
3.43 Reporting is provided to the Executive Committee with metrics on privacy incidents and NDBs (see paragraph 2.118). Quarterly reporting to the Security Committee (discussed at paragraphs 2.10, 2.40, and 2.118) includes metrics on privacy incidents and whether they were identified internally (through an internal assurance mechanism) or externally.

3.44 Figure 3.3 shows that the number of externally identified privacy incidents, both substantiated and unsubstantiated, has been increasing over time (this figure does not differentiate between the two, and just shows incidents as reported prior to assessment). Services Australia has attributed this increase primarily to ‘significant’ increases in ‘customer privacy complaints relating to fraudulent activity within online accounts’ (myGov) where clients ‘have contacted the agency after identifying suspected unauthorised access to their online account’.

77 An ‘incident’ involves client or employee personal information being collected, used, accessed, disclosed, or destroyed without required consent or appropriate legal authority.

78 OAIC, Data breach preparation and response, A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth), July 2019, available from <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response> [accessed 13 October 2025].

Figure 3.3: Internally and externally identified privacy incidents (substantiated and un-substantiated), 2021–22 to 2024–25



Source: ANAO analysis of Services Australia reporting to its executive on privacy matters.

3.45 The reporting to the Security Committee includes details of the nature and the cause of privacy incidents (both internally and externally identified), but does not further disaggregate this data for external complaints, or report on the seriousness of privacy complaints, including whether these resulted in NDBs. This limits Services Australia’s capacity to understand client privacy concerns, monitor trends, identify and address emerging risks and implement continuous improvement.

3.46 The OAIC receives complaints from stakeholders and members of the public about entities across the government and non-government sectors. The proportion of complaints made about Services Australia when compared to all government entities fell from 32.66 per cent in 2018–19 (130 about Services Australia, 268 about the rest of government) to 12.61 per cent in 2024–25 (44 about Services Australia, 305 about the rest of government). See Appendix 4.

Recommendation no. 7

3.47 Services Australia undertake analysis and reporting of privacy complaints to understand trends, identify emerging risks and promote continuous improvement in its management of privacy.

Services Australia response: *Agreed.*

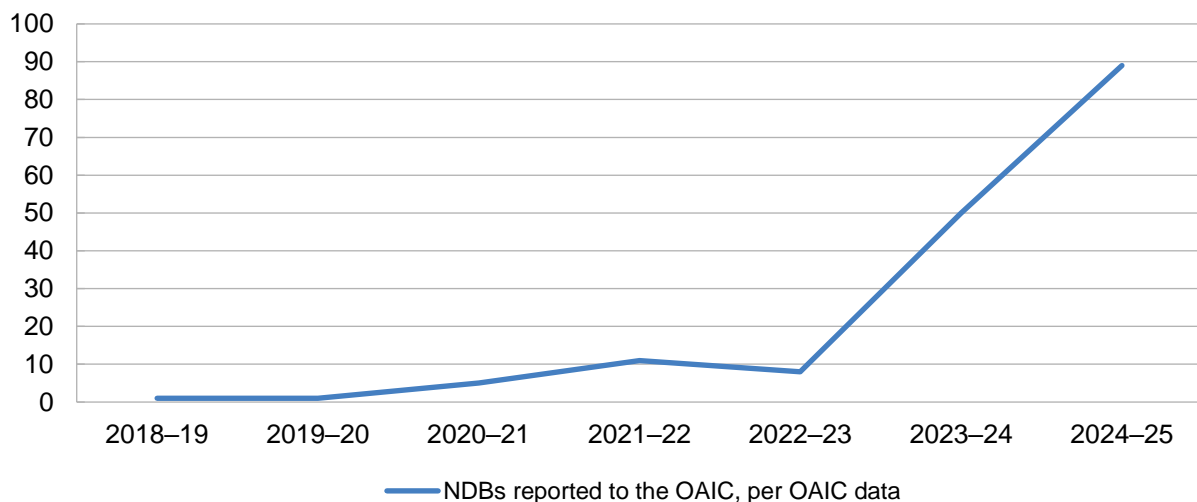
3.48 *Services Australia is committed to continuous improvement in uplifting the analysis and reporting of Privacy Incidents, NDBs, and complaints; to provide greater insights on the Agency's privacy risk environment.*

Notifiable data breaches

3.49 The *Privacy Amendment (Notifiable Data Breaches) Act 2017* established the NDB scheme, which requires entities to 'notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved'.

3.50 Services Australia reported 165 NDBs to the OAIC between 2018–19 and 2024–25. Figure 3.4 shows the NDBs reported by year.⁷⁹ The number of NDBs occurring due to malicious or criminal actions has been increasing over time — 82 NDBs in 2024–25 related to malicious or criminal actions, compared to 50 in 2023–24 and seven in 2022–23. The increasing volume of NDBs driven by an increase in the number of 'malicious or criminal attack' is consistent with trends reported by the OAIC.⁸⁰

Figure 3.4: Number of NDBs reported per financial year by Services Australia to OAIC



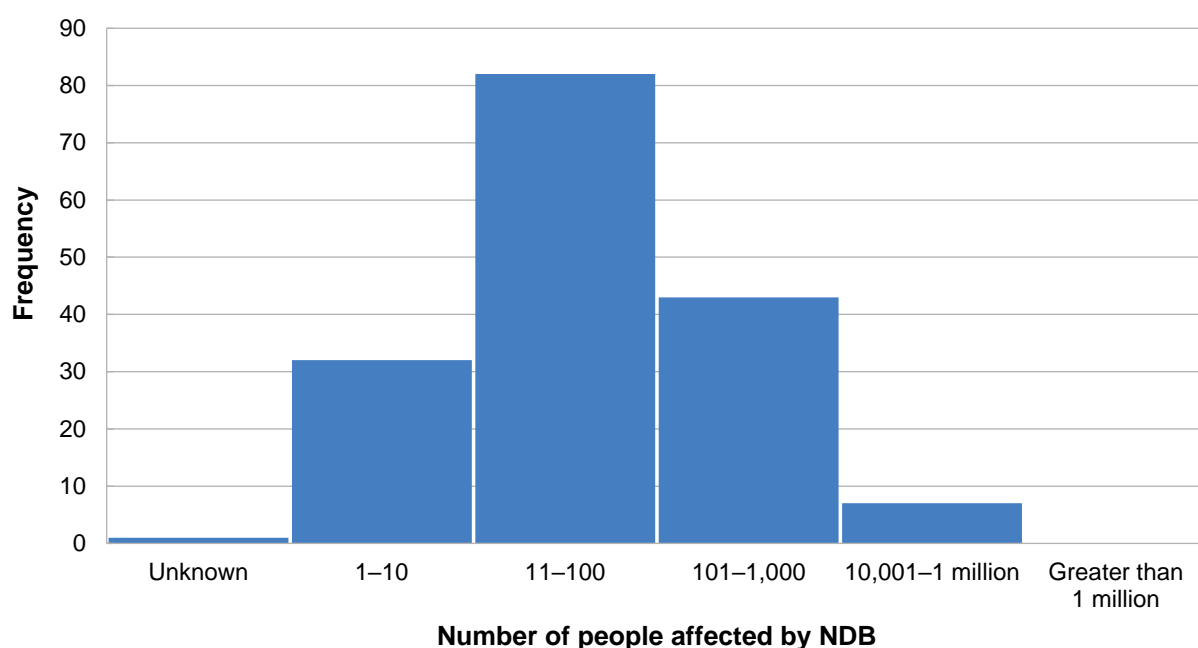
Source: ANAO analysis of OAIC data on NDBs reported by Services Australia.

⁷⁹ The ANAO has relied on the information provided by the OAIC for analysis the number of NDBs each financial year, as Services Australia's records of its NDBs did not contain complete date fields for all events.

⁸⁰ The OAIC reported 'Malicious or criminal attack' as the source of 69 per cent of breaches in the six months to December 2024, an increase of 17 per cent from the previous report. OAIC, *Notifiable Data Breaches Report: July to December 2024*, OAIC 13 May 2025, available from <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2024> [accessed 16 June 2025].

3.51 Figure 3.5 provides a breakdown of NDBs by the number of people affected in each given NDB. Around one-third of NDBs (50 of 165) affected between 11 and 100 people. There were no NDBs that affected one million or more individuals.

Figure 3.5: Services Australia NDB events by number of people affected, 2019–20 to March 2025



Source: ANAO analysis of OAIC data reported by Services Australia.

3.52 The OAIC has developed a data breach preparation and response guide to assist entities meet their reporting obligations.⁸¹ Services Australia developed a Privacy Incident and Data Breach Response Plan, that incorporates OAIC guidance, to aid identification and reporting of privacy incidents and NDBs.

3.53 Services Australia requires that all privacy incidents, including any suspected NDBs, are reported to the PPIR branch ‘immediately’ after identification (see paragraph 3.39). The PPIR branch assesses each to determine if an NDB has occurred and if reporting to the OAIC is required. The assessment is required to be completed within 30 days, consistent with subsection 26WH(2b) of the Privacy Act.⁸²

3.54 Figure 3.6 shows the number of confirmed NDBs per financial year, with the number of these that were and were not assessed within the 30-day requirement. Between 1 July 2019 and 30 June 2025, 46 (27 per cent) of the 170 confirmed NDBs were processed within the 30-day timeframe, and 123 (72 per cent) were not processed in the required timeframe.⁸³ One NDB had its

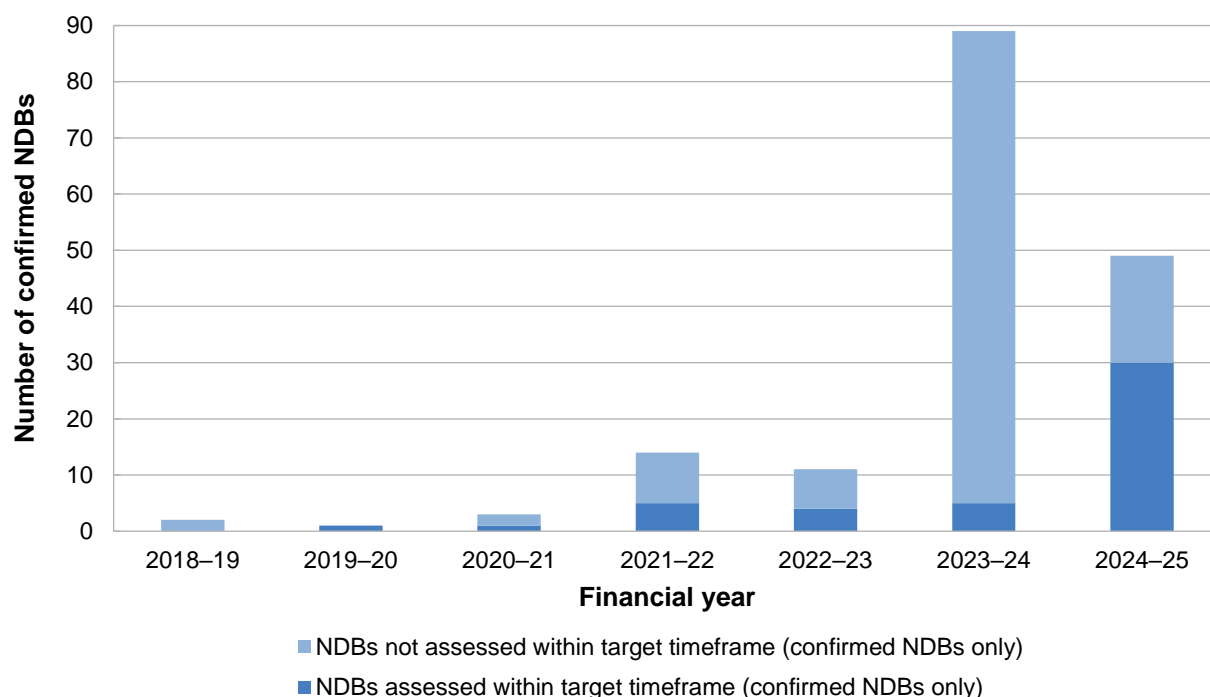
81 OAIC, *Data breach preparation and response*, available from <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response> [accessed 26 November 2024].

82 Under section 26WH of the Privacy Act, an entity must ‘take all reasonable steps to ensure that the assessment is completed within 30 days’. For the purpose of this analysis, the clock starts once the PPIR branch receives the potential NDB.

83 This is the number recorded in Services Australia’s dataset, see footnote 79.

assessment completion date registered as after its incident date. Services Australia internal briefings note that an increase in the number of reported incidents, when compared to historical averages, has meant that processing times for NDBs has increased.

Figure 3.6: Identification of NDBs within 30 days after notification of privacy incident



Note: The number of NDBs in each given year differs to those presented in Figure 3.4 as this data represents the date on which each NDB occurred, rather than when each NDB was reported to the OAIC.

Note that one NDB for 2020–21 shows its assessment completion date as occurring after the incident date, and is therefore not included in this figure.

Source: ANAO analysis of Services Australia data, showing work records and logs as created by Services Australia processing staff.

3.55 A September 2023 internal audit report on NDBs found that Services Australia’s internal assessments of NDBs were not being completed within the 30-day statutory timeframe. This internal audit recommended that Services Australia implement a centralised ‘register for recording suspected data breaches to support’ monitoring and oversight of the breaches, and compliance with the 30-day assessment requirement. Services Australia reported these recommendations as closed in October 2023. The ANAO has not verified their implementation.

3.56 The Privacy Act requires entities to notify the OAIC and affected individuals of NDBs ‘as soon as practicable’. Services Australia aims to notify the OAIC within three business days, and affected individuals within 10 business days of the NDB assessment being completed. Table 3.1 shows that Services Australia has not met these target timeframes. This is consistent with the findings of the internal audit report discussed in paragraph 3.55, which found that:

there were delays in notifying the affected individuals in all notifiable data breaches examined in this audit — [and] there was no clear or apparent reason for the delays based on records and consultations with the Privacy and Personal Information Branch.

3.57 Services Australia advised the ANAO on 30 July 2025 ‘that notifying individuals is a complex undertaking requiring data extraction to ensure notifications are accurately addressed and delivered to customers’, and that each notification also involves risk assessments:

to ensure customers identified as experiencing vulnerability or who are at risk, can be provided with appropriate support to understand what occurred and what they need to do.

3.58 The internal audit also recommended that Services Australia incorporate ‘processes for internal escalation and notification to OAIC when the agency is unable to meet statutory timeframes’ into the Privacy and Data Breach Response Plan, which alongside the recommendation discussed in paragraph 3.55, was intended to increase Services Australia’s oversight on NDB case handling and notifications.

3.59 Services Australia advised the ANAO on 4 September 2025 that, since June 2025, a new ‘Data Breach Mailout service’ has been instituted to enable Services Australia staff to provide NDB notifications to affected customers via surface mail or electronic means. The impact and success of this is subject to ongoing evaluation and monitoring by Services Australia.

Table 3.1: Services Australia reporting of confirmed NDBs to the OAIC and clients

Financial year	Total NDBs	Reporting to the OAIC — not within target	Reporting to clients	
			Not within target	NDBs with reporting exemption ^a
2019–20	1	0 (0%)	0 (0%)	0
2020–21	4	2 (50%)	2 (50%)	0
2021–22	14	11 (79%)	10 (71%)	0
2022–23	11	6 (55%)	4 (40%)	1
2023–24	89	82 (92%)	43 (60%)	17
2024–25 ^b	49	42 (86%)	36 (82%)	5
2025–26 Q1	13	4 (8%)	1 (8%)	1

Note a: Exemptions made under *Privacy Act 1988* section 26WN Exception — enforcement related activities.

Note b: 37 NDBs in 2024–25 (76 per cent) were reported to the OAIC between three and 10 business days after the completion of assessment.

Source: ANAO analysis of Services Australia data.

NDB assurance

3.60 Services Australia does not have a documented overarching process for assuring its the compliance with the Privacy Act when assessing potential NDBs (see paragraphs 3.38 to 3.39). Services Australia advised the ANAO on 2 April 2025 that the PPIR branch assures itself of its compliance with the Privacy Act when assessing potential NDBs (privacy incidents — see paragraphs 3.38 to 3.39) by referring to the Privacy Act and OAIC information, and using these as guides, during the NDB assessment and determination process. These assurance processes are limited to activities undertaken during the processing of NDBs.

Opportunity for improvement

3.61 In implementing recommendation 8, Services Australia could incorporate an assurance strategy for its NDB processes to support consistency in processing.

Does Services Australia have appropriate assurance arrangements over its management of the privacy of client information?

Services Australia does not have a privacy assurance strategy. There are a range of internal controls and assurance processes, including user access monitoring, quality monitoring of calls and internal audit, that provide assurance over the management of personal information. Services Australia has unresolved ANAO user access controls audit findings which are not being addressed at a pace commensurate with the increasing risks to privacy.

3.62 Subsection 16(b) of the *Public Governance, Performance and Accountability Act 2013* (the PGPA Act) requires that an accountable authority establishes and maintains an appropriate system of internal control. Section 17 of the APP Code requires that agencies must monitor compliance with its privacy practices, procedures and systems regularly.

3.63 The *Australian Privacy Principles Guide* states that entities consider implementing ‘a program of proactive review and audit of the adequacy and currency of the entity’s APP Privacy Policy and of the practices, procedures and systems implemented under APP 1.2’.⁸⁴

Internal controls and detections

3.64 Services Australia has internal controls aimed at detecting and preventing inappropriate access and sharing of personal information, including the following.

- Enhanced Staff Access Restriction: System flagging in Centrelink systems to detect where staff have accessed their own records or those belonging to family members.
- High-profile individuals monitoring: Where an individual has been flagged as high profile (celebrity, media relevance, etc.), their information access logs are checked each week to determine if inappropriate access has occurred.
- Enterprise Data Warehouse user access control: Access permissions are siloed, and access roles are applied based on business justifications. Some external users in partner agencies have access. All users only have access to front-end representations of data, and not the underlying data itself (i.e. they cannot modify it).
- Data loss prevention (DLP) policy: Email filtering and monitoring to identify outbound emails which may be carrying personal or operational information, and/or may be addressed to inappropriate recipients. These detections are determined by a range of business rules designed to detect inappropriate information management.

84 OAIC, *Australian Privacy Principles Guidelines*, December 2022, available from <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines> [accessed 22 January 2025].

3.65 ANAO testing of the DLP policy found no indication of systemic issues or failures in Services Australia's email monitoring processes.

Code of conduct investigations

3.66 In 2023–24, Services Australia undertook 116 code of conduct investigations related to potential improper personal information access; 115 of were detected through a compliance or monitoring system; and 111 investigations found a breach had occurred. Two employees were terminated, 16 had a reduction in salary, 55 received a fine, and 81 received a reprimand. Code of conduct investigations can result in multiple penalties being applied, with 154 total penalties applied against 116 code of conduct investigations in 2023–24.

3.67 Since July 2021, there have been 16 criminal matters related to the misuse of personal information by Services Australia staff, and three referrals made to the National Anti-Corruption Commission relating to the misuse of personal information.

User access controls

3.68 Auditor-General Report No.39 of 2024–25 *Interim Report on Key Financial Controls of Major Entities*⁸⁵ contained seven moderate open findings against Services Australia relating to controls over information management and access. Five of these findings relate to Services Australia's management of client privacy in the context of Medicare and Centrelink service delivery and were unresolved as of May 2025. These findings relate to IT governance, privileged user management, monitoring of super users, and Medicare mainframe and user access management.

- IT Governance: an overall assessment of the 'increasing number of IT governance issues' present at Services Australia. It was 'first identified in 2022–23 as a significant audit finding', and 'downgraded to a moderate audit finding' in 2024–25 in recognition of Services Australia's implementation of remedial actions and ANAO recommendations.
- Privileged User Management: minor finding in 2020–21 and upgraded to a moderate finding in 2022–23, the finding 'relates to the ineffective logging and monitoring of user accounts with access to high-risk, financially significant transactions in the SAP enterprise resource planning system'.
- Monitoring of super users (Medicare, Child Support and Health): minor audit finding in 2020–21 and upgraded to a moderate finding in 2022–23, the finding 'relates to the ineffective monitoring of user accounts with extensive access rights (privileged users) within the Medicare, Child Support and Health mainframes.'
- Monitoring of super users (Centrelink): identified in 2022–23, this finding relates to 'ineffective monitoring of user accounts with extensive access rights (privileged users) within the Centrelink mainframe'.
- Medicare mainframe passwords and user access management: Identified as separate minor audit findings and amalgamated and upgraded in 2023–24 to one moderate audit finding, this relates to weaknesses 'in relation to passwords and user access management for the Medicare Mainframe system'.

85 Auditor-General Report No. 39 of 2024–25, *Interim Report on Key Financial Controls of Major Entities*, ANAO, Canberra, 2025, pp. 99–100, available from <https://www.anao.gov.au/work/financial-statement-audit/interim-report-key-financial-controls-of-major-entities-2024-25> [accessed 16 June 2025].

3.69 These findings indicate ongoing deficiencies and represent privacy risks related to inappropriate access by staff to personal information. The risks associated with these findings are not clearly identified in Services Australia risk management plans, but are addressed through preventative and detective controls, including privacy training, mainframe user access monitoring and email monitoring (see paragraph 3.64).

3.70 Four of these findings were unresolved after two years. While Services Australia is taking actions to address controls reports findings and recommendations, it is not doing so at a pace commensurate with the higher privacy risks associated with the increasing volume of data breaches and malicious actors.

Enterprise Data Warehouse and Data Lake

3.71 Services Australia has two main data repositories for data and analytics purposes, the Enterprise Data Warehouse (EDW) and Data Lake, that hold personal information of its clients. The EDW is a central repository for data on shared service deliveries across the Centrelink, Medicare, and Child Support programs delivered by Services Australia. As of May 2025, there were 1,553 users registered for access to the EDW; 1,219 from Services Australia, and 334 from external entities.⁸⁶

3.72 A review undertaken by Services Australia in May 2024 found that, despite the roles and profiles assigned to users as access controls, Centrelink data in the EDW was not structured in such a way as to limit access to specific programs or payments, meaning that external users could potentially view personal information not relevant to their work. In response, Services Australia sought to 'bolster the agency's legal foundation and security infrastructure' through improvement of access controls and by 'establishing clear and defensible legal authority for data disclosure'.

3.73 Services Australia has sought to address this through the 'Enterprise Data Warehouse Uplift' project, due to be completed by June 2026. This includes issuing public interest certificates to support the sharing of data between Services Australia and policy agencies, primarily under the *Social Security (Administration) Act 1999*, *Student Assistance Act 1973*, *A New Tax System (Family Assistance) (Administration) Act 1999*, and *Paid Parental Leave Act 2010*. These certificates define the authorised uses of information and who in a given external entity can access and use the information, providing a framework under which external users and Services Australia can define obligations and limitations on access and seeks to provide coverage to Services Australia for ongoing inadvertent or inappropriate access risks.

Quality Call Framework

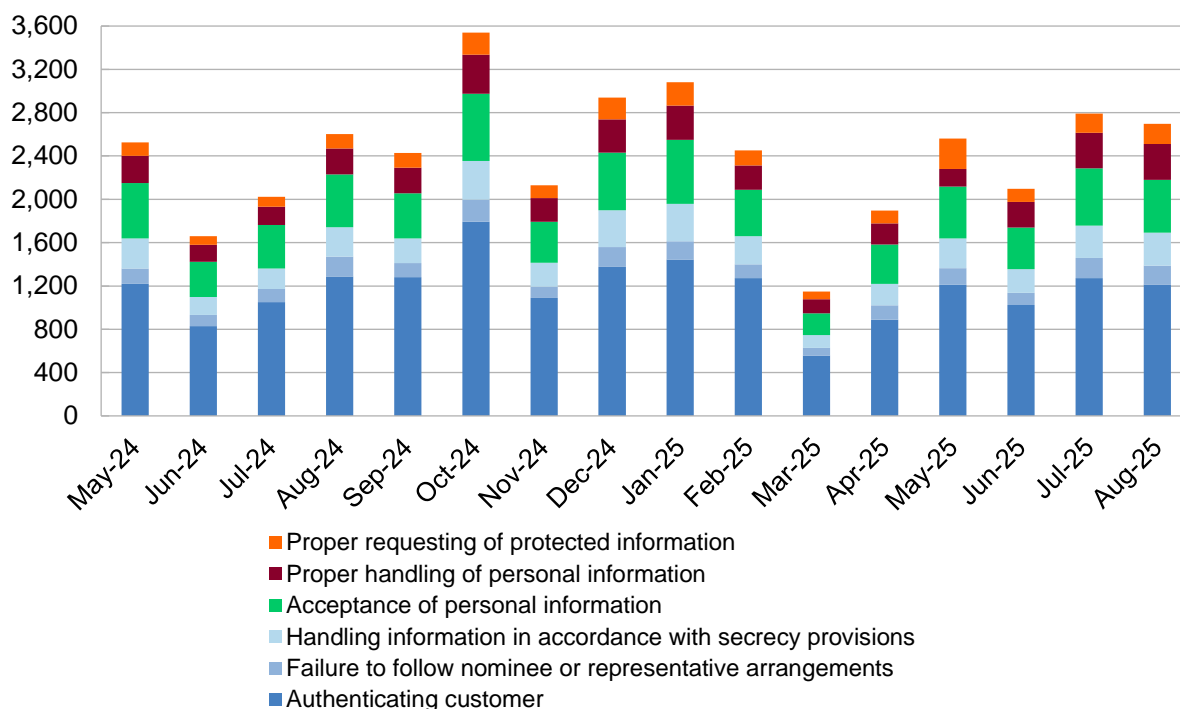
3.74 Services Australia monitors a sample of telephone interactions under its Quality Call Framework (QCF) program to assess whether officers meet standards in their interactions with clients, including in relation to privacy and secrecy requirements. In 2024–25, 282,465 calls were checked from a population of 44,269,308 inbound and 7,837,822 outbound calls.

3.75 The assessment of calls includes considerations of whether a client's 'privacy and secrecy [was] maintained throughout the call in accordance with relevant legislation' and whether there was the appropriate provision of a standardised privacy statement. Figure 3.7 shows that the largest

⁸⁶ Ten users were from the Department of Employment and Workplace Relations, 30 from the Department of Education, 24 from the Department of Health and Aged Care, 76 from the Department of Social Services, 113 from the Department of Veterans' Affairs, and 81 from the National Disability Insurance Agency.

causes of privacy errors were failure to properly authenticate clients' identities, and errors in accepting personal information.

Figure 3.7: Quality Call Framework checking: privacy and secrecy errors identified, May 2024 to August 2025



Note: The number of errors presented in this table is not equal to the number of calls which contained errors, as calls can be flagged for multiple errors.

Source: ANAO analysis of Services Australia data and internal reporting provided on the Services Australia intranet.

3.76 In quarter 1 of 2024–25, Services Australia registered 2,102 privacy incidents and identified 7,053 privacy and secrecy errors through QCF checking. This indicates that not all privacy and secrecy errors detected through QCF checking meet the threshold to be reported as privacy incidents. An error needs to be specifically identified as having a privacy component, where a potential breach could or did occur, to be recorded as a privacy incident. Services Australia advised the ANAO on 6 June 2025 that most errors which are also privacy incidents are events where a customer service officer failed to properly validate a client's identity.

3.77 Dashboards containing the QCF checking data are available on Services Australia's intranet and available to all staff; data is also shared with various team leaders across the organisation, as well as the Quality and Capability Committee who receive high-level analysis to inform them on overall trends.

Internal audit

3.78 Services Australia undertook 59 internal audits between July 2020 and June 2025. The ANAO identified 17 internal audits that assessed topics relevant to privacy practices, procedures and systems:

- seven internal audits made 15 recommendations for the management of privacy (see Table 3.2); and

- ten internal audits covered privacy-relevant topics (information communication technology, mandatory training, risk management plans, workforce capability and training, fraud control and debt management) but made no recommendations relating to privacy.

3.79 Table 3.2 summarises the ANAO's analysis of the status of privacy recommendations made in internal audits between July 2020 and April 2025.

Table 3.2: Internal audits finalised between July 2020 and June 2025 with privacy recommendations and their closure status as of June 2025

Report	Date	Number of privacy recommendations	Summary of recommendations	Status
External Access by Partner Agencies	July 2020	1	To strengthen the effectiveness of access controls	Closed
Effectiveness in Implementing Recommendations (Internal Audit and other)	June 2023	1	To improve the governance of implementing recommendations from OAIC privacy assessments	Closed
Data Matching for Concession Card Holders — PBS Programme	July 2023	1	To improve processes for personal information contained in emails	Open
Notifiable Data Breaches	September 2023	2	To improve oversight, monitoring and reporting to meet statutory requirements	Closed
Privacy — Updating Customer Details	April 2025	2	To ensure compliance with the Privacy law compliance checklist	Open
Customer Identity Management	April 2025	2	To improve processes and controls	Open
Management initiated review: Services Australia's Guidelines Relating to the Intertwinement of Customer Records in Medicare	April 2025	6	To implement governance, administrative, training and ICT solutions that remove causes for processing errors	Open

Source: ANAO analysis.

3.80 The review of Services Australia's guidelines relating to the intertwinement of client records in Medicare (April 2025) was initiated in response to the Australian Information Commissioner determination in 'ATQ' and CEO of Services Australia (23 January 2025).⁸⁷ This determination found that Services Australia had interfered with the privacy of a client because their Medicare records

⁸⁷ 'ATQ' and CEO of Services Australia (Privacy) [2025] AICmr 19 (23 January 2025), available from <https://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2025/19.html> [accessed 30 June 2025].

had become intertwined with those of another person. It directed Services Australia to undertake several steps to ensure that ‘the conduct is not repeated or continued’, including:

(ii) within 3 months of the determination, conduct a review which assesses the effectiveness of the Guidelines as they relate to the intertwining of customer records and the implementation of those Guidelines in practice, and produce a report containing the findings and recommendations arising from the review (review report);

(iii) provide the OAIC with a copy of the review report, together with a timeline for implementing any recommendations outlined in the review report, within 30 days of finalising the report;

3.81 Services Australia advised the ANAO in August 2025 that all six recommendations are expected to be implemented by 31 January 2026.

3.82 Services Australia also engaged an independent auditor as directed by the Privacy Commissioner in the determination ‘WZ’ and Chief Executive Officer of Services Australia (13 April 2021) to assess privacy practices, procedures and systems against APP 11 when de-linking Centrelink records of separated partners. The findings and recommendations of the independent audit are discussed in case study 2.

3.83 Between July 2020 and April 2025, Services Australia did not undertake an internal audit concerning the handling of personal information in the Centrelink, Medicare and Child Support programs, except in response to a direction from the Australian Information Commissioner (see case study 2). Services Australia has a high privacy risk profile, delivering complex public services and handling significant amounts of personal information. This requires ongoing assurance that the ‘reasonable steps’ Services Australia must take under the Privacy Act to protect personal information are commensurate with the risk profile and any changes in the risk environment.

Opportunity for improvement

3.84 Services Australia could include audits of the handling of personal information in Centrelink, Medicare and Child Support programs in its internal audit program.

Overarching approach to monitoring compliance with privacy obligations

3.85 Services Australia does not have an overarching strategy to assure compliance with the Privacy Act and APP Code. A privacy assurance strategy in operation with a privacy risk management plan (see recommendation 1) could support regular reviews of the privacy management plan, and support assurance of compliance with requirements for privacy threshold assessments (see paragraph 3.11), privacy impact assessments (see paragraph 3.20) and notifiable data breaches (see paragraph 3.60).

Recommendation no. 8

3.86 Services Australia implements a privacy assurance strategy to assess compliance with its privacy obligations.

Services Australia response: *Agreed.*

3.87 *Services Australia will incorporate a privacy assurance strategy statement in the next iteration of the Agency's Privacy Management Plan to provide confidence that the Agency's privacy initiatives and activities have been implemented and carried out as planned to adequately address the Agency's privacy obligations.*

Has Services Australia implemented recommendations from the Office of the Australian Information Commissioner?

Of the 13 recommendations made by the OAIC in three privacy assessments between 2020 and 2023, Services Australia has implemented nine, partially implemented two, and two recommendations were superseded by events.

3.88 The OAIC undertakes privacy assessments of entities regarding their management of personal information in accordance with the APPs. The OAIC published three privacy assessments relating to Services Australia between 2020 and 2023.

- Securing personal information: Services Australia (formerly Department of Human Services), data matching activities (20 July 2020).⁸⁸
- Handling of personal information Services Australia (formerly Department of Human Services) Annual Investment Income Report (AIIR) data matching program (15 January 2021).⁸⁹
- Handling personal information — Services Australia's role as the Identity Exchange (16 February 2023).⁹⁰

3.89 Services Australia agreed to implement all 13 recommendations from the three privacy assessments. Services Australia has largely implemented these recommendations. Two recommendations were partially implemented with no documentation of risk assessment,

88 OAIC, *Securing personal information: Services Australia (formerly Department of Human Services), data matching activities*, 20 July 2020, available from <https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-assessments/securing-personal-information-services-australia-formerly-department-of-human-services-data-matching-activities> [accessed 20 May 2025].

89 OAIC, *Handling of personal information Services Australia (formerly Department of Human Services) Annual Investment Income Report (AIIR) data matching program*, 15 January 2021, available from <https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-assessments/handling-of-personal-information-services-australia-formerly-department-of-human-services-annual-investment-income-report-aiir-data-matching-program> [accessed 20 May 2025].

90 OAIC, *Handling personal information: Services Australia's role as the Identity Exchange*, 16 February 2023, available from <https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-assessments/handling-personal-information-services-australias-role-as-the-identity-exchange> [accessed 20 May 2025].

processes and details for managing risk to reflect current practice. Appendix 5 summarises the ANAO analysis of implementation of recommendations.

3.90 The closure of OAIC recommendations, including sign-off by an appropriate governance committee and appropriate recording of the decision, has improved over time. In November 2023, Services Australia implemented a Privacy Risk Recommendations Implementation Framework.

- The recommendations made in the report *Handling of personal information: Services Australia's role as the Identity Exchange* (16 February 2023) were closed by the Enhanced myGov and Digital Identity (EMDI) Delivery Board on 27 June 2023. The implementation of the five recommendations made in this report was timely and the closure appropriately recorded.
- The recommendations from two earlier OAIC privacy assessments were not closed by an appropriate committee. Services Australia advised the OAIC of the closure of these recommendations in response to OAIC follow-up over two years after the publication of the OAIC report.

3.91 Case study 2 outlines how Services Australia responded to a determination from the Australian Information Commissioner and Privacy Commissioner.

Case study 2. Addressing Family and Domestic Violence (FDV) risks arising from separating partners

On 13 April 2021, the Australian Information Commissioner and Privacy Commissioner (the Privacy Commissioner) made a determination⁹¹ that Services Australia had interfered with the complainant's privacy by disclosing the complainant's new address to her former partner, in breach of APPs 6, 10.2 and 11.1. The Privacy Commissioner stated:

The nature of this personal information was such that if its quality was not ensured, the individual would be subject to adverse consequences. The adverse consequence being risk of exposing her personal information to the former partner. This is particularly the case for an individual who had claimed to experience domestic violence and had produced an AVO [Apprehended Violence Order] to the Agency. As such, I consider that more rigorous steps were required to ensure that individuals fearing domestic violence do not have their updated addresses disclosed to their former partner.

The Privacy Commissioner declared that Services Australia must pay the complainant \$19,980 in compensation, undertake an independent audit to assess its policies, procedures and systems for partner separation against the requirements of APP 11, and inform the Privacy Commissioner of that audit report and implementation of recommendations.

Services Australia engaged EY to undertake the independent audit, 'Handling of personal information — Services Australia, linkage of partner records (APP 11)', which was finalised on 3 November 2021. The independent audit reported that there were 141,821 Centrelink clients who transitioned from 'Partnered' to 'Separated' during 2020–21. The report identified a range of positive practices and deficiencies, noting that:

91 'WZ' and Chief Executive Officer of Services Australia (Privacy) [2021] AICmr 12 (13 April 2021), available from <https://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/12.html> [accessed 21 November 2024].

[T]he internal practices, procedures and systems to de-link customer records across Centrelink, Medicare and Child Support are complex. There are multiple tasks that may need to be performed by the customer separately across Centrelink, Medicare, and Child Support to protect their personal information from unauthorised access by their former partner. This process becomes more complex for vulnerable customers affected by FDV [Family and Domestic Violence] because the timing and completion of all tasks are important to help protect the customer's safety.

There were 18 recommendations, all accepted by Services Australia, including updating training, risk assessments, operational blueprints and system controls. Services Australia tracked implementation of recommendations and reported progress to the OAIC.

In response to one recommendation, Services Australia developed a new operational blueprint, Separating safely — protecting personal details, in June 2022.

In April 2025, EY undertook an internal audit to assess the effectiveness of controls implemented from the 2021 independent audit. This report identified that there was increased use of operational blueprints relating to privacy, including more than 60,000 uses of the separating safely operational blueprint. The internal audit made three recommendations that were accepted by Services Australia.

On 8 October 2025, the government introduced the Regulatory Reform Omnibus Bill 2025, which includes provisions for Services Australia to share information within the agency for the purposes of administering the Centrelink, Medicare and Child Support programs.



Dr Caralee McLiesh PSM
Auditor-General

Canberra ACT
2 December 2025

Appendices

Appendix 1 Entity responses

Services Australia



Our Ref: EC25-002203

Chief Executive Officer
David Hazlehurst

Dr Caralee McLiesh PSM
Auditor-General for Australia
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601


Dear Dr McLiesh

**Services Australia's response to the Australian National Audit Office's performance audit
*Managing the privacy of client information in Services Australia***

Thank you for providing Services Australia (the Agency) with the opportunity to comment on the Australian National Audit Office's (ANAO) performance audit, *Managing the privacy of client information in Services Australia*.

The Agency welcomes the report and notes the report recommendations aimed at further strengthening the Agency's management of privacy.

Protecting privacy is a key part of the Agency's core business and promotes trust and confidence in the Agency to deliver government services to all Australians. The Agency actively promotes a culture of valuing and protecting information.

The Services Australia Privacy Policy is published on the Agency's website and provides information to the general public about how we manage our customer's personal information. The Privacy Policy is regularly updated, including for accessibility and readability and when the Agency implements new programs or changes to processes that affect the way we collect, handle, store, use and disclose information.

Privacy awareness is strengthened across the Agency through a range of education and training initiatives, targeted awareness activities and insights gained from privacy incident reviews. Quarterly Privacy Reports are tabled at the Agency's Security Committee, with relevant matters escalated to the Executive Committee, ensuring executive oversight of privacy risk.

Privacy risk is a feature in relevant business plans with responsible business areas managing privacy risk and incidents. Additionally, the Agency undertakes proactive assurance and pressure testing activities relating to privacy, fraud and security of information.

PO Box 7788, Canberra Business Centre ACT 2610 | www.servicesaustralia.gov.au

The Agency's Privacy Contact Officer Network embeds privacy contact officers at branch-level across all key business areas in the Agency, reporting directly to SES managers on privacy risk and linking directly to the Agency's Privacy Officers and Privacy Champion.

The Agency is committed to ensuring that people are aware of their right to privacy and provides avenues for customer feedback, including privacy complaints. Information on feedback and complaints is available on the Agency's website.

I would like to thank the ANAO for its cooperative and professional approach throughout the audit process.

Yours sincerely



David Hazlehurst

24 November 2025

Attorney-General's Department



Australian Government
Attorney-General's Department

Secretary

25 November 2025

Dr Caralee McLiesh PSM
Auditor-General for Australia
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Caralee.McLiesh@anao.gov.au

Dear Auditor-General

Thank you for providing the Attorney-General's Department (the department) with the opportunity to comment on the Australian National Audit Office's (ANAO's) proposed audit report on Managing the privacy of client information in Services Australia.

The department and our relevant portfolio agency, the Office of the Australian Information Commissioner (OAIC), appreciate the engagement with the ANAO during the audit process. This audit represents an important opportunity to consider the potential for improvements to the legal frameworks and processes governing the handling of Australians' personal information, in particular, government-related identifiers and Tax File Numbers.

The department supports the Attorney-General to administer the *Privacy Act 1988* (Privacy Act), and notes the importance of all regulated entities maintaining strong protections for Australians' personal information in accordance with the Privacy Act. I note Government agencies such as Services Australia are also subject to the Australian Government Agencies Privacy Code, which has a key objective of enhancing the privacy capability and accountability of agencies.

I note the three recommendations which pertain to the department's responsibility for the Privacy Act, including the Notifiable Data Breaches scheme. Attached to this letter is the department's summary response (Annexure A) and responses to recommendations (Annexure B). These constitute the department's formal response to the Auditor-General's proposed report.

Please contact Ms Celeste Moran, First Assistant Secretary, Identity and Information Division (Celeste.Moran@ag.gov.au) if you would like to discuss this response.

Yours sincerely

A handwritten signature in blue ink, appearing to read 'Katherine Jones'.

Katherine Jones PSM

3-5 National Circuit, Barton ACT 2600 Telephone (02) 6141 6666 www.ag.gov.au ABN 92 661 124 436

Department of Finance



Australian Government
Department of Finance

Matt Yannopoulos PSM
Secretary

Our Ref: EC25-001925

Dr Caralee McLiesh PSM
Auditor-General for Australia
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Dr McLiesh *Caralee,*

I refer to the Australian National Audit Office's (ANAO's) correspondence dated 28 October 2025 providing an extract of the proposed audit report, *Managing the privacy of client information in Services Australia*, pursuant to section 19 of the *Auditor-General Act 1997* and seeking the Department of Finance's (Finance's) response.

Thank you for the opportunity to respond to the matters raised in the extract. Finance's summary response to the extract is:

The Department of Finance notes the findings in the report extract.

I note that ANAO and Finance officials have consulted closely since the extract was received, resulting in the text of the relevant recommendation (Recommendation 5) being redrafted as follows:

2.121 There is limited reporting to the Australian Parliament by Australian Government entities on their compliance with the Privacy Act 1988. Entities are not required to report in annual reports on their management of privacy. The Attorney-General's Department, in consultation with the Department of Finance as required, consider advice to the Australian Government on options to improve the transparency of entities' compliance with the Privacy Act 1988.

Finance's response to the redrafted Recommendation 5 is as follows:

One Canberra Avenue, Forrest ACT 2603 • Telephone 02 6215 3445
Internet www.finance.gov.au

The Department of Finance agrees to the recommendation and welcomes the opportunity to work with the Attorney-General's Department to consider appropriate mechanisms to strengthen the transparency of Commonwealth entities' compliance with the Privacy Act 1988.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Matt', with a stylized flourish at the end.

Matt Yannopoulos PSM
Secretary

19 November 2025

Department of Social Services



Australian Government
Department of Social Services

Michael Lye
Secretary

Ref: EC25-002689

Dr Caralee McLiesh PSM
Auditor-General for Australia
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

OfficeoftheAuditorGeneralPerformanceAudit@anao.gov.au

Dear Dr McLiesh

Thank you for your correspondence of 28 October 2025 and for the opportunity to comment on the proposed Australian National Audit Office (ANAO) audit report 'Managing the privacy of client information in Services Australia'. I respond to Recommendation 4 as relevant to the Department of Social Services (the Department). The Department recognises the importance of this audit and appreciates the efforts and insights of the independent auditors.

The Department appreciates the opportunity that Recommendation 4 presents in evaluating and enhancing the existing data-matching frameworks, ensuring these are modernised to reflect current technologies and evolving data-matching practices.

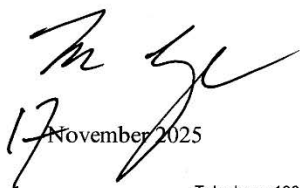
To ensure an arm's length consideration of data-matching activities undertaken by Services Australia and other government entities, the Department suggests Recommendation 4 should be managed by an independent reviewer or Australian Government entity not directly involved in data matching covered by the Audit. The Department is ready to provide support to the review should it go ahead.

As the administrator of the *Data-matching Program (Assistance and Tax) Act 1990*, the Department is committed to progressing any legislative or other change recommendations that may result from an independent review.

A summary of the Department's response and the editorial matters for proposed corrections of fact that the Department wishes to bring to the ANAO's attention are at **Attachment A**.

If you would like further information regarding this response, please contact Kayelle Drinkwater, acting Group Manager and Chief Data Officer, Data and Evaluation Group, at Kayelle.Drinkwater@dss.gov.au.

Regards


17 November 2025

GPO Box 9820 Canberra ACT 2601
Telephone 1300 653 227 • National Relay Service: TTY: 133 677, Speak and listen: 1300 555 727
Internet relay: www.relayservice.com.au
www.dss.gov.au

Office of the Australian Information Commissioner



Australian Government
Office of the Australian Information Commissioner

Our reference: D2025/029274

Dr Caralee McLiesh PSM
Auditor-General for Australia
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

By email: officeoftheauditorgeneralperformanceaudit@anao.gov.au

Response under s 19 of the *Auditor General Act 1997* – Managing the privacy of client information in Services Australia

Dear Auditor-General

I refer to your email of 28 October 2025 attaching an extract of the proposed audit report on ‘Managing the privacy of client information in Services Australia’ (Report). This letter sets out the Office of the Australian Information Commissioner’s (OAIC) formal reply to the Report.

As requested, my Office has separately provided the Australian National Audit Office with our summary response and responses to each of the recommendations to appear in the body of the Report.

The OAIC, as the independent privacy regulator, was provided with excerpts of the Report relating to:

- privacy risks arising from third-party data breaches, and
- data matching frameworks.

Third-party data breaches involving Services Australia customer identifiers

The OAIC agrees in principle that it would be beneficial for Services Australia to be notified of relevant third-party data breaches to enable Services Australia to take action to prevent future breaches and carry out its functions. Such arrangements could require legislative reform, which is a matter for Government.

If a new reporting obligation is to be imposed, it will be necessary to specify the entities to which the requirement applies and the threshold for notification. For example, consideration should be given to whether the obligation rests with third parties to directly notify Services Australia.

1300 363 992
oaic.gov.au/enquiry

T +61 2 9942 4099
F +61 2 6123 5145

GPO Box 5288
Sydney NSW 2001

www.oaic.gov.au
ABN 85 249 230 937

OAIC

The OAIC is not notified of all data breaches involving Services Australia or individual identifiers. The Notifiable Data Breaches scheme imposes a mandatory requirement on entities regulated under the *Privacy Act 1988* (Cth) (Privacy Act) to notify the OAIC if a data breach is likely to result in serious harm to an individual. Not all entities are subject to the Privacy Act and not all data breaches will meet the threshold for notification.

Data matching frameworks

The OAIC has a limited assessment and monitoring role in relation to the data matching activities under the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) (pursuant to the Privacy Act). We also administer the voluntary *Guidelines on data matching in Australian Government administration* (Voluntary Guidelines).

Data matching activities potentially create significant privacy impacts for individuals. It is important that these activities are conducted in compliance with privacy obligations, and that agencies conducting data matching programs consider and manage the privacy impacts of those programs during the program development.

The OAIC notes the Report's concerns around the suitability of current data matching frameworks. A review of the Voluntary Guidelines is currently underway and will include consultation with relevant agencies. Any review of the Privacy Act and the *Data-matching Program (Assistance and Tax) Act 1990* would be a matter for Government.

Please let us know if you have any queries regarding the above or wish to discuss any aspect of the Report further.

Yours sincerely



Elizabeth Tydd

Australian Information Commissioner

21 November 2025

Appendix 2 Improvements observed by the ANAO

1. The existence of independent external audit, and the accompanying potential for scrutiny improves performance. Improvements in administrative and management practices usually occur in anticipation of ANAO audit activity; during an audit engagement; as interim findings are made; and/or after the audit has been completed and formal findings are communicated.
2. The Joint Committee of Public Accounts and Audit (JCPAA) has encouraged the ANAO to consider ways in which the ANAO could capture and describe some of these impacts. The ANAO's corporate plan states that the ANAO's annual performance statements will provide a narrative that will consider, amongst other matters, analysis of key improvements made by entities during a performance audit process based on information included in tabled performance audit reports.
3. Performance audits involve close engagement between the ANAO and the audited entity as well as other stakeholders involved in the program or activity being audited. Throughout the audit engagement, the ANAO outlines to the entity the preliminary audit findings, conclusions and potential audit recommendations. This ensures that final recommendations are appropriately targeted and encourages entities to take early remedial action on any identified matters during the course of an audit. Remedial actions entities may take during the audit include:
 - strengthening governance arrangements;
 - introducing or revising policies, strategies, guidelines or administrative processes; and
 - initiating reviews or investigations.
4. In this context, the below actions were observed by the ANAO during the course of the audit. It is not clear whether these actions and/or the timing of these actions were planned in response to proposed or actual audit activity. The ANAO has not sought to obtain assurance over the source of these actions or whether they have been appropriately implemented.
 - On 11 February 2025, Services Australia published an updated privacy policy and a closed-circuit television (CCTV) privacy notice on its website describing the circumstances where it collects and uses CCTV video and still images (see paragraph 2.60).
 - In July 2025, Services Australia advised the ANAO that it had instructed its external legal advisor — who is undertaking a review of legislation and other instruments related to data matching — to also consider the *Data-matching Program (Assistance And Tax) Act 1990* (see paragraph 2.92).
 - Services Australia advised the ANAO on 30 July 2025 that it is aware of the revocation of the National Archives General Disposal Authority 24 in 2019 and is in the process of developing a data disposal policy for the Centrelink and Child Support Single Touch Payroll (STP) Phase 2 data matching program (see paragraph 2.101).
 - The ANAO's initial analysis of the OAIC's data for FOI requests for personal information showed an increase in Services Australia's refusal rate from Q1 2024–25. The OAIC's guidance for FOI reporting states that entities should not include 'deemed refusals' (those not processed within statutory timeframe) in reports of refused FOI requests. Services Australia advised the ANAO on 19 June 2025 that it had included deemed refusals. In July 2025, Services Australia advised the ANAO that it was revising the data and had identified 726 FOI matters potentially incorrectly reported. As of 19 September 2025, Services Australia data on the OAIC website had been corrected (see paragraph 2.71).

Appendix 3 Services Australia privacy management plan attribute maturity targets and assessments

1. Table A.1 shows Services Australia's self-assessment against each of the 21 maturity attributes in the privacy management plan framework. The four levels are initial, developing, defined and leader (see paragraphs 2.2 to 2.10).

Table A.1: Services Australia privacy management plan attribute maturity targets and assessments, 2022–23 to 2025–26

	2022–23 PMP		2023–24 PMP		2024–25 PMP		2025–26 PMP	
Attributes	Maturity assessment for prior financial year	Maturity target for coming financial year	Maturity assessment for prior financial year	Maturity target for coming financial year	Maturity assessment for prior financial year	Maturity target for coming financial year	Maturity assessment for prior financial year	Maturity target for coming financial year
Access and Correction	Leader ✓	Sustain at Leader	Leader ✓	Sustain at Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to leader
Assurance Model	Leader ✓	Sustain at Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to leader
Awareness	Defined ✖	Sustain at Defined	Defined ✓	Improve to Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to leader
Complaints and Enquiries	Defined ✖	Improve to Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to leader
Data breach Notification	Leader ✓	Sustain at Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to leader
Privacy Incident and Data Breach Response Plan	Leader ✓	Sustain at Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to leader
Data Quality Processes	Defined ✓	Sustain at Defined	Defined ✓	Improve to Leader	Defined ✖	Sustain at Defined	Defined ✓	Sustain at defined
Dealing with Suppliers	Defined ✖	Sustain at Defined	Defined ✓	Improve to Leader	Defined ✖	Sustain at Defined	Defined ✓	Sustain at defined
External Privacy Policy and Notices	Defined ✓	Sustain at Defined	Defined ✓	Improve to Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to leader
Information Security Processes	Leader ✓	Sustain at Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to leader

	2022–23 PMP		2023–24 PMP		2024–25 PMP		2025–26 PMP	
Attributes	Maturity assessment for prior financial year	Maturity target for coming financial year	Maturity assessment for prior financial year	Maturity target for coming financial year	Maturity assessment for prior financial year	Maturity target for coming financial year	Maturity assessment for prior financial year	Maturity target for coming financial year
Internal Policies and Procedures	Defined ✖	Sustain at Defined	Defined ✔	Improve to Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to leader
Inventory of Personal Information	Defined ✔	Sustain at Defined	Defined ✔	Improve to Leader	Defined ✖	Sustain at Defined	Defined ✔	Improve to leader
Management and Accountability	Defined ✖	Sustain at Defined	Defined ✔	Improve to Leader	Defined ✖	Improve to Leader	Leader ✔	Sustain at leader
Privacy Champion	Defined ✖	Sustain at Defined	Defined ✔	Improve to Leader	Leader ✔	Sustain at Leader	Leader ✔	Sustain at leader
Privacy Impact Assessments	Defined ✖	Sustain at Defined	Defined ✔	Improve to Leader	Defined ✖	Sustain at Defined	Defined ✔	Sustain at defined
Privacy Management Plan	Defined ✔	Sustain at Defined	Defined ✔	Improve to Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to leader
Privacy Officer	Defined ✖	Sustain at Defined	Defined ✔	Improve to Leader	Defined ✖	Improve to Leader	Leader ✔	Sustain at leader
Privacy Training	Defined ✖	Improve to Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to leader
Privacy Values	Defined ✔	Sustain at Defined	Defined ✔	Improve to Leader	Defined ✖	Improve to Leader	Defined ✖	Improve to leader
Reporting and Escalation	Defined ✖	Improve to Leader	Defined ✖	Improve to Leader	Defined ✖	Sustain at Defined	Defined ✔	Sustain at defined
Risk Identification and Assessment	Defined ✔	Sustain at Defined	Defined ✔	Improve to Leader	Defined ✖	Sustain at Defined	Defined ✔	Sustain at defined

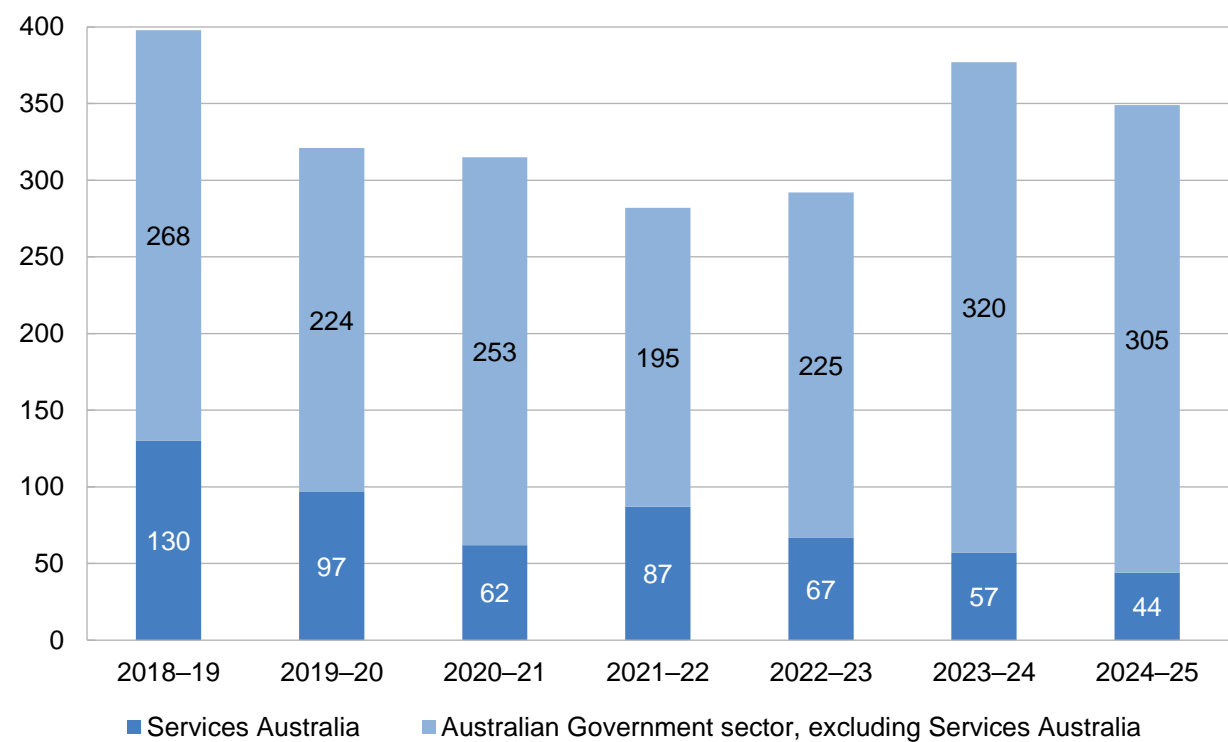
Key: A tick (✔) indicates that the maturity assessment met the prior-year PMP target. A cross (✖) tick indicates that the target was not met.

Source: ANAO analysis of Services Australia's privacy management plans, 2022–23 to 2025–26. Services Australia assessed against the Privacy Program Maturity Assessment Framework, from OAIC, *Interactive PMP Explained*, July 2018, page 24, available from <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/government-agencies/australian-government-agencies-privacy-code/interactive-privacy-management-plan> [accessed 22 January 2025].

Appendix 4 Complaints made to the Office of the Australian Information Commissioner

1. Figure A.1 shows the number of complaints made to the Office of the Australian Information Commissioner (OAIC) regarding Services Australia, and the remaining Australian Government sector. This data was provided by the OAIC and does not differentiate between complaints made specifically about privacy or about other matters for which the OAIC may oversee (see paragraph 3.46 for further discussion).

Figure A.1: Complaints made to the OAIC relating to Services Australia and the Australian Government sector, 2018–19 to 2024–25














Source: ANAO analysis of OAIC data.

Appendix 5 Implementation of OAIC recommendations

1. Table A.2 summarises the ANAO's analysis of Services Australia's implementation of 13 recommendations from the three Office of the Australian Information Commissioner (OAIC) privacy assessments published between 2020 and 2023 (see paragraphs 3.88 to 3.90).

Table A.2: ANAO analysis of the implementation status recommendations from three OAIC privacy assessments

Report and summary of recommendations	ANAO assessment of implementation
Securing personal information: Services Australia (formerly Department of Human Services), data matching activities (20 July 2020)	
1. That Services Australia regularly reviews its cyber security policy documents to ensure that they are up-to-date and accurately reflect current practices.	
2. That Services Australia: <ul style="list-style-type: none"> conducts risk-based assessments of whether hard disks of database servers holding personal information should be encrypted and whether internal traffic between web servers and databases should be encrypted. If Services Australia decides not to implement encryption, then it should also include in its risk assessment the alternative approaches to managing the risks associated with non-implementation documents the processes and outcomes of these considerations shares the record of personal information holdings, maintained by Services Australia's Operational Privacy Section, with the Cyber Security Branch to ensure that appropriate protections are applied to this information 	 No documentation of risk assessment
3. That Services Australia: <ul style="list-style-type: none"> considers introducing dedicated workstations for privileged users performing privileged tasks, particularly for privileged users with high levels of administrative access considers implementing multi-factor authentication for all users, and especially for privileged users documents the processes and decisions and/or includes details of alternative approaches to managing the risks associated with non-implementation of certain Information Security Manual controls. 	 No documentation of processes and decisions and details of alternative approaches
4. That Services Australia establishes formal communication channels between the Cyber Security and Privacy teams, including documenting the relationship between the two areas and the roles and responsibilities of each area in the event of a cyber security incident or eligible data breach.	
Handling of personal information Services Australia (formerly Department of Human Services) Annual Investment Income Report (AIIR) data matching program (15 January 2021)	
1. That Services Australia reviews its risk management processes for the AIIR program to ensure that all privacy and information security risks are appropriately monitored, identified, treated, recorded and reported to senior management.	Not assessed Recommendation superseded by events ^a

Report and summary of recommendations	ANAO assessment of implementation
2. That Services Australia regularly reviews and revises its cyber security policy documentation, such as the Cyber Security Incident Response (CSIR) Plan, to ensure that they are up-to-date, and accurately reflect current practices and language used in the Privacy Act.	
3. That Services Australia reviews and updates its privacy documentation to formalise the relationship between the Privacy and Cyber Security teams, as well as roles and responsibilities of each area, in the event of an eligible data breach or cyber security incident.	
4. That Services Australia, as part of its scheduled review of the AIIR program protocol, identifies if any additional information should be included in the protocol, consistent with the department's obligations under APP 1.2 and the OAIC's Guidelines on Data Matching in Australian Government Administration (Data Matching Guidelines). Should these details be considered sensitive in nature, the OAIC suggests that Services Australia considers also creating an internal, more detailed version of the protocol for auditing, monitoring and quality control purposes.	Not assessed Recommendation superseded by events ^a
Handling personal information — Services Australia's role as the Identity Exchange (16 February 2023)	
1. Amend Services Australia's privacy policy by adding information which clarifies Services Australia's role, and that the role involves handling personal information.	
2. Identify and document Services Australia's specific and measurable digital identity system (DIS) / trusted digital identity framework privacy goals and targets by either amending Services Australia's general privacy management plan or developing a separate plan.	
3. Develop an internal policy that clearly documents the separation of Services Australia's DIS functions and the privacy measures which apply to the Identity Exchange.	
4. Take appropriate steps to manage risks identified in the security assessments of the Identity Exchange.	
5. Test Services Australia's data breach response plan in relation to the Identity Exchange.	

Key:  Implemented  Partially implemented  Not implemented

Note a: Services Australia advised the OAIC on 18 September 2023 that the data matching program is indefinitely on hold and the OAIC accepted this advice.

Source: ANAO analysis of OAIC and Services Australia documents.

OAIC, *Securing personal information: Services Australia (formerly Department of Human Services), data matching activities*, 20 July 2020, available from <https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-assessments/securing-personal-information-services-australia-formerly-department-of-human-services.-data-matching-activities> [accessed 20 May 2025]

OAIC, *Handling of personal information Services Australia (formerly Department of Human Services) Annual Investment Income Report (AIIR) data matching program*, 15 January 2021, available from <https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-assessments/handling-of-personal-information-services-australia-formerly-department-of-human-services-annual-investment-income-report-aiir-data-matching-program> [accessed 20 May 2025]

OAIC, *Handling personal information: Services Australia's role as the Identity Exchange*, 16 February 2023, available from <https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-assessments/handling-personal-information-services-australias-role-as-the-identity-exchange> [accessed 20 May 2025].