Australian Government
Department of Home Affairs

Department of Home Affairs submission to the Inquiry into the management of client privacy in the Australian public sector

Joint Committee of Public Accounts and Audit

15 May 2026

Table of Contents

Inquiries Submission

Introduction

The Department of Home Affairs (the department) welcomes the opportunity to provide a submission to the Joint Committee of Public Accounts and Audit (the Committee) on its *Inquiry into the management of client privacy in the Australian public sector.*

The purpose of the submission is to provide an overview of the department's framework for managing and monitoring compliance with privacy obligations under the *Privacy Act 1988* (Privacy Act) and Australian Government Agencies Privacy Code (APP Code), and for maintaining client privacy information. The submission also demonstrates the department's approach to responding to data breaches, cyber threats and malicious actors.

Arrangements to manage privacy

The department has an established Privacy Operations Section to support the protection of client information across the entire organisation. As required by the APP Code, the department has a Privacy Champion and Privacy Officer.

The Privacy Operations Section is an established point of contact for the wider department to assist in processing privacy matters in accordance with its privacy obligations under the Privacy Act and the APP Code.

These privacy matters include but are not limited to:

- establishing and actioning a Privacy Management Plan which is reviewed annually
- supporting the wider department in undertaking Privacy Impact Assessments (PIAs) (which are published on the department's website) and actioning recommendations
- developing, implementing, reviewing and testing the department's Data Breach Response Plan (annually)
- contributing to the development of policies and procedures to address the handling of personal information tailored to specific clients of the department
- developing, reviewing, updating and publishing the department's Privacy Policy and departmental Privacy Notice (Form 1442i), annually and as required. Both of these are published on the department's website
- reviewing departmental policies to ensure processes appropriately address and comply with privacy obligations
- embedding the requirement for business areas to consult with the Privacy Operations Section when considering new projects and processes
- developing regular department wide privacy related communications and a dedicated Privacy SharePoint page with resources and guidance
- developing and delivering privacy training for the wider department on both an annual and as needed basis
- developing e-learning courses on the handling of personal information, with courses available as part of induction training and as stand-alone training packages
- investigating and responding to privacy complaints
- assessing suspected privacy breach incidents and reporting to the Office of the Australian Information Commissioner (OAIC) as per the requirements of the Notifiable Data Breach scheme, and
- stakeholder engagement to support ongoing monitoring of the wider department's privacy maturity.

Implementation of arrangements to manage the privacy of client information

Privacy Impact Assessments and Privacy Management Plans

The department undertakes privacy threshold assessments (PTAs) for projects involving new or changed ways of handling personal information. High risk projects are required to undertake a PIA. This consultation process has been embedded into the department's overarching project management framework. The department maintains a public PIA register on the department's website, which is updated regularly, and maintains an internal register of all PTAs and PIAs completed by the department.

The department develops a Privacy Management Plan in accordance with section 9 of the APP Code on an annual basis which is used to assess the department's overall privacy risk maturity profile across five elements including governance and culture, privacy strategy, privacy processes, risk and assurance and data breach responses.

The department publishes a Privacy Policy and Privacy Notice (Form 1442i) which is reviewed and updated annually, and as required. The department also has a privacy notice template which is used by program areas to create specific privacy notices relevant to their areas. The overarching Privacy Policy outlines the complaint mechanisms available to individuals when seeking to make a complaint regarding the department's handling of personal information. The Privacy Operations Section is responsible for managing and reporting all privacy related complaints received by the department.

Compliance with the Privacy Act in relation to privacy complaints and notifiable data breaches

The Privacy Operations Section is also responsible for investigating, managing and remediating privacy incidents and determining whether the incident constitutes a Notifiable Data Breach (NDB). The department has procedures in place outlining the breach reporting process, including taking reasonable steps to contain a breach, completing a suspected privacy breach form to determine whether any further containment measures, training, reporting or notification are required. The Privacy Operations Section also provides recommendations to mitigate future privacy incidents, including further training, developing a prevention plan or updating processes.

Under the NDB scheme the department has 30 days to assess whether an incident is likely to result in serious harm and, if so, to notify the OAIC and the affected individual/s. The department complies with the NDB notification requirements and notifies the OAIC. The department also notifies the affected individual/s and provides support to manage the incident. The department has developed a Data Breach Response Plan which incorporates OAIC guidance, to assist in the identification and reporting of privacy incidents and NDBs. Internal reporting of privacy incidents also occurs at the executive level.

Use of notifiable data breach and privacy complaint data

The department maintains a centralised register for recording privacy complaints and incidents, this data is used to inform and develop training programs, address procedural, system and staff capability issues and develop resources and guidance material for staff. It is also used to assess risk, identify trends and support continuous improvement in privacy controls and practices.

The department has a range of internal controls and assurance processes in place, including user access monitoring, internal audits, staff training and compliance activities, and the internal publishing of policies, processes and procedures ensuring consistent staff guidance and privacy obligations are clearly understood.

Integrated privacy and cyber governance

The Privacy Operations Section works closely with the department's cyber and security teams to identify, manage and resolve incidents involving client information. This partnership strengthens our privacy oversight, allowing us to quickly contain threats, assess the impact on client data, and coordinate efforts in managing data-related incidents.

The Department also has responsibility for developing policy on cyber security and driving forward implementation of the Government's *2023-2030 Australian Cyber Security Strategy.* Under the Strategy the Department is working across Government to explore policy options and initiatives to better protect data from unauthorised access and to uplift cyber resilience across the economy. The Department's focus is on Government and critical infrastructure sectors which run and maintain systems that all Australians rely on.

Overarching approach to monitoring compliance with privacy obligations and ensuring compliance with Privacy Act/Code

The Privacy Operations Section conducts regular progress reviews against the Privacy Management Plan and uses reporting data to assess and support assurance of compliance for the requirements of the NDB scheme, PTAs, PIAs and ongoing privacy obligations. The Section fosters continued stakeholder engagement to support ongoing monitoring of the wider department's privacy maturity.

Number of notifiable data breaches, by financial year, since 2022-23, including method of identification

Year	No. of NDBs	Method of identification
2022-23	12	Staff and business area self-reporting suspected incidents with final assessment made by the Privacy Operations Section.
2023-24	6	Staff and business area self-reporting suspected incidents with final assessment made by the Privacy Operations Section.
2024-25	26	Staff and business area self-reporting suspected incidents with final assessment made by the Privacy Operations Section. One identification by the Privacy Operations Section through media reporting of an incident.
2025-26*	8	Staff and business area self-reporting suspected incidents with final assessment made by the Privacy Operations Section.

*Number as of 17 April 2026

The increase in notification of NDBs during the 2024-25 FY coincides with the implementation of a privacy awareness and training campaign indicating an increased awareness of privacy obligations amongst staff and improved reporting processes.

Summary

The department thanks the Committee for the opportunity to make a submission to the *Inquiry into the management of client privacy in the Australian public sector*. The department is committed to protecting client privacy through strong governance, effective compliance measures, and continuous improvement. We recognise the importance of safeguarding personal information and actively work to ensure our privacy practices meet legislative requirements, manage risks, and maintain public trust.