Australian Government
Department of Foreign Affairs and Trade

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

INQUIRY INTO THE MANAGEMENT OF CLIENT PRIVACY IN THE AUSTRALIAN PUBLIC SECTOR

May 2026

INTRODUCTION

The Department of Foreign Affairs and Trade (DFAT) thanks the Joint Committee of Public Accounts and Audit (Committee) for the opportunity to provide a submission to this important inquiry.

DFAT has a diverse range of functions, including delivering Australia's foreign, trade and development policy, providing consular assistance to Australians overseas, issuing Australian passports and supporting Australia's international engagement through a network of overseas posts and domestic offices.

In undertaking these functions, DFAT collects, holds, uses and discloses significant volumes of personal information relating to members of the Australian public, including passport and consular information. DFAT also manages personal information relating to employees, locally engaged staff, contractors, grant and scholarship applicants and recipients, tenderers and suppliers, individuals connected with foreign arrangements, and foreign nationals engaged through diplomatic, trade, development and mobility programs.

DFAT recognises the sensitivity of the personal information it handles and the trust placed in it by the public. DFAT is committed to strong privacy governance, transparency and continuous improvement in the management of personal information.

TABLE OF CONTENTS

1 ARRANGEMENTS TO MANAGE PRIVACY

1.1 Governance and oversight arrangements

DFAT has mature privacy governance arrangements supported by a strong culture of compliance. Oversight is led by DFAT's Privacy Champion (the Chief Counsel), supported by designated Privacy Officers and a specialist Privacy Team within the Legal Division.

Privacy governance is overseen through established accountability structures, including biannual reporting to DFAT's Executive Board and its external Audit and Risk Committee. Privacy performance and emerging risks are also reported biannually to the Privacy Champion, with statistics proactively published in DFAT's Annual Report to promote transparency.

DFAT's policy framework also addresses privacy risks associated with third-party service providers. Standard contracting templates include privacy clauses requiring compliance with Australian privacy law, cooperation in managing privacy incidents and prompt reporting of actual or suspected breaches to DFAT.

1.2 Risk assessments

DFAT assesses itself as having a high privacy risk profile due to the scale and sensitivity of personal information handled through its consular, passport and related functions.

Privacy risk identification and assessment are embedded within DFAT's broader enterprise risk management framework. Privacy risks are explicitly recognised in DFAT's Risk Management Policy and are incorporated into divisional and overseas post risk registers to ensure risks are considered in the context of local operating environments and service delivery activities. This approach supports early identification of emerging risks and promotes shared accountability for managing privacy risks across DFAT.

New projects or changes to existing processes that involve the handling of personal information are subject to Privacy Threshold Assessments (PTAs) to determine whether they present a high privacy risk and whether a Privacy Impact Assessment (PIA) is required. Where projects are assessed as presenting a high privacy risk, PIAs are undertaken to identify and assess potential privacy impacts and to develop mitigation strategies that support privacy-by-design.

Privacy risks are also assessed through DFAT's privacy breach management processes in accordance with DFAT's Privacy Breach Response Plan (PBRP). All suspected or actual privacy incidents are centrally assessed to determine their root causes, severity and risk of potential harm to individuals. These assessments inform remedial action, targeted training, system or process changes and broader risk mitigation strategies. Trend analysis of breaches and complaints is used to identify recurring risk drivers, particularly those associated with human error in high-volume operational areas.

In addition, DFAT's compliance with the *Privacy Act 1988* forms part of DFAT's annual Legislative Compliance Assurance Process (LCAP), which includes independent assessment of DFAT's compliance assurance arrangements. Findings from LCAP, together with insights from internal audit activity and external oversight bodies are used to inform privacy risk assessments and to strengthen controls over time.

Through this layered and integrated approach, DFAT seeks to ensure that privacy risks are identified early, assessed proportionately, escalated appropriately and managed in a manner commensurate with DFAT's risk profile and community expectations.

1.3 Policies to manage the privacy of client information

DFAT maintains a comprehensive suite of policies, procedures and operational guidance to support appropriate handling of personal information.

DFAT's publicly available Privacy Policy explains how personal information is collected, used, disclosed and stored; how individuals may access or correct their personal information held by DFAT; and how privacy complaints are handled. The policy is reviewed and updated regularly, most recently in February 2026.

Operational guidance materials provide staff with practical direction, promote consistent decision-making and support the embedment of privacy-by-design across DFAT. These materials are readily accessible to all staff on a dedicated privacy intranet page.

A central element of the framework is DFAT's Privacy Breach Response Plan (PBRP), which establishes a whole-of-department approach to managing actual or suspected privacy breaches. The PBRP sets out roles, responsibilities, escalation pathways and notification criteria and applies to all staff and contracted service providers. It emphasises early containment, harm mitigation and consistency of response.

The PBRP is supported by Standard Operating Procedures for Responding to Common Privacy Breaches, providing scenario-based guidance on incidents most frequently encountered in operational environments.

Together, these policies provide a structured and proportionate framework for managing client privacy and maintaining public trust.

1.4 Education and training arrangements

Education and training are central to DFAT's privacy management approach and to embedding a strong culture of privacy awareness.

Privacy training is mandatory for all staff and contractors on commencement and annually thereafter. Staff undertaking overseas postings or supporting the delivery of DFAT's passport functions must also complete specific privacy training addressing heightened risks in overseas crisis and passport processing environments.

DFAT has developed tailored privacy training videos covering key obligations under the *Privacy Act 1988*, the management of privacy breaches and the operation of PTAs and PIAs. Training is practical and operationally focused, supporting early risk identification and application of privacy-by-design principles.

The Privacy Team delivers targeted training to high-risk areas such as the Australian Passport Office and the Consular and Crisis Management Division, focusing on common risk scenarios, recent incidents and practical safeguards.

In June 2025, DFAT arranged for the Australian Government Solicitor to present a bespoke training session entitled 'Privacy Law Reforms: What You Need to Know', covering the amendments to the *Privacy Act 1988* introduced in late 2024. The session was recorded and all staff were encouraged to attend the session or view the video, which continues to be available for viewing.

DFAT participates in the Office of the Australian Information Commissioner's (OAIC) Privacy Awareness Week campaign each year. This normally involves whole-of-department communication pieces (such as all-staff emails from the Privacy Champion, posters and lock screens) and targeted updates to DFAT's senior executive.

DFAT's dedicated privacy intranet page serves as a central repository for policies, training videos, guidance, templates and contact information.

1.5 Monitoring and reporting arrangements

Monitoring of privacy compliance is undertaken centrally by the Privacy Team within the Legal Division, which maintains oversight of privacy incidents, complaints, enquiries, PTAs and PIAs. Incidents are recorded and assessed to determine causes, severity and required remediation. Incidents and outcomes are recorded in a matter management database, allowing for generation of statistics and reports. This information supports trend analysis, targeted training and system improvements.

Privacy reporting is integrated into DFAT's broader governance framework, with biannual reporting to the Privacy Champion, Executive Board and Audit and Risk Committee. Significant or systemic issues are escalated promptly through established channels, including through arrangements set out in the PBRP.

DFAT supports transparency by voluntarily publishing privacy statistics, including substantiated breaches, complaints and notifiable data breaches, in its Annual Report.

Monitoring is further supported through the LCAP, internal audits and periodic reviews of privacy governance artefacts. Insights are incorporated into reporting and used to inform updates to policies, procedures and training.

2 IMPLEMENTATION OF ARRANGEMENTS TO MANAGE THE PRIVACY OF CLIENT INFORMATION

2.1 Privacy Impact Assessments and Privacy Management Plan

DFAT has established structured processes to meet its obligations under the *Privacy (Australian Government Agencies — Governance) APP Code 2017* (APP Code), including requirements to undertake PIAs for high-privacy-risk projects and to maintain a current Privacy Management Plan (PMP).

PTAs are required to be completed by business areas and assessed by the Privacy Team for all projects involving new or changed ways of handling personal information.

These processes are centrally managed by the Privacy Team and the processes are communicated through the dedicated privacy intranet page, which includes resources such as FAQ documents and templates. DFAT has also created a bespoke training video providing all staff with guidance on the PTA and PIA process, supporting early and consistent consideration of privacy risks.

Where a project is assessed as high privacy risk, a PIA is undertaken by an external provider and recorded in DFAT's publicly available PIA register.

DFAT maintains an annually reviewed PMP, approved by the Privacy Champion, documenting DFAT's privacy governance framework, risk profile, maturity assessment outcomes and improvement actions. The PMP is published on the privacy intranet page to promote transparency and shared accountability.

2.2 Compliance with the *Privacy Act 1988* – complaints and notifiable data breaches

DFAT has centrally coordinated arrangements to ensure compliance with the *Privacy Act 1988*, including processes for handling privacy complaints and assessing actual or suspected data breaches, including potential notifiable data breaches (NDBs).

The PBRP provides a whole-of-department framework for responding to actual or suspected privacy breaches, including providing guidance on roles, reporting requirements, escalation pathways and notification criteria. Staff and contracted service providers must promptly report suspected or actual breaches, enabling early containment, investigation and assessment of harm.

Standard Operating Procedures for Responding to Common Privacy Breaches provide scenario-based guidance on incidents such as misdirected emails, document loss, unauthorised access, third-party incidents and malicious cyber activity.

The Privacy Team centrally assesses all incidents to determine whether they constitute a privacy breach and whether they meet the NDB threshold. Where required, DFAT notifies the OAIC and affected individuals. DFAT may also notify the OAIC and affected individuals even where the threshold is not met, to support transparency and harm mitigation.

DFAT's Privacy Policy outlines how individuals may lodge privacy complaints with DFAT or the OAIC. Internal Privacy Complaint Handling Procedures, which are documented and published on DFAT's privacy intranet page, ensure complaints are referred to the Privacy Team, assessed independently and responded to in writing.

2.3 Use of data on privacy complaints and notifiable data breaches

Information from complaint handling and breach assessment processes is centrally recorded, enabling a whole-of-department view of privacy performance and emerging risks. The Privacy Team conducts trend analysis to identify systemic issues and reports insights through established governance channels.

Aggregated privacy data and information about NDBs is regularly reported to the Privacy Champion, Executive Board and Audit and Risk Committee, supporting informed decision-making and prioritisation of privacy initiatives.

Outcomes of breach assessments are used to strengthen preventative controls, update guidance and deliver targeted training, particularly in areas handling large volumes of personal or sensitive information. DFAT's Privacy Team has also used the outcome of assessments to inform privacy breach response simulations with key business areas, building resilience and readiness for future breaches.

2.4 Assurance arrangements

DFAT has a layered assurance framework for managing client privacy and compliance with the *Privacy Act 1988* and the APP Code, aligned with the three lines of defence model.

First-line assurance is provided by business areas responsible for complying with privacy policies, completing PTAs (for assessment by the Privacy Team), implementing PIA recommendations and reporting breaches. Operational processes are supported by system controls, access management and mandatory training.

Second-line assurance is provided by the Privacy Team, which oversees privacy governance, reviews PTAs and PIAs, assesses breaches and complaints, advises on NDB obligations, undertakes trend analysis and reports to senior governance forums. The PMP provides a structured mechanism to assess the effectiveness of privacy practices annually.

Third-line assurance is provided through internal audit and the annual LCAP, which includes independent assessment of compliance arrangements under the *Privacy Act 1988*. DFAT also considers findings from external bodies such as the OAIC, the Australian National Audit Office and parliamentary committees. Recent improvements include the establishment of a Privacy Contact Officer Network within the Australian Passport Office (a measure discussed in the Auditor-General Report No.12 2025–26 Performance Audit titled "Managing the Privacy of Client Information in Services Australia".

Together, these arrangements provide assurance that privacy risks are effectively managed and that lessons learned are embedded across DFAT.

3 OVERARCHING COMPLIANCE APPROACH

3.1 *Privacy Act 1988*

DFAT adopts a comprehensive, risk-based approach to compliance with the *Privacy Act 1988*, reflecting the scale and sensitivity of the information it manages. Compliance is embedded across governance arrangements, operational practices, training and assurance activities.

Central coordination within the Legal Division provides authoritative advice (which can be supplemented by external legal advice where required), oversees complaints and breaches and supports consistent interpretation of obligations. DFAT gives effect to its obligations through a suite of policies, controls and mandatory training, supported by clear escalation pathways and access to specialist advice.

Operational compliance is reinforced through day-to-day practices, with particular emphasis on timely identification and management of breaches. DFAT also employs a range of organisational and technical controls, including role-based access controls and ICT safeguards.

Privacy complaints are handled through documented procedures that support fair, timely and independent assessment, with complaint data used to inform systemic improvements.

Transparency underpins DFAT's approach. DFAT engages constructively with oversight bodies and voluntarily publishes privacy statistics in its Annual Report, supporting public confidence and continuous improvement.

3.2 *Privacy (Australian Government Agencies – Governance) APP Code 2017*

Compliance with the APP Code is embedded in DFAT's privacy governance framework through defined roles, documented processes and regular oversight.

DFAT maintains a documented PMP, reviewed regularly and approved annually by the Privacy Champion, in accordance with the APP Code. The PMP is published on the privacy intranet page to promote transparency and accountability.

DFAT has appointed Privacy Officers and a senior executive SES Band 2 Privacy Champion. These roles provide leadership, specialist advice and coordinated oversight of privacy risks, complaints and breaches.

DFAT undertakes PTAs for early privacy risk identification and has established documented processes to ensure that PIAs are conducted for all high-risk privacy projects. DFAT also maintains a publicly available PIA register. Ongoing monitoring, staff training and reporting arrangements support compliance with Parts 3 and 4 of the Code.

Through these measures, DFAT maintains clear governance, systematic assessment of privacy impacts and ongoing monitoring to support sustained compliance with the APP Code.

4 NOTIFIABLE DATA BREACHES SINCE 2022-23

Financial Year	Number of NDBs	Method of Identification
2022–23	1	Identified through internal privacy breach reporting and assessment processes
2023–24	0	N/A
2024–25	1	Identified through internal privacy breach reporting and assessment processes
2025–26 (to 28 April 2026)	0	N/A

5 CONCLUSION

DFAT recognises that effective management of personal information is critical to maintaining public trust. Given the scale and sensitivity of the information it holds, DFAT places strong emphasis on robust governance, clear accountability, staff capability and proportionate controls to manage privacy risks and meet its obligations under the *Privacy Act 1988* and the APP Code.

DFAT remains committed to continuous improvement, using data, assurance activities and lessons learned from incidents, complaints and assessments to strengthen controls and enhance staff awareness. DFAT will continue to engage constructively with oversight bodies and adapt its privacy arrangements in response to evolving risks, reforms and community expectations.