Australian Government

Department of Social Services

**Bronwyn Worswick**
Chief Counsel

Committee Secretary
Joint Committee of Public Accounts and Audit
PO Box 6021
Parliament House
CANBERRA ACT 2600
Email: jcpaa@aph.gov.au

Dear Committee Secretary

**SUBMISSION TO JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT – INQUIRY INTO CLIENT PRIVACY IN THE AUSTRALIAN PUBLIC SECTOR**

Please find attached the Department of Social Services' submission to the Joint Committee of Public Accounts and Audit inquiry into client privacy in the Australian public sector.

The department welcomes the opportunity to contribute to the Committee's examination of privacy risk management, information handling and incident response across the public sector, and appreciates the Committee's focus on practical application, accountability and continuous improvement in this area.

The department also thanks the Committee for the extension of time provided to submit its response by 22 May 2026.

Should the Committee require any further information or clarification in relation to the submission, the department would be pleased to assist.

Yours sincerely

Bronwyn Worswick
Chief Counsel
22 May 2026

Australian Government
Department of Social Services

# Submission to the Joint Committee of Public Accounts and Audit

## Inquiry into Client Privacy in the Australian Public Sector

Department of Social Services

**May 2026**

# Contents

Executive Summary ..... 2

Department's Privacy Risk Profile ..... 2

Inquiry's Terms of Reference ..... 4

Recommendations ..... 4

Response to the Terms of Reference ..... 5

Accountability, Visibility and Design: Frameworks used to identify and manage privacy risks, and meet the requirements of the *Privacy Act 1988 (Cth)* ..... 5

Incident learning - Effective management of privacy incidents, data breaches, cyber threats, and malicious actors ..... 8

System capability and application - Matters contained in and associated with ANAO Report No. 12 of 2025-26 ..... 11

Closing Statement ..... 14

Additional References ..... 16

# Executive Summary

The department welcomes the opportunity to contribute to the Joint Committee of Public Accounts and Audit (the Committee) inquiry into the management of client privacy in the Australian public sector (Inquiry).

The department is responsible for policy, programs and statutory schemes that rely on the use of personal information to deliver services, support decision-making and inform government outcomes. While strong privacy frameworks are in place, their application in practice is shaped by how information is used across different functions and arrangements, and where responsibilities and decision-making intersect.

This submission focuses on how privacy risks are identified, managed, responded to and understood in practice across complex operational environments. It draws from operational experience, external observations, and broader system insights to support the Committee's examination of client privacy across the public sector. This submission does not revisit the policy settings of the *Privacy Act 1988* (Cth) (Privacy Act) or Australian Privacy Principles (APPs). It focuses on how those settings operate in practice, particularly where responsibilities intersect and information is handled across multiple arrangements, and where constraints may arise despite established frameworks.

The department's experience points to a consistent theme—privacy frameworks are well-established, but their application can vary where responsibilities intersect, where judgement is required, and where information is handled across multiple arrangements. These conditions shape how effectively risk is identified, understood and managed. This is directly relevant to the matters under examination, including the identification and management of privacy risk, the response to incidents and emerging threats, enterprise visibility of risk, and the broader operational themes highlighted in recent audit activity. Based on this experience, five areas are identified where further attention could support more consistent and effective outcomes:

- strengthen accountability across shared arrangements,
- strengthen enterprise visibility of privacy risk,
- strengthen integration of privacy considerations into operational design,
- strengthen sector wide visibility and learning from privacy incidents and complaints, and
- strengthen practical guidance for complex and high-sensitivity environments.

Taken together, these areas reflect where existing arrangements can be strengthened to better support decision-making, oversight, operational visibility and consistent application in practice.

# Department's Privacy Risk Profile

**Operating context**

The Social Services Portfolio, led by the department, is responsible for policy, programs and statutory schemes that support individuals, families and communities across Australia.[1] This work relies on the

[1] The Social Services Portfolio comprises the Department of Social Services, the Domestic, Family and Sexual Violence Commission, the National Commission for Aboriginal and Torres Strait Islander Children and Young People, and the Australian Institute of Family Studies. The Department is also responsible for administering the National Redress Scheme for Survivors of Institutional Child Sexual Abuse.

collection and use of personal information, often highly sensitive in nature and connected to trauma, financial hardship, family and domestic violence, and other forms of vulnerability. In many cases, this information is also subject to specific legislative protections beyond the Privacy Act.[2]

**Legislative and delivery complexity**

Privacy risk is influenced by the breadth of the legislative framework. Obligations arise not only under the Privacy Act, but also through program specific legislation, secrecy provisions and policy settings that govern how information can be handled. While these frameworks provide a common baseline, they do not always align neatly in an operational context, particularly where information is used for multiple purposes across different programs and functions.

The department's risk profile is also shaped by how services are delivered. Personal information is not managed within a single organisational boundary. It is used across policy development, program administration, and service delivery, and often handled through shared arrangements with other entities and external providers.

This operating model reflects the broader structure of the Social Services Portfolio, where policy responsibility, program administration and service delivery may operate across different entities, systems, and governance arrangements.

**Evolving risk environment**

In this context, risk reflects how information moves between functions and entities, how it is used for service delivery, compliance, and policy purposes, and how decisions are made in practice. While the same legal framework applies, interpretation, capability and risk tolerance can differ.

The department has established governance, policy and assurance frameworks to manage these risks, supported by ongoing efforts to strengthen capability, improve information handling practices, and reduce unnecessary exposure. However, the overall risk profile is not determined by the absence of, or gaps within, these frameworks. Rather, it is shaped by the challenge of applying multiple, and at times inconsistent frameworks consistently in practice—particularly where responsibilities intersect, information is shared across arrangements, and decisions rely on judgement. In this context, privacy risk is dynamic and requires a system-wide perspective, rather than being managed in isolation within individual programs.

Further detail on the Portfolio's operating environment and approach to privacy management is available through publicly released materials including prior submissions, annual reports, and published privacy policies.[3] This summary focuses on what is most relevant to the Committee's inquiry.

[2] For example, personal information may also be 'protected information' subject to information handling requirements under the *National Redress Scheme for Institutional Child Sexual Abuse Act 2018* (Cth), the *Social Security Act 1991* (Cth) and the *Child Support (Assessment) Act 1989* (Cth).
[3] See 'Additional References' at page 16 below.

## Inquiry's Terms of Reference

On 9 April 2026, the Committee adopted an inquiry into the management of client privacy in the Australian public sector (the inquiry). As part of the inquiry, the Committee will examine:

- the frameworks used to identify and manage privacy risks, and meet the requirements of the Privacy Act, in public sector entities that manage information on private individuals,
- the ability of public sector entities holding personal information to respond effectively to data breaches, cyber threats, and malicious actors, and
- any matters contained in and associated with Auditor-General Report No. 12 of 2025-26: *Managing the Privacy of Client Information in Services Australia* (ANAO Report).

The Terms of Reference focus on how entities identify and manage privacy risk, how they respond to breaches and threats, and the issues highlighted in recent audit activity. Recent findings from the ANAO's Report provide a practical reference point. The ANAO Report indicates that the issue is not the absence of frameworks, but how consistently they are applied in practice.

The department's experience reflects similar pressures. Privacy risk is often managed within individual programs or functions, while responsibility, information handling and decision-making extend across different areas and entities. This can make it harder to see where risk is building, to apply controls consistently and to draw insight from incidents beyond the immediate response. These factors inform the department's view that the challenge is not in establishing frameworks or inadequacies in existing frameworks, but in how they operate in practice. The observations and recommendations in this submission are directed to that point.

The Committee invited the department to make a submission.

# Recommendations

The observations below do not seek to restate established privacy obligations or existing guidance. They reflect areas where applying those frameworks consistently in practice can become more challenging across shared, interconnected or evolving operating environments. The recommendations focus on opportunities to strengthen accountability, visibility of risk and practical application across the system.

1. **Strengthen accountability across shared arrangements.**

   Information handling responsibilities are often distributed across functions, systems, or entities, making end-to-end visibility of privacy risk more difficult in practice. Stronger alignment between accountability, oversight and operational handling would support more consistent escalation, assurance, and decision-making across shared environments.

2. **Strengthen enterprise visibility of privacy risk.**

   Privacy risks are often managed within individual programs, activities, or operational areas, while broader patterns and interdependencies can be harder to identify across the system. Stronger enterprise-level visibility would support earlier identification of emerging issues and more consistent oversight across interconnected environments.

3. **Strengthen integration of privacy considerations into operational design.**

   Operational models, information flows, and delivery arrangements are often established early in design processes. More consistent integration of privacy considerations at these early stages would support stronger implementation across complex operating environments.

4. **Strengthen sector wide visibility and learning from privacy incidents and complaints.**

   Privacy incidents and complaints can provide important insight into how controls operate in practice and where pressures or recurring issues may be emerging. However, broader visibility across the public sector remains limited, particularly for incidents that fall outside formal reporting thresholds. More structured sharing and analysis of incident and complaint information would support stronger system-wide learning, earlier identification of trends and more proactive risk management.

5. **Strengthen practical guidance for complex and high-sensitivity environments.**

   Some operating environments involve overlapping legislative obligations, sensitive information and decisions that depend heavily on context and judgment. Applying general privacy principles consistently in these situations can become more difficult where information is shared across multiple parties, systems or arrangements. More practical guidance grounded in real world scenarios would support stronger and more consistent decision-making across complex environments.

# Response to the Terms of Reference

## Accountability, Visibility and Design: Frameworks used to identify and manage privacy risks, and meet the requirements of the *Privacy Act 1988 (Cth)*

### Operating environment and information handling

The department handles personal information across a broad range of functions connected to social policy, program administration and statutory schemes. This includes grants administration, public consultation and engagement activities, complaints and review processes, and delivery of programs involving highly vulnerable individuals, for example, the National Redress Scheme.

Information may be collected directly by the department, provided through applications and assessment processes, received from other Commonwealth entities or through shared service delivery arrangements and external providers. Depending on the context, the same information may support policy development, program oversight, service delivery, assurance activities, compliance processes or legal obligations.

The department's operating environment also involves structured information sharing and reporting arrangements across funded organisations, government entities and shared delivery environments. In some cases, policy responsibility, operational administration, and service delivery functions operate

across different entities or portfolio arrangements. Information may therefore be collected, accessed, shared, or relied upon by multiple parties for related but distinct purposes.

These arrangements require information handling activities to operate across interconnected systems and legislative frameworks while maintaining clear oversight, consistent protections, and effective coordination between entities. Recent machinery of government changes, including the transfer of Services Australia and NDIS related responsibilities to different portfolios have altered aspects of governance and oversight across parts of the broader operating environment. However, information handling and operational activities continue to operate across interconnected arrangements requiring ongoing coordination, visibility, and assurance.

**Legislative and operational complexity**

The department manages information within multiple legislative and operational frameworks. In addition to the Privacy Act and the APPs, some information is also subject to secrecy provisions and program specific legislative protections that affect how information can be collected, used, disclosed, and shared. These frameworks do not always align neatly in practice. Applying legislative obligations consistently can require careful assessment where:

- information relates to vulnerable individuals,
- responsibilities intersect across entities,
- multiple legislative obligations apply to the same information, and
- operational decisions rely heavily on context and judgments.

The operating environment is also increasingly digital and interconnected. Information may move across systems, reporting platforms and shared delivery environments involving Commonwealth entities, contracted providers and funded organisations. This increases the importance of maintaining consistent governance, practice controls, and visibility of risk across operational environments.

**Privacy governance and assurance**

The department identifies and manages privacy risks through a combination of enterprise risk management processes, privacy specific governance arrangements, operational controls and assurance activities. Privacy risk management is integrated into the department's broader enterprise governance framework and considered alongside information security, cyber security, and fraud risks to support a coordinated and proportionate control environment.

The department maintains a suite of governance documents and operational materials to support compliance with the Privacy Act, the APPs, the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Privacy Code) and Notifiable Data Breaches Scheme (NDB Scheme). These include:

- Privacy Policy,
- Privacy Management Plan,
- Data Breach Response Plan (DBRP),
- Personal Information Holdings Register,
- operational guidance and templates, and
- staff instructions and training materials.

These documents are reviewed regularly to assess privacy maturity, operational effectiveness and areas requiring capability uplift or refinements.

Governance and reporting arrangements are in place to support executive oversight of privacy risks and obligations. This includes reporting through senior executive governance forums and oversight by a dedicated Privacy Champion, supported by senior Privacy Culture Leads across work areas. These arrangements are intended to improve visibility of privacy risks, support consistent messaging, and strengthen privacy capability across the department.

**Operational controls and workforce capability**

Privacy considerations are incorporated into policy development, program design and operational activities through privacy assessments and broader risk management processes. The department continues to strengthen its approach to data minimisation and information handling at the point of design. This includes ongoing consideration of:

- what information is collected,
- whether collection remains necessary and proportionate,
- how information is retained and shared,
- whether unnecessary exposure can be reduced, and
- how access controls and de-identification measures can reduce risk.

The department seeks to support privacy protection through proportionate collection practices, de-identification processes, role-based access controls, and structured reporting arrangements where appropriate. For example, the Data Exchange framework supports program reporting and outcomes measurement while reducing collection of unnecessary personal information through de-identified reporting arrangements.

Privacy risks are identified at various stages of a program or activity lifecycle. In practice this includes:

- policy development and program design,
- implementation of new systems or activities,
- operational delivery and information sharing arrangements,
- ongoing assurance and reporting activities, and
- review of incidents, complaints, and emerging risks.

The department recognises that workforce capability is critical to protecting client privacy and supporting consistent information handling practices. Staff are required to comply with privacy and confidentiality obligations as part of their employment and complete mandatory privacy training. Additional guidance and targeted training are provided to higher-risk or data-intensive work areas where specialised handling requirements apply. This includes dedicated guidance and training for staff working in the National Redress Scheme, where information may involve sensitive personal histories and protected information subject to additional legislative controls.

Operational controls are also supported through contractual arrangements and assurance activities where information is handled by other entities, including funded organisations and service providers. These arrangements may include requirements relating to privacy compliance, confidentiality

obligations, incident identification and reporting, and engagement with the department in managing privacy incidents or complaints.

The department also continues to consider how privacy protections can be maintained as digital capability, automation and emerging technologies evolve, including through ongoing review of data handling practices and minimisation approaches.

**Visibility of risk across interconnected environments**

The department's framework provides a structured basis for identifying and managing privacy risk. However, applying these arrangements consistently in practice can become more complex where responsibilities, systems and information handling activities intersect across multiple environments. While governance and accountability arrangements may formally allocate responsibilities, maintaining clear operational visibility of privacy risk can become more difficult where information handling activities occur across multiple systems, entities or functions. This can affect how emerging issues are identified, understood, and escalated across interconnected environments.

Similarly, privacy risks are often assessed at the level of individual programs or initiatives. While this supports local decision-making, it does not always provide a complete view of how risks intersect or accumulate across activities. Emerging pressures may therefore not always be readily visible beyond the point at which they arise.

The department also recognises the importance of embedding privacy considerations as early as possible during policy and operational design. While privacy assessments and related processes are undertaken, there can be practical limitations where key aspects of operational design, system functionality or information use have already been established before privacy issues are fully examined.

These pressures do not reflect an absence of framework or governance. Rather, they arise from applying established obligations within complex operating environments involving shared responsibilities, interconnected systems, evolving technologies, and multiple legislative requirements.

The department's recommendations are directed to these broader operational challenges. They focus on strengthening accountability across shared arrangements, improving visibility or privacy risk across interconnected activities, supporting earlier integration or privacy considerations into operational design, and enhancing practical application of privacy obligations across complex environments.

## Incident learning - Effective management of privacy incidents, data breaches, cyber threats, and malicious actors

**Incident learning, response capability, and emerging threats**

The department maintains established arrangements to identify, assess and respond to privacy incidents, complaints, and data breaches, including those arising from malicious or intentional activity. These arrangements are designed to support timely containment, minimise harm to affected individuals, maintain continuity of services and meet obligations under the Privacy Act and the NDB Scheme. Documented procedures are in place to support:

- identification and escalation of suspected incidents,
- containment and risk assessment,
- remediation and recovery activities,
- notification obligations where required, and
- review of lessons learned and control improvements.

Privacy incident management is integrated with broader information security, cyber security, and fraud control arrangements, allowing incidents to be escalated and managed according to their nature, severity, and potential impact. In practice, incidents can arise from a range of sources, including:

- human error,
- system failures,
- inappropriate access or handling of information,
- activity by external actors, including cyber enabled threats, and
- handling arrangements involving third parties or shared delivery environments.

The department's experience is that many incidents arise through operational handling issues and human error, including misdirected communications, access issues, or breakdowns in process controls. At the same time, the department recognises the evolving threat environment and the importance of maintaining appropriate controls and response capability in relation to cyber security risks, malicious actors, and unauthorised access attempts.

Preventative and detective controls are applied across the information lifecycle, including access controls, monitoring arrangements, system security measures, and escalation pathways appropriate to risk. The department also undertakes periodic testing of incident response arrangements, including its DBRP, and uses incident reviews to improve guidance, training, templates and operational controls over time.

**Shared arrangements and third-party handling**

As noted above, some information is managed through shared arrangements involving funded organisations, external providers or other government entities. In these situations, effective incident management can require coordination across multiple areas or parties. To support these environments contractual or assurance arrangements are used to establish expectations relating to:

- privacy compliance,
- secure information handling,
- incident identification and reporting,
- cooperation during investigations and remediation activities, and
- escalation and engagement where notification obligations may arise.

These arrangements are intended to support more consistent management of privacy risks across interconnected operational environments.

**Visibility of incidents and sector wide learning**

Public reporting under the NDB Scheme provides useful visibility of Eligible Data Breaches (EDBs) and common incident categories, including malicious or criminal activity, human error and system fault. Reporting by the Office of the Australian Information Commissioner indicates that malicious or criminal activity remains a significant contributor to EDBs nationally, while human error also continues to be a substantial source of incidents. However, the department's experience is the EDBs represent only part of the broader privacy risk landscape. Many privacy incidents fall outside notification thresholds, such as:

- lower-level handling errors,
- near misses,
- access issues,
- delays in escalation,
- incidents involving third parties,
- incidents that do not result in or do not present a risk of serious harm, and
- operational issues resolved before notification obligations arise.

While these matters may not require formal notification, they can still provide important insight into how controls operate in practice, where operational pressures exist and how risks emerge across different environments. These lower-level incidents, near misses and complaints can also act as early indicators of control weakness or emerging operational issues before more significant incidents occur.

This creates limitations in understanding the broader privacy risk landscape across the public sector. Agencies can learn from their own incidents and complaints but there is limited visibility of:

- the overall volume and nature of incidents across entities,
- recurring operational pressures or control weaknesses,
- how incidents and complaints are resolved and mitigated,
- where risks arise more commonly through human error, system issues, shared arrangements, or malicious activity, and
- common themes emerging across sectors or delivery environments.

The department's experience is that stronger outcomes depend on more structured use of incident, complaint and assurance information. Looking across incidents and complaints collectively rather than individually can support earlier identification of recurring issues, strengthen preventative controls, and improve consistency of response across operational areas. The department also considers that timely escalation and effective internal coordination are important to maintaining visibility of emerging issues. Where incidents and complaints are not escalated early or remain isolated within operational areas, broader patters, system pressures, or recurring weaknesses may be more difficult to identify in a timely way.

**Continuous improvement and emerging risks**

The department continues to invest in strengthening its response capability through:

- targeted training and awareness activities,
- ongoing review of incident response arrangements,

- integration of lessons learned into guidance and controls,
- increased focus on near misses and complaint trends, and
- strengthen coordination across privacy, cyber security, and fraud functions.

Internal incident and complaint information is also used to identify areas requiring additional support, guidance or capability uplift. This may include targeted engagement with higher-risk operational areas, refinement of controls, or updates to training materials and response procedures. The department's experience is that incident and complaint trends can also help identity broader operational pressures that may contribute to increased risk, including workload pressures, constrained timeframes, or weaknesses in process application.

The department recognises that privacy risk continues to evolve alongside increasing digital retention, interconnected systems and emerging technologies. While no control environment eliminates risk entirely, continued focus on operational learning, visibility of emerging pressures and practical application of controls remains important to strengthening privacy risk management over time.

These observations support the department's recommendation to strengthen sector wide visibility and learning from privacy incidents and complaints. A more structure approach to collecting and analysing incident and complaint information across the public sector would support better identification of recurring issues, emerging pressures, and opportunities for practical improvement across agencies and delivery environments.

## System capability and application - Matters contained in and associated with ANAO Report No. 12 of 2025-26

The department acknowledges the findings and observations outlined in the ANAO Report, which examined aspects of client information management, privacy risks, and related control environments within the Australian public sector.

The ANAO Report reinforced the importance of maintaining enterprise-level visibility of privacy and information handling risks across complex operational environments, particularly where activities, systems or responsibilities intersect. More broadly, the ANAO Report highlighted that the key challenge is not necessarily the existence of governance frameworks or controls, but how effectively information about risk, assurance and control performance are brought together, understood and applied in practice.

The department has considered these observations within its own operating environment and has undertaken targeted activities to strengthen governance, oversight, assurance and operational visibility of privacy and information handling.

**Governance, accountability, and visibility of risk**

Consistent with the broader themes of the audit, the department has reviewed and refined governance arrangements to support clearer executive oversight of privacy, information security, and broader handling risks. Privacy risks continue to be integrated into broader enterprise risk management processes, supported by escalation and reporting pathways to senior leadership.

Greater emphasis has also been placed on improving visibility of risks and controls effectives across operational activities, rather than considering issues only within individual programs or functions.

The department has strengthened reporting arrangements to support more structured executive visibility of:

- incidents and complaints,
- emerging risks and operational pressures,
- assurance findings,
- control effectiveness, and
- areas requiring capability uplift or management attention.

This includes quarterly reporting to senior executives on privacy matters in accordance with the Privacy Code. The department's experience is that governance frameworks are most effective when assurance information, incident trends and operational insights are considered collectively to support decision-making, prioritisation, and early identification of emerging issues across activities.

**Identification and management of privacy risks**

Emphasis was placed on the importance of identifying and managing privacy and information handling risks early and consistently across policy development, program design, and service delivery activities. This includes consideration of risks associated with:

- increased data sharing,
- interconnected systems,
- digital service delivery,
- operational handling environments, and
- shared delivery arrangements.

The department has also reviewed the alignment between privacy risk assessments, operational controls, and broader information security measures to support a more integrated and coordinated approach to risk management. These activities are intended to improve visibility of risk across operational environments and support earlier identification of issues where responsibilities, systems or information handling activities intersect.

**Controls, assurance, and operational uplift**

The findings also drew attention to the role of effective controls and assurance mechanisms in supporting compliance with legislative and policy requirements and in maintaining confidence that controls are operating effectively in practice. The department has undertaken targeted reviews of relevant controls and assurance processes, including access management arrangements, monitoring, and incident detection mechanisms, reporting and escalation pathways, and internal review and assurance activities.

Greater emphasis has also been placed on how information from incidents, complaints and assurance activities is analysed and used to inform operational improvements, rather than being considered in isolation. This includes using operational insights to:

- refine guidance and procedures,

- strengthen controls,
- identify recurring issues or operational pressures, and
- support more targeted capability uplift activities.

The department has also established processes to monitor implementation of improvement activities arising from assurance work and relevant observations from the ANAO Report through existing governance forums and reporting mechanisms.

**Workforce capability and professional judgement**

Workforce capability and consistent application of obligations in practice also emerged as important themes. The department has strengthened training, guidance and awareness activities relating to privacy obligations, ethical decision-making, and appropriate information handling, particularly in higher-risk or data-intensive operational areas. This includes targeted support for staff working in environments involving sensitive or protected information, including the National Redress Scheme.

Following broader reforms arising from the Royal Commission into the Robodebt Scheme, the department has also implemented mandatory ethics training intended to strengthen professional judgement, reinforce individual accountability and support lawful, ethical, and privacy-aware information handling of information in policy and program administration. The department recognises that effective management of privacy risk depends not only on formal controls, but also on the capability of staff to apply legislative obligations and operational guidance consistently within complex and evolving environments.

**Shared arrangements and operational complexity**

Consideration was also given to risks that can arise where information handling activities occur across shared service environments, third-party arrangements or interconnected operational models. The department has reviewed relevant contractual and governance arrangements to ensure expectations relating to privacy compliance, information handling, incident reporting and cooperation during investigations or remediation activities are clearly articulated and supported by appropriate assurance mechanisms. These activities recognise that operational complexity can increase where:

- multiple entities are involved in handling information,
- systems or responsibilities intersect, and
- information is relied upon for different purposes across operational environments.

The department's experience is that maintaining clear accountability, visibility of risk and consistent operational application becomes increasingly important within these arrangements.

**Continuous improvement and operational learning**

The department recognises that privacy risk management requires ongoing review and continuous improvement as operational environments, technologies and service delivery arrangements evolve. Accordingly, the department continues to incorporate lessons learned from assurance activities, incidents and complaints, operational reviews, governance reporting, and relevant external reviews and observations.

The department considers that the ANAO Report reinforces broader operational themes reflected throughout this submission, particularly the importance of:

- maintaining visibility of risk across activities,
- strengthening accountability where responsibilities intersect,
- improving enterprise-level assurance,
- embedding privacy considerations early in operational design, and
- making more effective use of operational information to support prevention, response, and continuous improvement.

These observations inform the recommendations outlined in this submission.

# Closing Statement

The department acknowledges the key role of the Committee in examining public sector accountability, performance, and the practical operation of privacy protections across government. The department welcomes the opportunity to contribute to the Inquiry and to support consideration of how privacy risks are identified, managed, and responded to in increasingly interconnected and complex operating environments.

This submission draws on the department's operational experience in applying privacy obligations across policy development, program administration, statutory schemes, and shared delivery arrangements. It reflects an environment where information may move across multiple systems, entities, and legislative frameworks. In this context, frameworks and obligations are well established. The greater challenge lies in maintaining visibility of risk across activities, ensuring consistent operational application, and supporting clear accountability where responsibilities, systems and information handling arrangements intersect.

The department has continued to strengthen its governance, assurance, incident response and workforce capability arrangements, including through activities undertaken in response to broader audit findings and operational learning. The department also recognises that privacy maturity is strengthened through ongoing review, practical application, capability uplift, and more effective use of operational insights drawn from incidents, complaints, and assurance activities.

The recommendations outlined in this submission are directed toward areas where further system wide improvement may support stronger and more consistent outcomes across the public sector. They focus on:

- strengthen accountability across shared arrangements,
- strengthen enterprise visibility of privacy risk,
- strengthen integration of privacy considerations into operational design,
- strengthen sector wide visibility and learning from privacy incidents and complaints, and
- strengthen practical guidance for complex and high-sensitivity environments.

The department remains committed to strengthening its privacy, information handling, and risk management practices in response to evolving service delivery models, technological change, and the

broader threat environment. The department looks forward to the outcomes of the Inquiry and stands ready to provide further information or clarification if required.

# Additional References

| Resource | URL |
|---|---|
| **Privacy Act Review - Submission** | https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/consultation/view_respondent?_b_index=180&uuId=104594517 |
| **Overarching responsibilities and principal legislation** | https://www.dss.gov.au/legislation-we-administer |
| **Privacy Policies** | |
| Department of Social Services | https://www.dss.gov.au/using-our-website/privacy-policy |
| National Redress Scheme | https://www.nationalredress.gov.au/about/privacy |
| Domestic, Family and Sexual Violence Commission | https://www.dfsvc.gov.au/resources/commission-privacy-policy |
| National Commission for Aboriginal and Torres Strait Islander Children and Young People | https://www.ncatsicyp.gov.au/column-4/privacy-policy |
| Australian Institute of Family Studies | https://aifs.gov.au/compliance-reporting/policies-procedures/privacy |
| **Annual Reports** | |
| Department of Social Services | https://www.dss.gov.au/annual-reports |
| Domestic, Family and Sexual Violence Commission | https://www.transparency.gov.au/portfolio-entities-companies/social-services/domestic-family-and-sexual-violence-commission |
| National Commission for Aboriginal and Torres Strait Islander Children and Young People | https://www.transparency.gov.au/portfolio-entities-companies/social-services/national-commission-for-aboriginal-and-torres-strait-islander-children-and-young-people |
| Australian Institute of Family Studies | https://aifs.gov.au/resources/collections/annual-reports |