

Strategic Review – Final Report

Office of the Australian Information Commissioner

19 February 2024



Nous Group acknowledges Aboriginal and Torres Strait Islander peoples as the First Australians and the Traditional Custodians of country throughout Australia. We pay our respect to Elders past, present and emerging, who maintain their culture, country and spiritual connection to the land, sea and community.

This artwork was developed by Marcus Lee Design to reflect Nous Group's Reconciliation Action Plan and our aspirations for respectful and productive engagement with Aboriginal and Torres Strait Islander peoples and communities.

Disclaimer:

Nous Group (**Nous**) has prepared this report for the benefit of the Office of the Australian Information Commissioner (the **Client**).

The report should not be used or relied on for any purpose other than as an expression of the conclusions and recommendations of Nous to the Client as to the matters within the scope of the report. Nous and its officers and employees expressly disclaim any liability to any person other than the Client who relies or purports to rely on the report for any other purpose.

Nous has prepared the report with care and diligence. The conclusions and recommendations given by Nous in the report are given in good faith and in the reasonable belief that they are correct and not misleading. The report has been prepared by Nous based on information provided by the Client and by other persons. Nous has relied on that information and has not independently verified or audited that information.

© Nous Group

Contents

Executive summary.....	5
Part 1: Background and context.....	18
1 Overview of the Strategic Review.....	19
2 Overview of the OAIC.....	22
3 Drivers of change.....	34
Part 2: The OAIC's operating model.....	45
4 Strategy, regulatory posture and approach.....	46
5 Governance.....	69
6 Organisational structure.....	80
7 Organisational capability.....	86
8 Processes and systems.....	100
9 Resourcing and resource allocation.....	113
Appendix A Implementation of recommendations.....	137
Appendix B Details of the Strategic Review.....	147
Appendix C Overview of the OAIC's functions and roles.....	150
Appendix D Privacy Act Review Impact Assessment.....	154
Appendix E Governance model options considered.....	163
Appendix F Structure model options considered.....	166
Appendix G Key workforce metrics.....	171
Appendix H Resourcing Modelling Methodology.....	172
Appendix I Resourcing Options.....	177

Acronyms, abbreviations and terminology

Terminology	Explanation
AAT	Administrative Appeals Tribunal
ACCC	Australian Competition and Consumer Commission
AGD	Attorney-General's Department
AI	Artificial intelligence
AIC Act	<i>Australian Information Commissioner Act 2010</i>
APS	Australian Public Service
CDR	Consumer Data Right
CII	Commissioner-initiated investigation
Digital ID	A form of digital identification, where Australians can verify their identity online without repeatedly supplying copies of sensitive documents ¹
EL	Executive Level (Level in APS staffing)
EVP	Employee value proposition
FOI	Freedom of information
FOI Act	<i>Freedom of Information Act 1982</i>
FOI Senate Inquiry	Senate Inquiry into the operation of Commonwealth FOI laws
FOIC	Freedom of Information Commissioner
FTE	Full-time equivalent
IC	Australian Information Commissioner
Information rights	The rights associated with both privacy and freedom of information
IPS	Information Publication Scheme
NDB	Notifiable Data Breach
OAIC	Office of the Australian Information Commissioner
Ongoing funding	Funding that an agency or department receives on a continuing basis, for activities that do not have a specific end date
PC	Privacy Commissioner
PGPA Act	<i>Public Governance, Performance and Accountability Act 2013</i>
Privacy Act	<i>Privacy Act 1988</i>
Privacy Act Review	The review of the Privacy Act as set out in the <i>Privacy Act Review Report 2022</i>

¹ <https://ministers.ag.gov.au/media-centre/strengthening-australias-digital-id-system-30-11-2023>

Terminology	Explanation
RAC	Regulatory Action Committee
Regulated entities	In respect of the FOI Act – government agencies; in respect of the Privacy Act – all entities that have obligations under that Act
Regulator Performance Resource Management Guide	Guide published by the Department of Finance in December 2022
SES	Senior Executive Service (Level in APS staffing)
Terminating funding	Funding with a specified end date that is provided in relation to a specific group of activities

Executive summary

The Strategic Review

The Office of the Australian Information Commissioner (OAIC) and the Attorney-General's Department (AGD) commissioned a Strategic Review of the agency. The purpose of the Strategic Review was to ensure that the OAIC is well positioned to deliver its statutory functions as the national privacy and information access regulator into the future. Nous Group (Nous) was engaged to complete the Strategic Review.

This report responds to the Strategic Review's Terms of Reference and considers, reports on and provides recommendations about how the OAIC can ensure it is best positioned to deliver its functions as the national privacy and information access regulator and respond to future challenges. The report covers a range of elements of the OAIC's operating model and environment to make recommendations about the suitability of current arrangements and suggest changes that might be required to enable the OAIC to respond to future challenges.

Nous conducted the Strategic Review between November 2023 and February 2024. We undertook multiple engagements with OAIC staff and leaders, interviewed external stakeholders, reviewed and analysed extensive documentation, and considered the arrangements of analogous agencies. The Strategic Review was overseen by a Steering Group comprising senior officials from the OAIC, the Attorney-General's Department, and the Department of Finance.

The OAIC's role

The OAIC plays a critical – and necessarily evolving – role in protecting and promoting information rights

Through its regulation of privacy and information access under the *Privacy Act 1988* (Privacy Act) and the *Freedom of Information Act 1982* (FOI Act), the OAIC plays a critical role in promoting and upholding the privacy and information access rights of all Australians. It is therefore in Australia's national interest that the agency is as well placed as possible to perform these roles in a rapidly evolving operating context.

The OAIC's functions, set out in the *Australian Information Commissioner Act 2010* (AIC Act), include:

- freedom of information (FOI) functions, which are about giving the Australian community access to information held by the Australian Government (the Government) in accordance with the FOI Act (and other Acts)
- privacy functions, which are mainly about protecting the privacy of individuals in accordance with the Privacy Act (and other Acts)
- Information Commissioner (IC) functions, which are strategic functions concerning Australian Government information management policy and practice.

In its role as the regulator for privacy, the OAIC helps to protect all Australian citizens by promoting privacy rights, and preventing and addressing privacy harms. The OAIC's role as a privacy regulator has evolved as the growth of the digital economy has led to an expansion in the volumes of personal information collected, used and shared. The agency is at the forefront of a critical and challenging balancing act for privacy regulators globally: maximising the many benefits of the digital economy while also protecting the privacy of citizens and minimising the significant harms that can occur when personal data is accessed and shared unlawfully.

Its role as the FOI regulator is critical in safeguarding Australia's FOI system. This system is seen as vital to a healthy, transparent and well-functioning democracy; the rule of law; government transparency and

accountability; and enabling public engagement with government decision-making.² Eighty-three per cent of respondents to the 2022 Cross Jurisdictional Information Access Study agreed that public access to government information improves transparency and accountability.³

The OAIC's operating environment

The OAIC's operating environment is changing – in particular, the rapid growth of the digital economy and advances in artificial intelligence (AI) will profoundly impact personal privacy

The privacy landscape for the OAIC over the next decade is likely to look markedly different to that of the past ten years. Advances in technology and the ongoing growth of the digital economy are expected to have a profound impact on personal privacy. Rapid growth in the sophistication and applications of AI, new technologies like biometric authentication and profiling, the likelihood of larger and more frequent data breaches, and increased cyber crime are creating a more complex and faster-evolving operating environment for the OAIC.

Societal expectations about privacy protection are changing as technology evolves and data breaches become more frequent and more harmful. Eighty-nine per cent of respondents to the Australian Community Attitudes to Privacy Survey 2023 said they would like government agencies to do more to protect their personal information.⁴

Community expectations around accountability and transparency are increasing, with 91 per cent of respondents to the 2023 Australian Government Information Access Survey indicating it was important to have the right to access government information, up from 84 per cent in 2019.⁵ At the same time, trust in the national government has declined over the long term, highlighting the importance of actions that maintain or rebuild public trust.⁶ Many witnesses to the 2023 Senate Inquiry into the operation of Commonwealth FOI laws (FOI Senate Inquiry) called for a more responsive FOI culture among agencies and increased OAIC guidance.

The Government has articulated what it expects of the OAIC and has significantly increased its funding

In response to rapidly evolving technologies and societal expectations, the Government initiated several reviews and reforms that will shape the OAIC's future functions and priorities – most notably the recent Privacy Act Review. Proposals from this review will materially change some OAIC functions and introduce new functions. Many of the Privacy Act Review's recommendations will require the OAIC to adapt and enhance its capabilities to take on new responsibilities, which will have flow-on impacts for its supporting and enabling functions.

The Government set out its priorities for the OAIC in the Attorney-General's 2023 Statement of Expectations. The Government expects the OAIC to promote and regulate the protection of personal information in line with the objects of the Privacy Act and access to information through the operation of the FOI Act.⁷ It also acknowledges the increasing importance of the online environment for the economy, education and social connections. It expects the OAIC to focus on regulatory activities that address privacy harms arising from the practices of online platforms and services that impact individuals' choice and control; promote awareness of privacy risks; provide guidance about how to protect personal information online; and take an integrated approach to embedding compliance and enforcement policies, project

² FOI Senate inquiry, p 7.

³ Office of the Victorian Information Commissioner, [Cross Jurisdictional Information Access Study](#), May 2022.

⁴ Office of the Australian Information Commissioner, [Australian Community Attitudes to Privacy Survey 2023](#), August 2023.

⁵ Office of the Australian Information Commissioner, [Australian Government Information Access Survey 2023](#), September 2023.

⁶ Measuring What Matters dashboard, '[Trust in national government](#)', July 2023.

⁷ Attorney-General's Statement of Expectations, p 2.

planning and risk management activities in respect of the Consumer Data Right (CDR). The Government also expects the OAIC to address privacy breaches, deal with entities that are not complying with privacy obligations, promote awareness of privacy risks and provide guidance to regulated entities and individuals.⁸

The OAIC's total funding has increased significantly over the past four years, from \$21 million to \$46 million. This includes a 79 per cent increase in ongoing funding over the same period. Of this funding, \$23 million is terminating and tied to specific measures. These measures include funding to support a standalone Privacy Commissioner (PC), to progress investigations and enforcement action in response to privacy and data breaches, to enhance the OAIC's data and analytics capability, and to support the Privacy Act Review. Terminating funding measures accounted for half of the agency's total funding in 2023-24, a relatively high proportion of terminating funding compared to other regulators. s47C

The OAIC's increased funding has been accompanied by significant staff growth, with a 55 per cent increase in full-time equivalent (FTE) numbers between 2020 and 2024.

Demand for the agency's critical functions has grown, contributing to substantial case backlogs

Under its legislative remit, the OAIC has a range of functions and powers. At least 37 different pieces of legislation (primary and subordinate) confer functions, powers or responsibilities on the IC, or create requirements for other bodies to consult with the IC on privacy matters. Some of these functions are mandatory, while others are discretionary; some are triggered by external drivers and others are applied at the OAIC's initiation. For the Strategic Review, we characterised functions that are mandatory under legislation as 'critical' and functions that are discretionary under legislation as 'strategic'. To operate effectively as the regulator for privacy and FOI, the OAIC must balance a range of critical and strategic functions under its core pieces of legislation, as well as functions and powers under a wide range of other legislative instruments.

The OAIC has continued to see high and growing demand for two of its critical, mandatory functions: IC reviews and privacy complaints. The total number of requests the OAIC has received each year for IC reviews has grown steadily by 16 per cent annually since 2015. The number of privacy complaints has fluctuated over the past decade, with significant data breaches generating fresh peaks in the number of new complaints received. Since 2016, the number of new privacy complaints received each year by the OAIC has grown by 5 per cent annually.

As the number of new cases has exceeded the number that have been resolved, the case backlog – as measured by the number of cases unresolved for more than 12 months – has grown. This has been most pronounced in the OAIC's IC review jurisdiction.

The OAIC's evolving operating model

The OAIC has shifted its regulatory posture and transformed its operating model in response to external drivers of change

The OAIC has substantially changed its operating model over the past two years in response to its evolving operating environment. The changes include shifting the agency's regulatory posture by establishing a Major Investigations Branch, introducing structural changes to service FOI and CDR

⁸ Attorney-General's Statement of Expectations.

functions and deliver corporate functions, expanding external partnerships, improving processes and initiating a Systems Review to consider and address system limitations.

The OAIC has also transitioned from having the majority of its staff working in Sydney to a fully hybrid and remote workforce. These changes occurred largely in response to the COVID-19 pandemic and the need to rapidly scale up its workforce of specialists in a tighter-than-usual labour market.

The composition of the Executive team has seen significant flux and change

Since 2014, the IC has also held the PC role (the current IC was appointed in 2018). Between 2014 and 2021, the FOI Commissioner (FOIC) role was vacant, with the IC also carrying out those functions. Between 2021 and early 2024, three different people acted in the FOIC role, with only one of them formally appointed.

In 2024, the OAIC will move to a three-Commissioner model for the first time in many years. This will necessitate changes that align with each new Commissioner's desired strategic direction. It will also require the implementation of operational structures, practices and supports that help the three Commissioners to operate in a coordinated and productive manner.

s47C

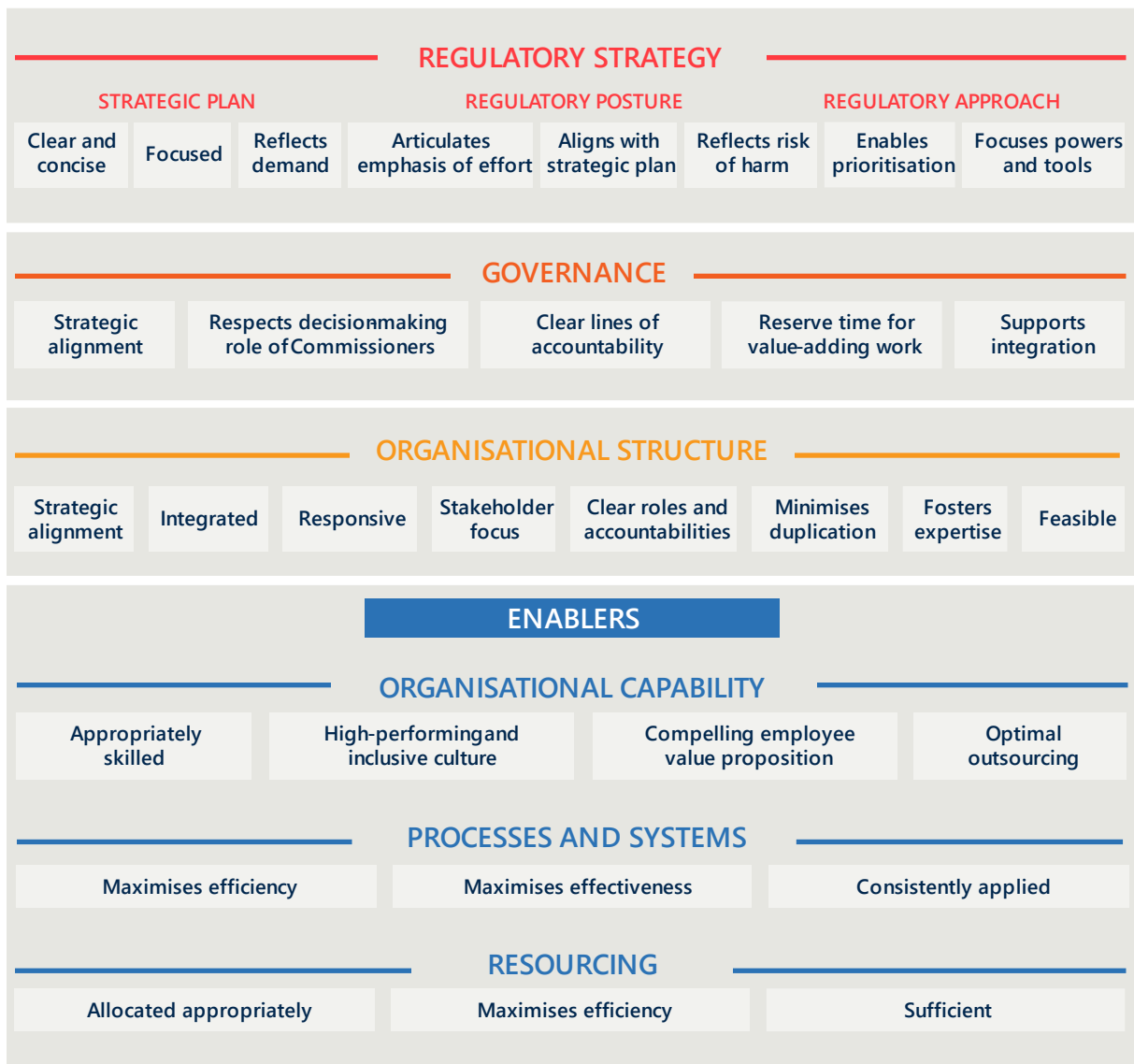


The analytical framework for the Strategic Review

Nous developed an analytical framework to guide the Strategic Review. It outlines the elements of the OAIC's operating model that we considered in response to the Terms of Reference of the Review. Figure 3 shows the framework and assessment criteria developed for each element of the operating model.

These criteria were used to test the suitability of the OAIC's current operating model and to guide recommendations around what the OAIC should change to ensure it is best positioned to deliver on its functions as the national privacy and information access regulator and to respond to future challenges. Questions used to guide analysis relating to each criterion in the framework are included at the start of the relevant chapter in this report.

Figure 3 | Strategic Review analytical framework



Structure of this report

This report has two main parts:

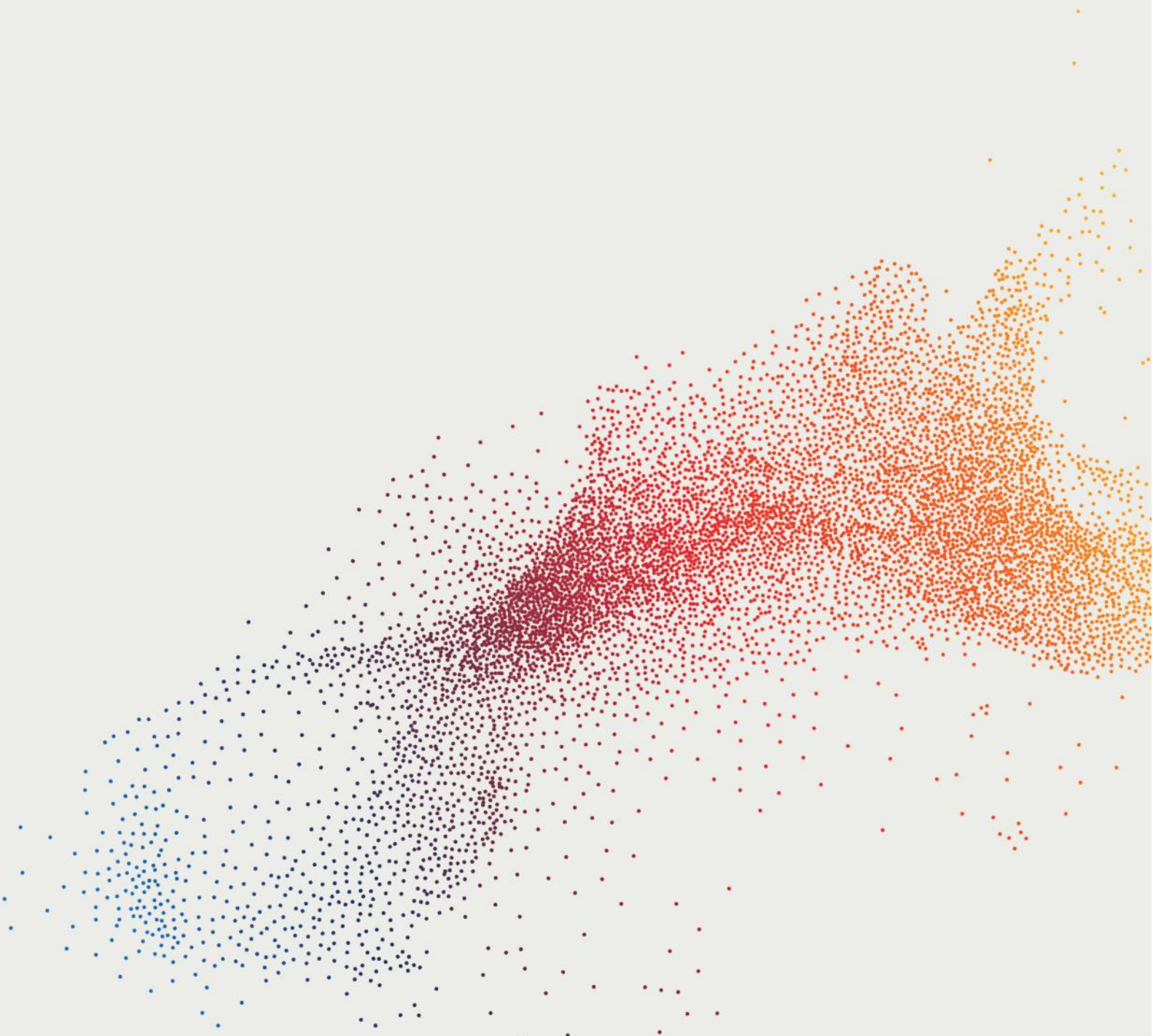
1. **Background and context** | Provides an overview of the Strategic Review, the OAIC, and the drivers of change the agency must respond to in order to achieve its purpose and future functionality as a regulator.
2. **The OAIC's operating model** | Outlines the current state, opportunities and challenges, and recommendations about the future state in respect to key elements of the OAIC's operating model – regulatory strategy, governance, structure, processes and systems, organisational capability, and resourcing and resource allocation.

Table 2 summarises how the Terms of Reference map to the elements of our analytical framework and the corresponding chapters of this report.

Table 2 | Report structure

Terms of Reference	Relevant analytical framework elements	Report reference
The extent to which the OAIC's <ul style="list-style-type: none"> • organisational capability • structure • governance • resourcing are suitable to achieve the OAIC's purpose and future functionality, or require amendment	Drivers of change	Chapter 3
	Organisational capability	Chapter 7
	Organisational structure	Chapter 6
	Governance	Chapter 5
How resource allocation can be optimised to maximise efficiency and support the OAIC's statutory functions	Resourcing	Chapter 9
	Processes and systems	Chapter 8
How the OAIC can best respond to the likely continuing growth to the volume and complexity of its core statutory workload	Resourcing	Chapter 9
	Drivers of change	Chapter 3
	Strategy, regulatory posture and approach	Chapter 4
	Processes and systems	Chapter 8
	Organisational capability	Chapter 7
How to ensure the effectiveness of the OAIC as a regulator in responding to changing technology, the growth of the digital economy and increasing cyber crime	Resourcing	Chapter 9
	Drivers of change	Chapter 3
The role of the OAIC in providing advice and reports to government about privacy, information access and information management	Strategy, regulatory posture and approach	Chapter 4
	Strategy, regulatory posture and approach	Chapter 4

Part 1: Background and context



1 Overview of the Strategic Review

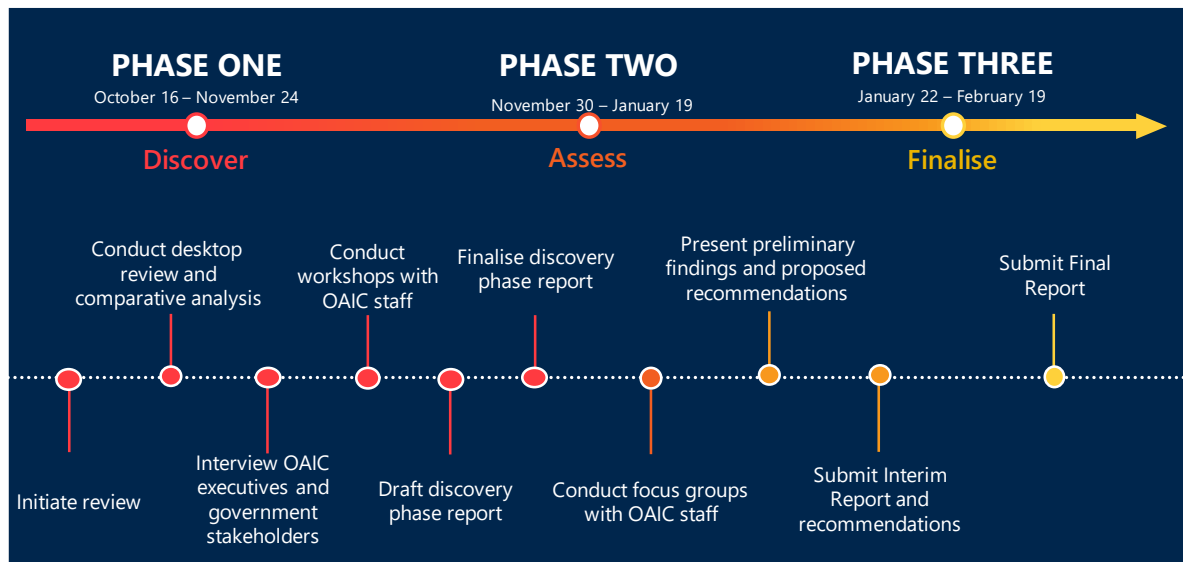
This chapter provides an overview of the scope, governance and data sources for the Strategic Review.

The OAIC and the AGD commissioned the Strategic Review of the OAIC. The purpose of the Review was to ensure that the OAIC is well positioned to deliver its statutory functions as the national privacy and information access regulator into the future.

The Strategic Review comes as data, information and privacy systems are becoming increasingly challenging and complex. How effectively the OAIC performs its role as the primary regulator of these systems is therefore increasingly important for all Australians.

The Review was conducted over 16 weeks, from October 2023 to February 2024. Timelines and key milestones are shown in Figure 4.

Figure 4 | Timelines for the Strategic Review



1.1 Strategic Review scope

The key elements of the Terms of Reference of the Review are outlined in Figure 5. The full Terms of Reference can be found in Appendix A.

Figure 5 | Scope of the Strategic Review as per the Terms of Reference

The reviewer should consider, report, and make recommendations about how the OAIC can ensure it is best positioned to deliver on its functions as the national privacy and information access regulator and respond to future challenges. Recommendations should cover:

1. the extent to which the OAIC's
 - a. organisational capability
 - b. structure
 - c. governance
 - d. resourcing
 are suitable to achieve the OAIC's purpose and future functionality, or require amendment
2. how resource allocation can be optimised to maximise efficiency and support the OAIC's statutory functions
3. how the OAIC can best respond to the likely continuing growth to the volume and complexity of its core statutory workload
4. how to ensure the effectiveness of the OAIC as a regulator in responding to changing technology, the growth of the digital economy and increasing cyber crime
5. the role of the OAIC in providing advice and reports to government about privacy, information access and information management.

The Strategic Review occurred in parallel with several other reforms and announcements that will have a bearing on the OAIC's functions as a regulator and how it can be best positioned to respond to future challenges. These include the release of the report from the Senate Inquiry into the operation of Commonwealth FOI laws (FOI Senate Inquiry), the appointment of the new FOIC and the new PC, and the announcement by the IC (also the agency head) that they will not be seeking a third term in the role. The release of the Australian Government's (the Government's) response to the Privacy Act Review and agreement to its recommendations in full or in principle also preceded the start of the Strategic Review by several weeks.

Figure 6 outlines several upcoming decisions to be made by the Government and/or the OAIC. These decisions are relevant to the OAIC's future priorities and operating model. Where these decisions relate to the Terms of Reference, they have been considered to some extent and referred to throughout this report as part of our review of the OAIC's evolving operating environment.

Figure 6 | Upcoming decisions that are relevant to the outcomes of the Strategic Review

Upcoming decisions relate to:

1. the recommendations from the FOI Senate Inquiry
2. the future funding implications for the OAIC from the Privacy Act Review and the Government's response

s47C

1.2 Strategic Review governance

The Strategic Review has been overseen by the OAIC Strategic Review Steering Group, which comprises senior representatives from the OAIC, the AGD and the Department of Finance. The Steering Group is responsible for:

- developing the Terms of Reference, which were endorsed jointly by the OAIC Commissioners and the Secretary of the ADG
- engaging with the reviewer (Nous) during the Review to ensure relevant matters were considered
- providing feedback to the reviewer in relation to a draft review report
- considering the Review outcomes and providing advice on potential next steps.

1.3 Strategic Review method and data sources

The Strategic Review drew on a wide range of data sources, which are summarised in Figure 7. Appendix B contains a more detailed overview of the methodology and data sources, and details of the stakeholders the Strategic Review team engaged.

Figure 7 | Overview of key data sources for the Strategic Review



2 Overview of the OAIC

This chapter provides an overview of the OAIC. It outlines relevant context, including legislative responsibilities and functions, a snapshot of recent demand and performance, and key events that have affected the OAIC's operations.

Figure 8 | Summary of context

- The OAIC's core role is as regulator of FOI and privacy. Established in 2010 under the *Australian Information Commissioner Act 2010* (AIC Act), the OAIC is an independent statutory agency within the Attorney-General's portfolio. It administers the *Privacy Act 1988* (Privacy Act) and *Freedom of Information Act 1982* (FOI Act).
- The OAIC is responsible for protecting privacy and information access rights, and managing information policy in Australia. The OAIC's purpose is to promote and uphold privacy and information access rights. Through its regulation of privacy and information, the agency supports effective government, a strong Australian economy and human rights. Australia's national interest requires that the OAIC is well placed to perform its role.
- In recent years, the agency has experienced changes to Commissioners, Senate inquiries, and legislative reform giving the OAIC additional powers and responsibilities. Its remit has expanded to cover the CDR, the Notifiable Data Breaches scheme, the Digital ID and regulation of the COVIDSafe app.
- The OAIC must balance its resources across core non-discretionary work required under its legislation and more strategic and enabling work where it has greater discretion. It must broadly perform certain functions, such as managing privacy complaints and IC reviews, in line with demand for these functions. It can undertake other discretionary functions, such as investigations and assessments, in a more targeted and strategic manner.
- The OAIC's current structure, size and resourcing reflect its legislative responsibilities. The OAIC has 193 staff working across Australia and separated into five branches that cover privacy, FOI and CDR functions. The agency is currently led by the IC and PC – a dual role performed by a single individual – and the FOIC.
- The OAIC has experienced changes to its Commissioners and was involved in Senate inquiries in 2023. The FOIC role was left vacant from 2015 to mid-2021, while the PC and IC roles have been filled by a single individual since 2015. The FOI Senate Inquiry into the operation of the Commonwealth FOI laws saw considerable focus on the processes and resourcing of the OAIC's FOI Branch.
- Agency staff direct most of their efforts towards making decisions in respect of IC reviews and FOI complaints in the OAIC's FOI jurisdiction, and privacy complaints in its privacy jurisdiction.
- This focus on making decisions in respect of IC reviews and privacy complaints has meant that increased demand for these functions has been keenly felt across the organisation.
- The OAIC has implemented a series of initiatives in response to its evolving operating environment and greater size and scope. These initiatives have been effective in responding to changing demands in an evolving external landscape.
- The OAIC met most but not all performance measures in the past financial year. Key areas where it could improve to achieve its performance measures relate to the time taken to finalise IC reviews, Commissioner-initiated investigations (CIIs) and Notifiable Data Breaches (NDBs).

- Stakeholders reflected positively on the OAIC and its approach. The OAIC received its highest score for the regulation of CDR and its lowest score for the extent to which its activities are risk-based and data-driven.

2.1 The OAIC's legislative context

The OAIC's core role is as regulator of freedom of information and privacy rights

The OAIC is Australia's national privacy and information access regulator. Established in 2010 under the AIC Act, the OAIC is an independent statutory agency within the Attorney-General's portfolio that administers the Privacy Act and FOI Act.

The AIC Act sets out a range of the OAIC's functions, including:

- FOI functions, which are about giving the Australian community access to information held by the Government in accordance with the FOI Act (and other Acts)
- privacy functions, which are mainly about protecting the privacy of individuals in accordance with the Privacy Act (and other Acts)
- IC functions, which are strategic functions concerning Australian Government information management policy and practice.

The AIC Act also provides the IC with the ability to delegate powers and functions that are conferred on the IC under provisions in other legislation.

The OAIC is empowered to perform its privacy functions under the Privacy Act. These functions include regulating the handling of personal information, investigating complaints, conducting assessments and providing advice and guidance about privacy rights and obligations. Handling of privacy complaints is the most significant privacy function exercised by the OAIC (in terms of effort), and complaints can be lodged if an applicant is concerned that their personal information has been mishandled.

Under the FOI Act, the OAIC is responsible for protecting the public's right of access to government-held information. The Act empowers the OAIC to perform a range of functions, including reviewing decisions made by agencies and ministers under the FOI Act (IC reviews), handling FOI complaints, monitoring compliance with the FOI Act, and producing guidance to support the application of that Act. Most FOI matters received by the agency are IC review applications, which can be requested if an applicant disagrees with a decision made by an agency in response to an FOI request or if the agency has not made a decision within the time the FOI Act allows.

The OAIC regulates Australian Government entities and officials (in relation to FOI and privacy) and the private sector (in relation to privacy).

It is responsible for protecting privacy and information access rights, and managing information policy

The OAIC's purpose is to promote and uphold privacy and information access rights.¹⁸ Through its regulation of privacy and information access under the Privacy Act and the FOI Act, the agency supports effective government, a strong Australian economy and human rights. Australia's national interest requires that the OAIC is well placed to perform this role. This is a challenging ask of the agency as the privacy and

¹⁸ [OAIC Annual Report 2022–23](#).

FOI landscape is constantly evolving and the OAIC must be at the forefront of the Government's response to whole-of-society future challenges.

The OAIC's roles matter to Australians and to the Government. Eighty-four per cent of Australians want more control or choice over the collection and use of their personal data.¹⁹ Over 90 per cent of Australians believe it is important that they have a right to access government information.²⁰ The Attorney-General's Statement of Expectations for the OAIC acknowledges the OAIC's 'invaluable work' as it reorients elements of its mandate.

It has a broad remit, which the Government has expanded in recent years

The OAIC has a broad range of functions under around 37 different pieces of legislation, including the *Competition and Consumer Act 2010* (in relation to CDR), the *My Health Records Act 2012* and the Privacy (Credit Reporting) Code 2014.

The OAIC's remit has expanded in recent years. Legislative change has given the OAIC additional powers and responsibilities, including new information-gathering powers in the NDB scheme; information-sharing and enforcement powers; powers and functions under the Competition and Consumer (Consumer Data Right) Rules 2020; and privacy regulation of the Digital ID and the COVIDSafe app.

It must strike a balance between performing core non-discretionary work required under legislation and its discretionary strategic and enabling work

The OAIC has some discretion about how it performs its legislated functions. It must perform certain functions, such as managing privacy complaints and IC reviews, broadly in line with demand for these functions. Other functions, including investigations and assessments, are discretionary and can be undertaken in a more targeted and strategic manner.

The OAIC has many roles for an agency of its size, reflecting the breadth of primary and subordinate legislation that fall within its remit. As a result, its priorities and resourcing allocation need to be regularly reassessed for appropriateness.

The Strategic Review team developed a framework for mapping the OAIC's statutory functions by the following three categories:

- **CRITICAL** | Mandatory functions required by legislation that are critical responsibilities for meeting privacy and FOI obligations
- **STRATEGIC** | Other activities related to privacy and FOI that the OAIC is empowered – but not mandated – to exercise by legislation
- **SUPPORTING** | All other functions that, while not directly involved in the regulatory process, are vital for the OAIC to operate.

The functions in each category across the OAIC's core regulatory remit are shown in Figure 9. Appendix C provides more detail about statutory obligations mapped to the agency's functions.

¹⁹ OAIC, Australian Community Attitudes to Privacy Survey, August 2023, p 18.

²⁰ Information and Privacy Commission and Woolcott, Cross Jurisdictional Information Access Study, June 2023, p 6.

Figure 9 | Key functions and roles

	CRITICAL	STRATEGIC	SUPPORTING
PRIVACY	<ul style="list-style-type: none"> Assess privacy complaints Administer the Notifiable Data Breaches scheme Approve code development Develop and approve legislative instruments Develop legislative instruments 	<ul style="list-style-type: none"> Initiate privacy investigations Conduct privacy assessments Produce regulatory guidance for privacy legislation Develop research and educate the public on privacy (for example, the Australian Community Attitudes to Privacy Survey) Provide advice in relation to the operation of privacy functions Conduct monitoring for privacy functions 	
FOI	<ul style="list-style-type: none"> Assess IC reviews Assess and investigate FOI complaints Assess extension of time applications Assess vexatious applicant declaration applications Administer the Information Publication Scheme (IPS) 	<ul style="list-style-type: none"> Conduct FOI investigations Conduct FOI monitoring Prepare FOI guidelines Provide advice and training on matters relevant to the operation of the FOI Act 	
CDR	<ul style="list-style-type: none"> Monitor and manage the privacy and confidentiality functions of CDR 	<ul style="list-style-type: none"> Conduct CDR assessments Develop CDR regulatory guidance CDR monitoring for small businesses and individuals Develop CDR guidelines and provide advice 	
INFORMATION		<ul style="list-style-type: none"> Engage in information management policy development Perform strategic functions relating to information management in government 	

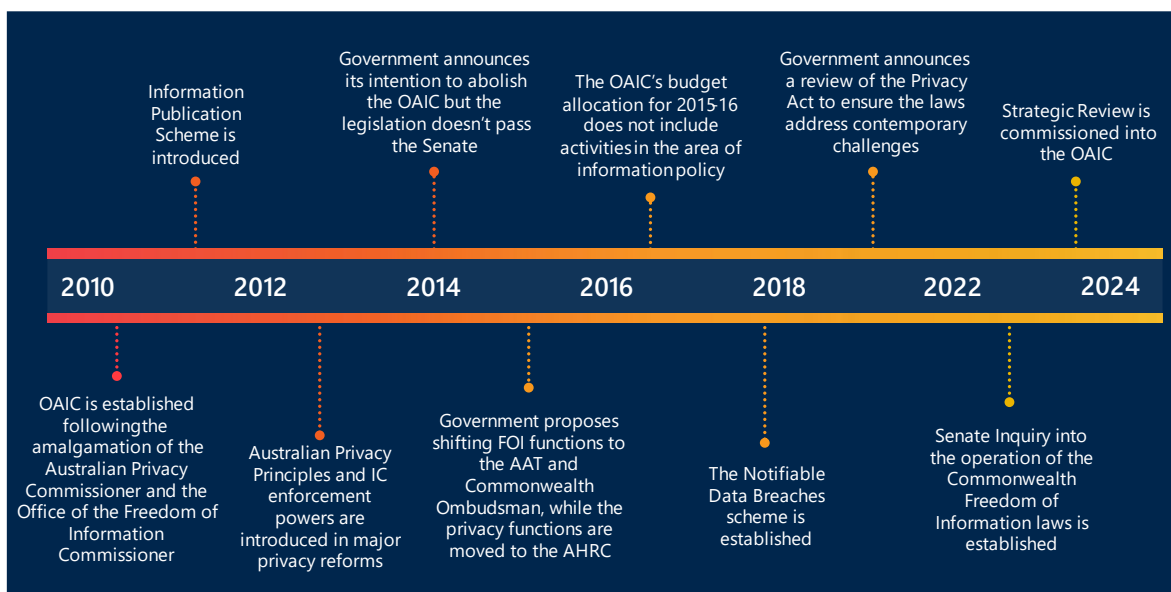
	CRITICAL	STRATEGIC	SUPPORTING
OTHER	<ul style="list-style-type: none"> Adhere to public service employment standards Ensure proper financial management and reporting Ensure workplace health and safety compliance 	<ul style="list-style-type: none"> Provide expert advice on privacy to government agencies and other entities involved in Digital ID development Provide guidance to healthcare providers on best practices for managing personal information within the My Health Record system 	<ul style="list-style-type: none"> Conduct people management and development Recruit staff and conduct onboarding Engage in data management and analytics Provide administrative and support services Conduct communication and engagement Create content and manage publication Manage technology systems Conduct procurement and resource management Abide by <i>Public Governance, Performance and Accountability Act 2013</i> (PGPA Act) requirements

2.2 The OAIC’s operating model

Since it was established in 2010, the OAIC has experienced significant changes that have required the agency to adapt and expand to respond to evolving needs and challenges in privacy protection and information management. The agency’s growing remit has required new functions, and it has had to respond to growing demand for FOI matters.

These key developments and reforms are outlined in Figure 10.

Figure 10 | Timeline of key events

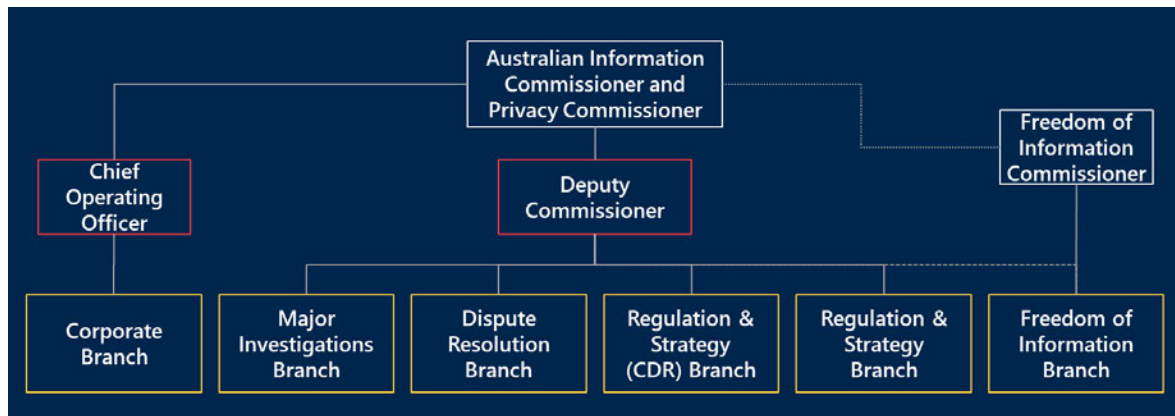


In 2014, the Government proposed abolishing the OAIC as part of its 'smaller government' agenda, with a proposal to move the OAIC's functions to other agencies. The legislation to dissolve the OAIC lapsed in the Senate at the end of 2014. **s47C**

The current structure, size and resourcing reflect the agency's legislative responsibilities

The OAIC has 193 staff working across Australia and separated into five branches that cover privacy, FOI and CDR functions. The agency is currently led by the IC and PC – a dual role that is performed by a single individual – and the FOIC. The OAIC's structural arrangements are shown in Figure 11.

Figure 11 | OAIC structure



The agency received around \$46 million in funding in 2023-24, split evenly across ongoing and terminating funding. Over the past ten years, its total resourcing has increased significantly from an initial base of \$10 million. It has had a 117 per cent increase in ongoing funding over the decade and, since 2019, a considerable increase in funding for both ongoing base and terminating functions.

At least 37 different pieces of legislation confer functions, powers or responsibilities on the IC, or create requirements that other bodies consult with the IC on privacy matters.

An overview of the OAIC's current resourcing, staffing and structure is shown in Figure 12.

Figure 12 | Overview of resourcing, staffing and structure



The OAIC has adjusted to changes in Commissioners in recent years. The FOIC role was left vacant from 2015 to mid-2021, while the PC and IC roles have been fulfilled by a single individual since 2015. The decision to appoint three individuals to all three Commissioner roles was made in 2023 and will take effect in February 2024.

The agency has been the subject of several Senate inquiries in recent years. Most recently, the FOI Senate Inquiry focused on the processes and resourcing of the OAIC's FOI Branch, in addition to concerns raised about the agency's culture. The inquiry's recommendations are covered in more detail in chapter 3.

The OAIC has implemented reforms to its operating model in response to its changing operating environment and broader remit

The OAIC has made substantial changes across all elements of its operating model in the past few years in response to changing demands in an evolving external landscape. Key changes are shown in Figure 13.

Figure 13 | Overview of recent reforms to the OAIC's operating model

<p>REGULATORY POSTURE</p> <p>Established the Major Investigations Branch in 2022-23 to carry out significant investigations – receiving dedicated funding for this work</p> <p>Issued its second civil penalty and began Federal Court proceedings against Australian Clinical Labs</p>	<p>EXTERNAL PARTNERSHIPS</p> <p>Began regulating CDR in close partnership with the ACCC</p> <p>Began collaborating with other regulators as part of the Digital Platforms Regulators Forum</p> <p>Partnered with the NZ Office of the Privacy Commissioner to investigate Latitude Financial Services</p> <p>Began participating in Global Privacy Assembly working groups and became co-chair of the Digital Citizen and Consumer Working Group</p>		
<p>GOVERNANCE</p> <p>Established the Regulatory Action Committee in 2020-21 to assess regulatory options for responding to significant and emerging privacy risks</p> <p>Delegated IC reviews to the FOI Assistant Commissioner in December 2022</p>	<p>STRUCTURE</p> <p>Changed the FOI Branch structure to address the case backlog</p> <p>Divided the Regulation and Strategy Branch into two sub-branches, with one focused on new work related to CDR</p> <p>Introduced the Corporate Branch, with a senior Assistant Commissioner position carrying out the role of the OAIC's Chief Operating Officer</p> <p>Transitioned the agency from a shared services model with the Australian Human Rights Commission to bringing financial and HR functions in-house</p> <p>Expanded the Corporate Branch to include a data and reporting team</p> <p>Introduced a Digital ID Implementation team</p>	<p>PROCESSES</p> <p>Launched new initiatives to improve the time taken to provide clearance for operational matters</p> <p>Introduced the Complaints Continuum Committee to improve oversight of privacy complaints</p>	
<p>WORKFORCE CAPABILITY</p> <p>Transitioned to a fully hybrid and remote working model and away from a Sydney-centric footprint</p> <p>Substantially increased number of staff from 127 to 183 (45%) in the year to June 2023</p>	<p>CULTURE & LEADERSHIP</p> <p>Recorded a significant increase in scores in the latest APS Census results on the back of the Census Roadmap initiatives</p>	<p>RESOURCING</p> <p>Received an increase in agency funding of approximately 53% between 2022-23 and 2023-24. However, 50% of the 2023-24 funding is terminating (short-term) funding to cover one-off initiatives</p>	<p>OTHER ENABLERS</p> <p>Initiated a Technology Systems Review to address systems limitations, focusing on the case and document management systems</p>

The majority of the OAIC's efforts are directed towards case management activities

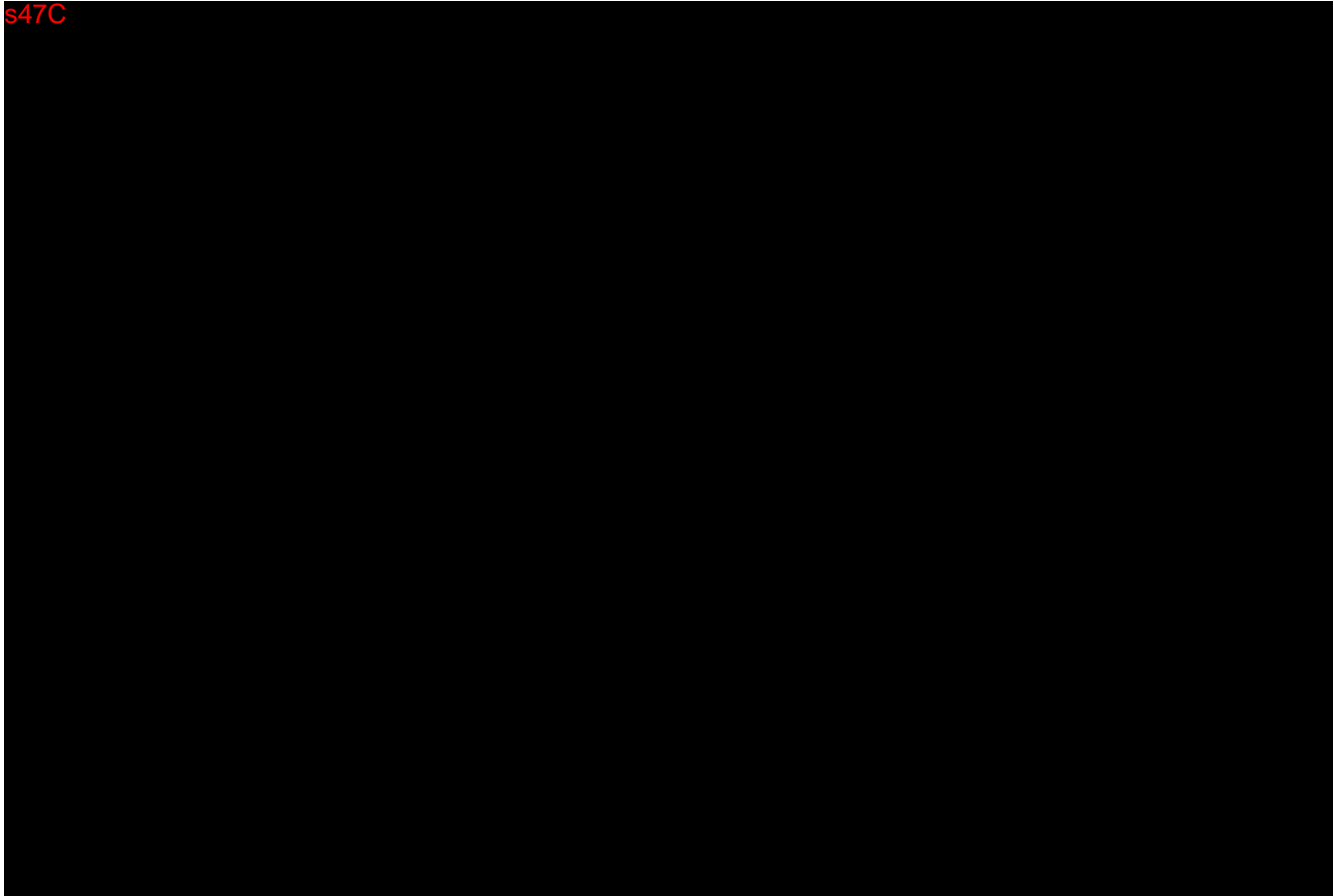
The majority of the OAIC's staff effort is directed towards making decisions related to IC reviews and FOI complaints in the OAIC's FOI jurisdiction, and privacy complaints in the agency's privacy jurisdiction. These are broadly referred to as 'assess and decide' activities, which are outlined in Figure 14. s47C

[REDACTED]

[REDACTED]

[REDACTED]

s47C



2.3 The OAIC's performance

The agency has continued to address its growing caseload while also performing its other significant functions, including monitoring, enforcement, regulatory guidance and advice.

Substantial staff effort is allocated to meeting demand for certain critical functions

s47C



The numbers of requests for IC reviews (see Figure 15) and privacy complaints (see Figure 16) have increased since the OAIC was established. As cases have grown faster than they have been resolved, the case backlog – as measured by the number of cases unresolved for more than 12 months – has risen. This has been most pronounced in the OAIC's IC review jurisdiction.

²¹ As assessed by the Strategic Review through a Workforce Allocation Survey that was circulated to all teams across the OAIC.

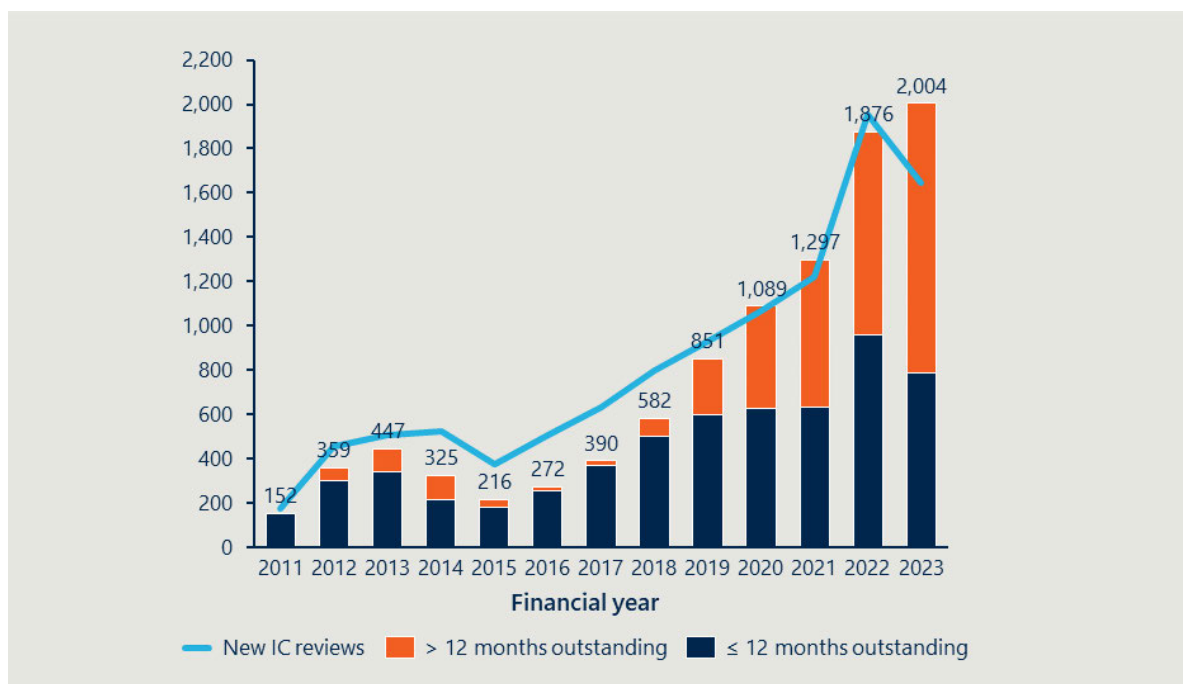
There are increasing numbers of applications for IC reviews of FOI decisions

The number of applications for IC reviews has increased steadily since 2015, with an average annual growth rate of 7 per cent over that period.

The increase in the number of IC reviews on hand is due to the backlog of IC reviews, the increasing complexity of applications seeking information relating to third-party individuals or national security matters, and an increase in the number of matters that are voluminous or raise multiple and overlapping exemption claims. Growth in the number of new IC review applications received and applications outstanding is shown in Figure 15.

As more IC review cases have been received by the OAIC than have been finalised in recent years, the number of cases over that are over 12 months old has steadily increased. There is no statutory timeframe for IC reviews but the OAIC's performance measures set a target of finalising 80 per cent of applications within 12 months. The average time taken to finalise an IC review in 2022-23 was 9.8 months.²²

Figure 15 | Number of IC reviews since 2011



Source: OAIC Annual Report 2013-14, OAIC Annual Report 2018-19, OAIC Annual Report 2022-23

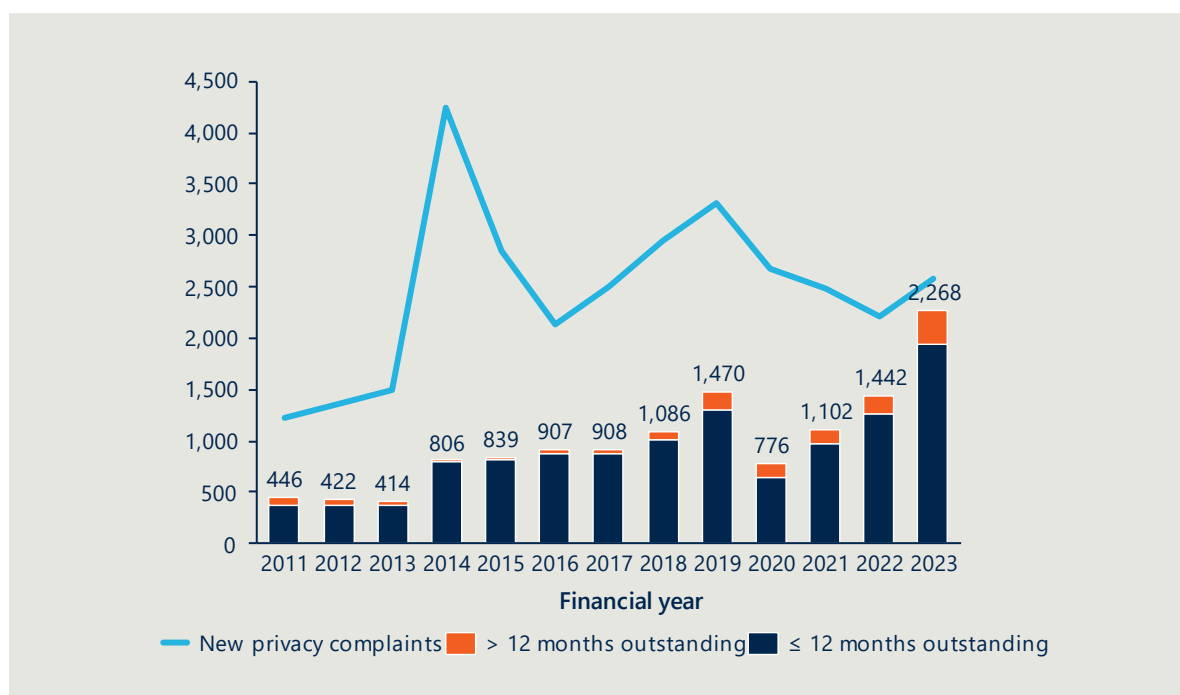
²² [OAIC Annual Report 2022-23](#).

The number of privacy complaints has fluctuated

Privacy complaints to the OAIC increased by 34 per cent in 2022-23 compared to 2021-22, but are below the 2014 peak.²³ Complaints have grown since 2011, as shown in Figure 16. As the OAIC has received more privacy complaints than it has finalised in recent years, the number of cases outstanding for more than 12 months has increased from low levels.

The increase in complaints relative to 2011 can largely be explained by a combination of increased public awareness of data privacy rights and greater use of digital services that handle personal data. A series of recent high-profile data breaches also elevated public concern about the handling of data, leading to a large uptick in privacy complaints over the past financial year.²⁴

Figure 16 | Numbers of privacy complaints since 2011



Source: OAIC Annual Report 2013-14, OAIC Annual Report 2018-19, OAIC Annual Report 2022-23

Most but not all performance measures were met in the past financial year

The OAIC Performance Measurement Framework outlines the agency's approach to evaluating its effectiveness in promoting and upholding privacy and information access rights, based on specific measures contained in its *Corporate Plan* and Portfolio Budget Statement.







Figure 17 shows how the OAIC performed last financial year against the subset of performance measures that relate to how the agency is performing its core roles. The OAIC met or was close to meeting all targets for five of the six selected performance measures. The performance measures cover a broad range of its regulatory activities, including significant functions that are unrelated to case management.²⁵

²³ The significant increase in privacy complaints in 2014-15 reflects approximately 1,000 complaints following an immigration data breach where the Department of Home Affairs published, in error, a detention report on its website that contained embedded personal information.

²⁴ The recent high-profile Optus, Medibank, Latitude Financial and Australian Clinical Labs data breaches have drawn attention to the handling of personal information.

²⁵ Overall, the OAIC achieved 69% (or 11 of 16) of its performance measures in FY23.

Figure 17 | Key Performance Outcomes 2022-23

PERFORMANCE MEASURE	TARGET	RESULT	OUTCOME
1.2.1 Time taken to finalise privacy complaints	80% of privacy complaints finalised within 12 months	84%	
1.2.2 Time taken to finalise privacy and FOI Commissioner-initiated investigations (CIIs)	80% of CIIs finalised within 8 months	68%	
1.2.3 Time taken to finalise Notifiable Data Breaches (NDBs)	80% of NDBs finalised within 60 days	77%	
1.2.4 Time taken to finalise My Health Record notifications	80% of My Health Record notifications finalised within 60 days	100%	
1.2.5 Time taken to finalise Information Commissioner (IC) reviews of FOI decisions made by agencies and Ministers	80% of IC reviews finalised within 12 months	78%	
1.2.6 Time taken to finalise FOI complaints	80% of FOI complaints finalised within 12 months	94%	

 Achieved  Not achieved

Source: OAIC Annual Report 2022-23

Stakeholders reflected positively on the OAIC and its approach

The OAIC conducted its first annual stakeholder survey in 2023 to establish a baseline for its regulatory performance.²⁶ The survey helped to assess the OAIC's performance against a number of performance measures.²⁷

Stakeholder feedback from the survey reflected a net positive view of the OAIC's collaborative efforts, giving an average score greater than 3 (where 1 = strongly disagree and 5 = strongly agree). The OAIC received its highest score for the regulation of CDR and its lowest score for the extent to which its activities are risk-based and data-driven.

Survey participants were generally satisfied with the OAIC's ability to:

- regulate and contribute to CDR (from the perspective of stakeholders involved in CDR regulation and engagement)
- raise awareness of opportunities to enhance online privacy legislation and online privacy risks
- provide guidance and advice on the operation of the IPS.

²⁶ The survey received responses from 102 stakeholders that work with the OAIC on issues relating to FOI (47), privacy (45) and CDR (10).

²⁷ These performance measures are: Effectiveness of the OAIC's contribution to the regulation of the Consumer Data Right; Effectiveness of the OAIC's contribution to the advancement of online privacy protections and policy advice; Effectiveness of the OAIC's advice and guidance on FOI obligations and the IPS in supporting government agencies to provide public access to government-held information; The extent to which the OAIC's regulatory activities demonstrate a commitment to continuous improvement and building trust; Extent to which to OAIC's regulatory activities demonstrate collaboration and engagement; and Extent to which the OAIC's regulatory activities are risk-based and data-driven.

3 Drivers of change

A range of economic, technological, social and political drivers will play key roles in shaping demand for the OAIC's work and its effectiveness as a regulator into the future. This chapter explores these drivers in detail and considers some of the likely implications for the OAIC's future regulatory strategy and elements of its operating model. It also provides important context for the findings and recommendations throughout this Strategic Review report.

Figure 18 | Relevant questions from the Terms of Reference

- How can the OAIC best respond to the likely continuing growth to the volume and complexity of its core statutory workload?
- How can the OAIC remain effective as a regulator in responding to changing technology, the growth of the digital economy and increasing cyber crime?

Figure 19 | Summary of key findings

TECHNOLOGICAL DRIVERS OF CHANGE

- Technological shifts will lead to new risks to privacy, and growing individual and community expectations that the OAIC will respond. As the digital transformation of our economy accelerates, the volume of data managed by entities regulated by the OAIC will continue to expand and the methods used to process this data will become ever more complex.
- Further developments in AI will have a profound impact on personal privacy. In response, the OAIC will need to develop regulatory guidance and enforce stricter controls on data sharing in respect of regulated entities.
- New technologies will challenge traditional frameworks for the protection of personal information. For example, biometric authentication and profiling systems continually collect vast amounts of data and are increasingly common. The OAIC's regulatory guidance will need to keep pace with these changes and provide clarity on emerging technologies and their potential impact on privacy.
- Data breaches are becoming larger in scale and more frequent amid growth in the digital economy and increasingly sophisticated cyber attacks. In response, the OAIC will need to play a role in ensuring organisations that collect personal information secure it effectively.
- Cyber crime is becoming more sophisticated and widespread, raising the risks to personal data security. The OAIC will need to contribute to government cyber security efforts and raise awareness through education initiatives.

SOCIAL DRIVERS OF CHANGE

- Changes in societal expectations are contributing to a desire for government to do more to uphold privacy and information access rights. Most Australians are now highly aware of their privacy rights due to recent large-scale data breaches, and they understand their right to access information held by public entities.
- The vast majority of Australians would like government agencies to act and do more to protect their personal information, including through legislative change. These expectations will likely lead to an increase in the OAIC's workload in relation to upholding privacy protections.

POLITICAL DRIVERS OF CHANGE

- The Government's expectations of the OAIC have evolved in response to increasing privacy harms. The OAIC is expected to take an approach that balances education of regulated entities to support voluntary compliance with enforcement to promote public confidence in the regulatory activities of the agency.
- Significant legislative and policy reforms and reviews – particularly the Privacy Act Review – will place greater demand on the OAIC. The proposed reforms from the Privacy Act Review will broaden the OAIC's enforcement powers and require updated regulatory guidance.
- The FOI Senate Inquiry's suggested reforms may require the OAIC to increase its engagement with agencies, meaning it will need to prioritise its efforts to develop guidance and build the capacity of decision-making agencies.
- In other areas of the OAIC's remit, expansions in scope and changes in legislation for CDR and Digital ID will require updated guidance.

The operating environment is changing – in particular, the rapid growth of the digital economy and advances in AI will have a profound impact on personal privacy

The privacy landscape for the OAIC over the next decade is likely to look markedly different to that of the past ten years. Advances in technology and the ongoing growth of the digital economy are expected to have a profound impact on personal privacy. Rapid growth in the sophistication and application of AI, new technologies such as biometric authentication and profiling, and the likelihood of larger and more frequent data breaches and increased cyber crime are combining to create a more complex and faster-evolving operating environment for the OAIC.

Societal expectations in relation to privacy protections are changing as technology evolves and data breaches become more frequent and more significant in their associated harms. Eighty-nine per cent of respondents to the Australian Community Attitudes to Privacy Survey 2023 would like government agencies to act and do more to protect their personal information.

Community expectations around accountability and transparency are increasing, with 91 per cent of respondents to the 2023 Australian Government Information Access Survey indicating it was important to them to have the right to access government information, up from 84 per cent in 2019.²⁸

In response to rapidly evolving technologies and societal expectations, the Government has initiated several reviews and reforms – most notably the Privacy Act Review – that will shape the OAIC's future functions and priorities.

Taken as a whole, these technological, social and political trends are expected to place increased demand on the OAIC's functions. The impact of these trends on the OAIC's functions is summarised at a macro level in Figure 20. The most significant impacts will be to the OAIC's privacy functions, as economy-wide digital transformation leads to vast amounts of data being hosted online, increasing the potential for large-scale data breaches and the need for enforcement action against regulated entities.

The remainder of this chapter explores technological, social and political trends that will shape the size and complexity of the OAIC's future statutory workload.

²⁸ [Australian Government Information Access Survey 2023](#).

s47C

3.1 Technological drivers of change

Technological shifts will lead to new risks to privacy and a growing expectation among individuals and the community that the OAIC will respond

As the digital transformation of our economy accelerates, the volume of data managed by entities regulated by the OAIC will continue to expand and the methods used to process this data will become ever more complex.

Advances in AI and machine learning will lead to regulated entities using more sophisticated data processing techniques. This will place pressure on the OAIC to provide advice and develop guidelines on how technologies can be developed, used and stored in ways that meets privacy obligations.³⁰ Data breaches are becoming larger and more common as the amount of personal data being exchanged through digital platforms grows and rates of cyber crime increase. These breaches are linked to the regulatory context within which they occur, so the OAIC's actions and legislative reform will be important to prevent problematic data practices and behaviour by regulated entities.

Some of the most significant technological drivers of change and their likely implications for the OAIC in the coming years are summarised in Figure 21.

²⁹ Analysis assumes that the OAIC will see greater demand placed on some of its functions following the Government's decision in relation to the Privacy Act Review recommendations.

³⁰ Currently, it is unclear which regulator or regulatory scheme will address emerging issues linked to AI safety and AI ethics. In the absence of a dedicated AI regulator, the OAIC is well positioned to have a role in minimising harms from AI while maximising benefits.

Figure 21 | Technological drivers of change and the implications for the OAIC

Driver	Description	Evolving risk landscape	s47C
Growing use of AI	<ul style="list-style-type: none"> Developments in AI will have a profound impact on personal privacy. Generative AI and large language models can collect personal data by making semi-hidden information more visible through reidentification, challenging the effectiveness of traditional privacy protections.³¹ AI tools can combine personal information with misleading information, which will pose a new type of threat to individual privacy. Like other participants in the economy, governments are increasingly using technology like AI to support decision-making. 	<ul style="list-style-type: none"> Without greater regulatory guidance on the use of personal information in AI and enforcement of AI-related privacy breaches, there is potential for large-scale erosion of individual privacy. The risk of AI tools being used to breach privacy is growing. Among Australian businesses, 68 per cent have already implemented AI technologies and a further 23 per cent are planning to implement them in the next 12 months.³² Trust in government could be reduced without greater transparency in relation to AI-enhanced government decision-making. 	s47C
New technologies that collect personal information	<ul style="list-style-type: none"> New technologies will challenge traditional frameworks for the protection of personal information. Biometric authentication and profiling systems continually collect vast amounts of data. This increases the volume of data to be protected and introduces potentially new forms of personal information that will need to be regulated. 	<ul style="list-style-type: none"> Personal information could be hacked and misused without consequences if new technologies continue to be used to collect this information. New technologies are collecting large volumes of personal information, with 83 per cent of Australians willing to use at least one biometric security technology in 2020.³⁴ 	s47C

³¹ [Problematic Interactions between AI and Health Privacy](#).

³² [CSIRO Australia's AI Ecosystem Momentum Report \(Feb 2023\)](#).

³³ [Safe and responsible AI in Australia consultation: Australian Government's interim response](#).

³⁴ [Australian Institute of Criminology – Changing perceptions of biometric technologies](#), 2021.

Driver	Description	Evolving risk landscape
Larger and more frequent data breaches	<ul style="list-style-type: none"> Data breaches are becoming larger in scale and more frequent amid growth in the digital economy and increasingly sophisticated cyber attacks. Breaches are increasingly occurring in the health and financial services sectors. Increasing amounts of data are expected to be collected in these sectors, including as part of the expansion of My Health Record. 	<ul style="list-style-type: none"> If data breaches are left unchecked and not investigated thoroughly, risk of identity theft and fraud will increase and there will be a loss of public trust in digital services and institutions. The risk posed by these breaches is large and growing, with significant data breaches resulting in millions of Australians having their information stolen and leaked on the dark web in 2022.³⁵ The most recent data shows that around 70 per cent of breaches are the result of malicious or criminal attacks.³⁶
Increasing cyber crime	<ul style="list-style-type: none"> Cyber crime is becoming more sophisticated and widespread, raising the risks to personal data security. Phishing, ransomware attacks and other forms of malicious activities are aimed at illegally accessing and exploiting personal data. 	<ul style="list-style-type: none"> Without regulatory action, increasing cyber crime will lead to more significant financial and personal losses from cyber attacks. There were 94,000 cyber crime reports in 2022-23, reflecting a 23 per cent increase compared to the previous financial year.³⁷ Australians lost over \$3 billion to scams in 2022. This is an 80 per cent increase on total losses recorded the prior year.³⁸

³⁵ [ASD Cyber Threat Report 2022-2023](#).

³⁶ [Notifiable Data Breaches Report: January to June 2023](#).

³⁷ [ASD Cyber Threat Report 2022-2023](#).

³⁸ [Targeting scams: report of the ACCC on scams activity 2022](#).

³⁹ [2023-2030 Australian Cyber Security Strategy](#).

s47C

3.2 Social drivers of change

Changes in societal expectations are contributing to a desire for government to do more to uphold privacy and information access rights

Societal expectations of individual privacy protection are changing as Australians become increasingly aware of their privacy rights and the importance of personal information security.⁴⁰ Awareness has grown following a number recent high-profile and large-scale data breaches that focused attention on online privacy and forced individuals to reflect on how their personal information is stored, managed and shared online.

The latest Australian Community Attitudes to Privacy Survey found that 62 per cent of Australians view the protection of their personal information as a major concern, but only 32 per cent feel in control of their data privacy. As a result, expectations about OAIC and broader government action are growing – 89 per cent of Australians would like government agencies to do more to protect their personal information, including through legislative change.⁴¹

Levels of public engagement on privacy issues and awareness of privacy rights are likely to increase, resulting in the OAIC needing to deal with more enquiries and complaints. When significant privacy breaches occur, expectations of government intervention are likely to increase, putting extra pressure on the OAIC's enforcement capacity.

Similarly, there is increasing public awareness of the right to access information held by public entities. Among respondents to the 2023 Australian Government Information Access Survey, 91 per cent indicated it was important to have the right to access government information, up from 84 per cent in 2019.⁴² Among respondents to the Information Access and Community Attitudes Study, 83 per cent agreed that public access to government information improves transparency and accountability.⁴³ This awareness will likely lead to more individuals exercising this right, increasing the volume of IC reviews and FOI complaints. Societal expectations reflect that the public wants more action to prevent government entities from delaying public requests for information or dealing with these requests inadequately.

⁴⁰ [Australian Community Attitudes to Privacy Survey, 2023.](#)

⁴¹ [Australian Community Attitudes to Privacy Survey, 2023.](#)

⁴² [Australian Government Information Access Survey 2023.](#)

⁴³ Office of the Victorian Information Commissioner, Cross Jurisdictional Information Access Study, May 2022.

3.3 Political drivers of change

The Government's expectations of the OAIC have evolved in response to increasing privacy harms

The Government clearly articulated its priorities for the OAIC in the Attorney-General's 2023 Statement of Expectations. It expects the OAIC to promote and regulate the protection of personal information in line with the objects of the Privacy Act and access to information through the operation of the FOI Act.⁴⁴

The Government acknowledges the increasing importance of the online environment for the economy, education and social connections. It expects the OAIC to focus on regulatory activities to address privacy harms that arise from the practices of online platforms and services that impact individuals' choice and control; promote awareness of privacy risks; provide guidance on how to protect personal information online; and take an integrated approach to embedding compliance and enforcement policies, project planning and risk management activities in respect of CDR. The Government also expects the OAIC to address privacy breaches and deal with entities that are not complying with privacy obligations. It also expects the agency to promote awareness and provide guidance on privacy risks to regulated entities and individuals.⁴⁵

Significant legislative and policy reforms and reviews – particularly the Privacy Act Review – will increase demand on the OAIC

The OAIC's remit will expand if the Government implements its recent legislative and policy reforms, with the most significant being the Privacy Act Review.

Some proposals in the Privacy Act Review will materially change certain functions the OAIC performs and introduce new functions. The proposals seek to bolster privacy protections, adapt policy guidance to the changing technology landscape and expand the OAIC's enforcement capabilities – for example, by empowering the IC to issue civil infringement notices for low-level administrative breaches of the Privacy Act. The Government has agreed or agreed in principle to most of these proposals.

The expansion of CDR to more sectors of the economy will also intensify the OAIC's regulatory role, requiring further resourcing and specific CDR capabilities.

The recently completed FOI Senate Inquiry could see legislative and policy changes in relation to the IC review and complaint processes if some of the Senate committee's recommendations are accepted by Government.

s47C



⁴⁴ Attorney-General's Statement of Expectations, p 2.

⁴⁵ Attorney-General's Statement of Expectations.

The proposed Privacy Act Review reforms will broaden the OAIC’s enforcement powers and require updated regulatory guidance

The Privacy Act Review proposed reforms enhance privacy protections in a range of ways that will increase the effectiveness of the OAIC, which will have strengthened enforcement powers. Key proposals that are likely to materially increase the OAIC’s responsibilities are outlined in Figure 22. Many of these proposals are expected to be implemented over the coming years.

Figure 22 | Overview of key Privacy Act proposals agreed by the Government

PROPOSAL	GOAL
Proposal 25.10 The OAIC should conduct a strategic internal organisational review with the objective of ensuring the OAIC is structured to have a greater enforcement focus.	Greater enforcement focus
Proposal 25.9 Amend the annual reporting requirements in AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground of section 41.	Increased transparency
Proposal 28.1 Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.	
Proposal 25.1 Create tiers of civil penalty provisions to allow for better targeted regulatory responses.	
Proposal 25.2 Amend section 13G of the Act to remove the word ‘repeated’ and clarify what a ‘serious’ interference with privacy may include.	Risk-based enforcement approach
Proposal 25.11 Amend subsection 41(dc) of the Act so the Information Commissioner has the discretion not to investigate complaints where a complaint has already been dealt with by an EDR scheme.	

The proposals outlined in Figure 22 are those that have been agreed by the Government. Those that have been agreed in principle and are likely to have an impact on the OAIC are provided in Figure 23. These proposals are subject to further consideration by the Government, including stakeholder consultation and impact analysis. A detailed analysis outlining the potential changes to the OAIC from the proposed reforms is contained in Appendix D.

Figure 23 | Overview of key Privacy Act proposals agreed in principle by the Government

Change	Reform proposals	s47C	Type of work	s47C
Enhanced enforcement powers	Proposals 25.1, 25.2, 25.4, 25.5 and 25.10: Introduction of new civil penalty provisions, public inquiry powers and structure to have a greater enforcement focus		Ongoing	

s47C

s47C

Change	Reform proposals	s47C	Type of work
Data security and privacy guidance enhancement. <small>47</small>	Proposals 21.3, 21.5, 28.1 and 28.4: Enhanced guidance on data security, breach responses and cross-agency cooperation in enforcement	s47C	Ongoing
Organisational and operational reforms	Proposals 25.6, 25.9 and 25.11: Greater cooperation with other bodies and introduction of new reporting requirements	s47C	Ongoing
Automated decision-making and emerging technology regulation	Proposals 13.2, 13.3, 19.1 and 19.2: Development of guidance for new technologies, privacy impact assessments, and automated decision-making processes	s47C	One-off
Increased transparency in data handling	Proposals 23.1 and 23.5: Enhanced transparency requirements for overseas data flows and entities' data handling practices	s47C	One-off
Vulnerability and consent guidance	Proposals 17.1 and 17.2: Development of guidance on handling data of vulnerable individuals and consent processes	s47C	One-off

s47C

s47C

The key recommendations made by the FOI Senate Inquiry are listed in Figure 24, along with an assessment of their expected impact on the OAIC if they are accepted by the Government.

Figure 24 | Overview of potential reforms from the FOI Senate Inquiry

Area	Suggested reforms			
Education, monitoring and guidance	The OAIC prioritises efforts to develop guidance and strengthen pathways for people accessing personal information outside FOI			
The OAIC's functions	Move IC review functions and the FOIC to the Commonwealth Ombudsman's Office or remove IC reviews and allow applicants to appeal directly to the Administrative Appeals Tribunal (AAT)			
Culture	An independent external review should be conducted into the OAIC's culture			

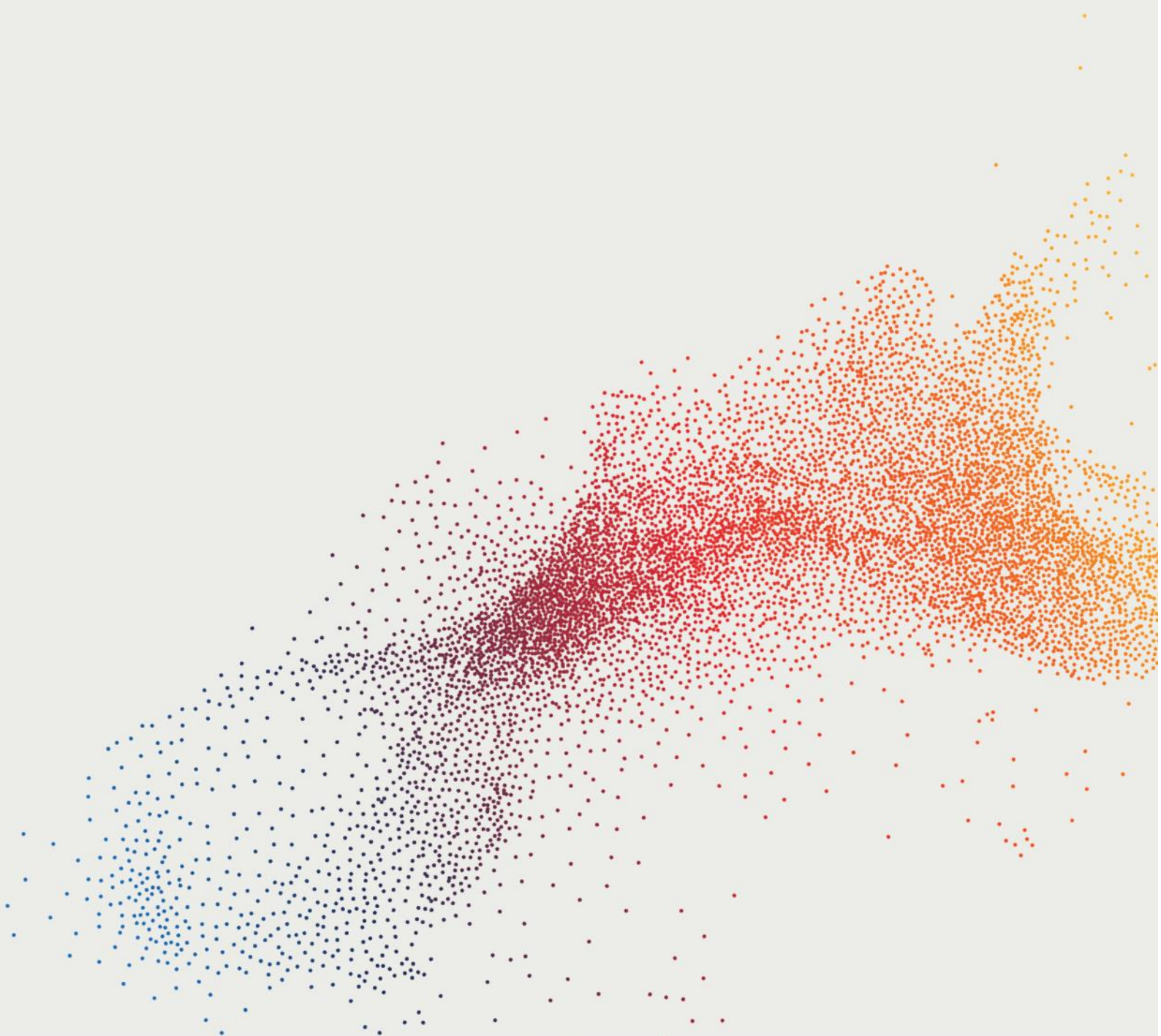
s47C

Expansions in scope and changes in legislation for CDR and Digital ID will require updated guidance

The OAIC will be impacted by the expected expansions in the scope of CDR and Digital ID. The expected impacts of these future changes on the OAIC are outlined in Figure 25 and Figure 26.

s47C

Part 2: The OAIIC's operating model



4 Strategy, regulatory posture and approach

Having a clear, modern and risk-based strategy, regulatory approach and posture will be critical to the OAIC's ability to respond to a growing workload and be an effective regulator of information. This chapter outlines the current state and recommendations for improvements that will enable the agency to achieve its purpose, improve its future functionality and best respond to changing demand on its workload as a result of the growing digital economy and increasing cyber crime.

Figure 27 | Relevant questions from the Terms of Reference

- How can the OAIC best respond to the likely continuing growth to the volume and complexity of its core statutory workload?
- How can the OAIC remain effective as a regulator in responding to changing technology, the growth of the digital economy and increasing cyber crime?
- What is the role of the OAIC in providing advice and reports to Government about privacy, information access and information management?

s47C



4.1 Introduction to effective regulatory strategy

The OAIC needs a clear regulatory strategy to be best positioned to respond to changes in technology and demand, and to maximise the potential impact of its regulatory action. Effective regulation is supported by a clear regulatory strategy. A regulatory strategy typically comprises a strategic plan, regulatory posture and approach. Each of these elements is explored in Figure 30.

Figure 30 | Overview of elements of regulatory strategy

ELEMENT	OVERVIEW
Strategic plan	<p>A strategic plan sets out the overarching purpose and vision, and what the regulator seeks to achieve, including:</p> <ul style="list-style-type: none"> regulatory purpose, articulating what it is, what it does and for whom. This should be derived from its legislative mandate and organisational context regulatory vision, identifying its desired future strategic objectives, identifying specific, longer-term goals it seeks to achieve.
Regulatory posture	<p>Regulatory posture describes where it will focus its effort. The regulator needs to decide what proportion of its activities will be about reacting to instances of non-compliance and what proportion will be proactive attempts to promote compliance. Some decisions around where to place regulatory emphasis are enshrined in the legislation administered by the regulator, but many involve considering the external operating environment and organisational priorities.</p>
Regulatory approach	<p>Regulatory approach is how the regulator uses its regulatory tools and powers to achieve its strategic plan and posture. It comprises:</p> <ul style="list-style-type: none"> how the regulator prioritises matters how the regulator exercises its regulatory functions in respect of the matters it prioritises. <p>A risk-based approach focuses resources and effort on the risks associated with non-compliance with rules, rather than the rules themselves. It is based on the notion that it is impossible to avoid all risks and that regulatory tools and powers should be used to effectively manage risks. One of the Regulator Performance Guide principles for best practice regulator performance is being 'risk-based and data-driven'.</p>

The analytical framework for the Strategic Review articulates the criteria we have used to:

- assess the effectiveness and appropriateness of the OAIC's current regulatory strategy
- identify changes that will enable the OAIC to respond to the likely continuing increases in the volume and complexity of its regulatory environment, and play an appropriate role in providing advice and reports to the Government.

These criteria and the associated tests are outlined in detail in Figure 31.

Figure 31 | Tests of effective regulatory strategy

CRITERIA	TEST
STRATEGIC PLAN	
Is clear and concise	Can the community, staff and regulated entities easily understand what the OAIC is seeking to achieve?
Is focused	Does the strategic plan set the OAIC's focus and direction and how it uses its regulatory powers and tools?

CRITERIA	TEST
REGULATORY POSTURE	
Articulates emphasis of effort	Does the regulatory posture describe where effort is focused and where the OAIC sits on the regulatory spectrum?
Reflects demand	Does the regulatory posture reflect current and future demand and expectations of the OAIC?
Aligns with strategic plan	Are regulatory tools and powers being used consistently to further the objectives in the strategic plan?
REGULATORY APPROACH	
Reflects risk of harm	Does the regulatory approach identify the greatest risks the OAIC is seeking to address?
Enables prioritisation	Does the regulatory approach prioritise high-risk matters with the greatest potential for harm?
Focuses powers and tools	Does the regulatory approach outline which powers and tools to apply to address that risk?

4.2 The strategic plan

The strategic plan outlines the agency's purpose and strategy for upholding information rights

The current strategic plan includes the elements expected of a regulator with the OAIC's remit. A high-level snapshot of the plan is shown in Figure 32. The OAIC's purpose, vision and key activities and/or strategic priorities have not changed since 2019.

Figure 32 | Summary overview of the current strategic plan

PURPOSE	Promote and uphold privacy and information access rights.			
VISION	To increase public trust and confidence in the protection of personal information and access to government-held information.			
STRATEGY	Prevent privacy harm and uphold the community's access to information rights in the areas of greatest impact and concern.			
KEY ACTIVITIES	Influence and uphold privacy and information access rights frameworks.	Advance online privacy protection for Australians.	Encourage and support proactive release of government information.	Take a contemporary approach to regulation.
SUCCESS MEASURES	The OAIC's regulatory outputs are timely.	The OAIC's activities support innovation and capacity for Australian businesses to benefit from using data, while minimising privacy risks for the community.	The OAIC's activities support government agencies to provide quick access to information requested and at the lowest reasonable cost, and proactively publish information of interest to the community.	The OAIC's approach to its regulatory role is consistent with better practice principles.
ENABLERS	Continuous improvement and building trust.	Adopting a risk-based and data-driven approach.	Collaboration and engagement.	

Source: OAIC's Corporate Plan 2023-24

Aspects of the plan already reflect an enforcement posture and risk-based approach. The strategy to 'prevent privacy harm and uphold the community's access to information rights in the areas of greatest impact and concern' is strong and reflects an intention to take a risk-based approach. This is bolstered by the OAIC's commitment to adopt a risk-based and data-driven approach to its activities in its key activity of 'taking a contemporary approach to regulation'.

s47C

4.3 The OAIC's regulatory posture

s47C



- A Major Investigations Branch was established in 2022-23. The OAIC has three open investigations – against Optus, Medlab and Medibank – in relation to significant data breaches. It launched its first civil proceedings in 2020 against Facebook and issued further proceedings against Australian Clinical Labs in 2023. Both proceedings are on foot in the Federal Court.
- The OAIC's Regulatory Action Committee (RAC) provides a forum for considering matters for enforcement. In recent years, matters identified through privacy assessment have been referred to the RAC and resulted in CII.
- The OAIC conducts assessments to monitor regulated entities' compliance with privacy obligations. These assessments enable identification of non-compliances and inform enforcement action.
- The OAIC conducted a CII and follow-up into the Department of Home Affairs' compliance with FOI processing timeframes in 2020. This investigation found shortfalls and made recommendations that have been implemented, significantly improving the department's FOI policy, procedures and outcomes for applicants.

s47C



s47C

The Government has provided strategic direction on the agency's changed regulatory posture in the Attorney-General's Statement of Expectations. It expects the OAIC to focus on addressing privacy harms, promote awareness of privacy risks and provide guidance to regulated entities and individuals.

In addition, the community and stakeholders expect more government intervention for both privacy and FOI (see section 3.2):

- The community would like government agencies to act and do more to protect their personal information (89 per cent of respondents to the Australian Community Attitudes to Privacy Survey 2023).
- Witnesses to the FOI Senate Inquiry called for a more responsive FOI culture, a proactive disclosure culture and stronger pathways for accessing personal information outside the FOI regime.
- Stakeholders who responded to the OAIC's first stakeholder survey would like to see more timely guidance and advice on the operation of the FOI Act.

4.4 The OAIC's regulatory approach

Regulatory approach puts regulatory posture into practice, by detailing how a regulator will use its tools and powers to deliver on the activities it decides to focus on under its regulatory posture. The OAIC's current regulatory approach has two key elements – its regulatory priorities and its regulatory action policies. Each element is discussed in this chapter, which also outlines the Strategic Review's recommended future regulatory approach for the agency.

4.4.1 Updating regulatory priorities will enable the OAIC to identify the highest risk matters for regulatory action

The OAIC has released its regulatory priorities

The OAIC published its regulatory priorities in 2023-24 to guide where it would direct resources. These priorities are set out in Figure 34. It uses these regulatory priorities to ensure that the OAIC's resources are focused on the prevention of privacy harm and upholding the community's access to information rights in the areas of greatest impact and concern.

Figure 34 | The OAIC's regulatory priorities

REGULATORY PRIORITIES	
1. Online platforms, social media and high privacy impact technologies	Harms which impact on individuals' choice and control, through opaque information practices or terms and conditions of service. Technologies and business practices that record, monitor, track and enable surveillance, and the use of algorithms to profile individuals in ways they may not understand or expect, with adverse consequences.
2. Security of personal information	Serious failures to take reasonable steps to protect information or report. Risks and mitigations have previously been publicised by the OAIC. Finance and health sectors.
3. Consumer Data Right	Coordinated compliance and enforcement activities by the OAIC and the ACCC. Ensuring that the fundamental privacy safeguards provided by the system are upheld by participants to protect consumers' information.
4. Proactive disclosure of government-held information	The need for agencies to make timely decisions and proactively disclose information to support an efficient access to information regime.

Source: [OAIC's Regulatory Priorities](#)

s47C

5 Governance

Governance will be an important enabler for the OAIIC to achieve its purpose and future functionality. This chapter outlines the Strategic Review's findings relating to governance. It considers the suitability of current governance arrangements in enabling the OAIIC to achieve its purpose and required future functionality. It also recommends amendments to governance arrangements.

Figure 38 | Relevant questions from the Terms of Reference

- To what extent is the OAIIC's governance suitable to achieve its purpose and future functionality?

Figure 39 | Summary of key findings

s47C

- The Strategic Review considered governance criteria, comparable models and legislative requirements to develop and refine options with the OAIIC Executive. The legislative requirements of the AIC Act, the Privacy Act, the FOI Act, the Public Service Act and the PGPA Act have also been considered.

s47C

s47C

The analytical framework for the Strategic Review articulates five criteria for the OAIC's governance arrangements, as set out in Figure 41. These criteria were tested and refined with the agency's Executive team. They were used by the Strategic Review team to test the suitability of the OAIC's current governance arrangements in achieving the agency's purpose and future functionality, and to inform recommendations related to its future governance arrangements.

Figure 41 | Assessing the suitability of the OAIC's governance

CRITERIA	TEST
Strategic alignment	To what extent do governance arrangements align with and enable the OAIC's overarching strategy and purpose to promote and uphold privacy and information access rights?
Respects decision-making role of Commissioners	To what extent are the decision-making roles of each Commissioner respected?
Show clear lines of accountability	Are there clear lines of accountability for each Commissioner and the governance structures that support them, in respect of the OAIC's remit?
Reserve Commissioner time for value-adding work	To what extent is the Commissioners' time reserved for value-adding work (decision-making and external-facing work, not operations)?
Supports integration	To what extent do governance arrangements support an integrated OAIC?

5.1 The OAIC's current governance

The OAIC's governance in recent years has been calibrated to several different Commissioner arrangements

The AIC Act provides for a three-Commissioner model that includes the IC, a PC and an FOIC. The IC is also the agency head for the purposes of the Public Service Act and is the accountable authority for the purposes of finance law provided under the PGPA Act.

The IC holds a unique role among the three Commissioners as agency head and accountable authority. As agency head, the IC has employer powers, and as accountable authority the IC is responsible for ensuring the OAIC is governed in a way that promotes the proper use of public resources and achieves the agency's purposes and financial sustainability.

The OAIC's current governance arrangements have been developed over time to meet the needs of the different Commissioner models it has operated under. In recent years, the IC has also fulfilled the PC role. Between 2014 and 2021, when the FOIC role was vacant, the IC also carried out those functions. Between 2021 and early 2024, three different people carried out the FOIC role, with only one of them formally appointed to the role.

The OAIC's current governance arrangements include a number of committees that advise the IC in relation to operational and strategic matters and statutory decision-making:

- The **Executive Committee** supports the IC to achieve the strategic objectives of the OAIC by ensuring executive focus on privacy and FOI priorities. The committee is chaired by the IC and comprises OAIC Commissioners and staff members at Senior Executive Service (SES) level.
- The **Operations Committee** ensures executive oversight of the management of the OAIC and several subcommittees (including the Health, Safety and Wellbeing Committee, the Security Governance

Committee, the Information Governance Committee and the OAIC Consultative Forum). The committee is chaired by the OAIC Deputy Commissioner and comprises SES-level and some Executive Level 2 staff members.

- The **Audit and Risk Committee** advises the IC on the appropriateness of the OAIC's financial reporting, performance measurement, system of risk oversight and management, and systems of internal control.
- The **Regulatory Action Committee** advises the IC on suitable regulatory responses to significant privacy risks.
- The **Diversity Committee** advises the IC on strategies and plans to promote a fair, inclusive and productive workplace.

The OAIC will soon return to a three-Commissioner model. In May 2023, the Government announced the appointment of a standalone FOIC and PC, increasing the permanent number of statutory information officers from one to three. The formal appointment of these two new Commissioners was announced in November 2023 and they will commence at the OAIC around the time of finalising this Strategic Review, in February 2024.

s47C



6 Organisational structure

A fit-for-purpose structure will be a critical enabler for the OAIC's future effectiveness and its ability to fulfil its purpose. This chapter describes the current structure and its alignment with the best practice criteria in our analytical framework. It also provides potential structural options that the OAIC could adopt going forward in response to several key drivers of change.

Figure 43 | Relevant questions from the Terms of Reference

- To what extent is the OAIC's structure suitable to achieve its purpose and future functionality?

Figure 44 | Summary of key findings

- The OAIC's current structure focuses firstly on the division between privacy and FOI work and then by the necessary functions associated with each regulated area. This structure reflects the extensive growth in the agency's staff and the areas it has regulated over the past ten years.
- The OAIC has made structural changes in recent years to support an increased enforcement focus. This includes standing up the Major Investigations Branch in October 2022 to facilitate large-scale investigations in a focused and direct manner.

s47C

s47C

s47C

6.1 The OAIC's current structure

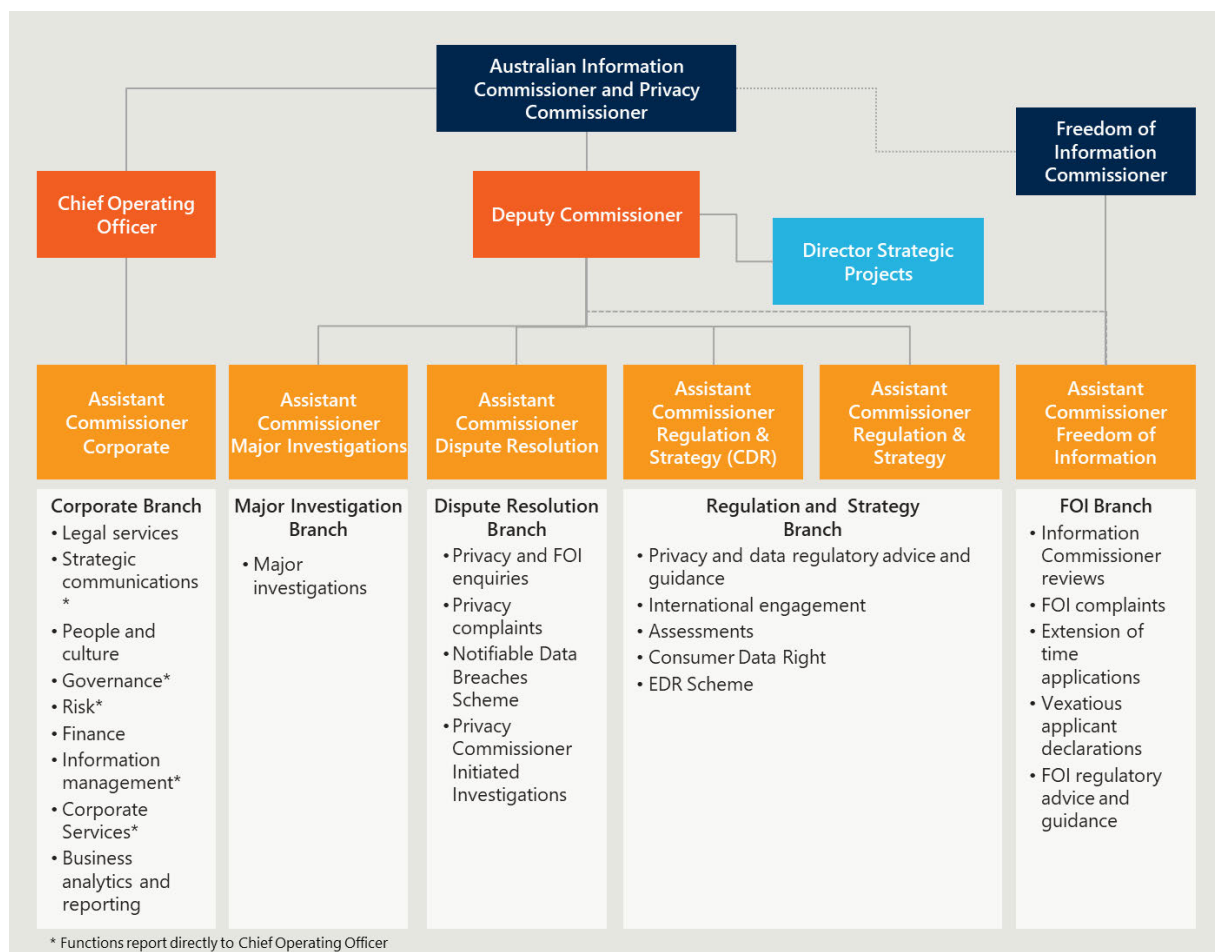
The current structure is organised by regulated area, with some functional elements

The current structure divides the agency into branches by regulated area and corporate functions. Figure 47 provides a high-level overview of this structure and the functions completed by each branch, which are split by regulated area and by the type of action completed.

This structure focuses firstly on the division between privacy and FOI work and then by the necessary functions associated with each regulated area. This structure reflects extensive growth in the agency's staff and the areas it has regulated over the past ten years.

Privacy and FOI, and their associated branches, are structured quite differently. FOI is organised as a single branch. Privacy is split across four branches: Major Investigations, Dispute Resolution, Regulation and Strategy, and Regulation and Strategy (CDR). The four privacy branches have overlapping areas of function, with Major Investigations covering large-scale privacy CIIs and NDBs, and the two Regulation and Strategy branches split by CDR-associated functions and Privacy (non-CDR functions). Within the current structure, all non-corporate branches report to the Deputy Commissioner, with the Corporate Branch reporting to the COO.

Figure 47 | The OAIC's current organisational structure



Recent structural changes supported greater emphasis on enforcement and increased supporting functions

Structural changes in recent years support an increased focus on enforcement. This includes standing up the Major Investigations Branch in October 2022 to facilitate a focused and direct approach to large-scale investigations, including into the Optus and Medibank data breaches. This branch receives cases through the Dispute Resolution Branch's work or by direction of the Commissioner or the broader Government. As such, it requires strong communication with the Dispute Resolution Branch to ensure that appropriate cases are picked up.

Other structural changes to the Corporate Branch, in FY23, introduced the COO to oversee and support the branch. The branch has expanded to include the Business Analytics, Data and Reporting team, which oversees data collection and analysis. Recently, this team has been supported by the Technical Services Systems Review team, which oversaw the Systems Review of the OAIC.

These changes have supported the OAIC as the scope and volume of its work has increased. In particular, the separation of the Major Investigations Branch and its associated investigations has streamlined its work and ensured that the Dispute Resolution team is not overwhelmed by a backlog of cases associated with these investigations. For the corporate functions, the changes have helped increase the agency's data knowledge base.

7 Organisational capability

Attracting and retaining the right people with the right skills and capabilities, and fostering an inclusive and high-performing culture, will play a critical role in enabling the OAIC to deliver on its regulatory strategy. This chapter outlines the Strategic Review's findings on the agency's organisational capability, the extent to which it is suitable to achieve the agency's purpose and future functionality, and outlines recommended amendments.

Figure 49 | Relevant questions from the Terms of Reference

To what extent are the OAIC's organisational capabilities suitable to achieve its purpose and future functionality?

Figure 50 | Summary of key findings

WORKFORCE CAPABILITY AND SKILLS

- The OAIC's workforce has undergone significant changes over the past three years. It has increased significantly in size, from 105 in 2020 to 162 in 2023. It has also moved towards a permanent hybrid working model and transitioned from being predominantly Sydney-based to being dispersed across the country. Turnover has been high across all branches over the past two financial years.
- These factors have posed challenges related to building and retaining corporate memory and know-how related to core functions.

s47C

EMPLOYEE EXPERIENCE

- The OAIC tends to attract people who are motivated to work at the agency because of its mission and purpose. Most staff therefore feel a strong sense of connection to the agency and to their work. Most staff also feel that the OAIC has an inclusive culture and workplace.
- Most staff feel motivated and challenged by their work – although those undertaking more repetitive work tend to feel less engaged. Given the relatively small size of the agency, its specialist nature, and its modest investment in learning and development, many staff feel that there are limited opportunities to learn and grow.
- Most staff feel the agency cares about their wellbeing, although many also report feeling stressed and overworked. The latter sentiment is more common in the FOI and Corporate branches.
- Remuneration is low compared with many other agencies and well behind equivalent state government and private sector roles – particularly in the legal and technology sectors. The

OAIC therefore needs to compete in the labour market on other factors such as purpose and workplace conditions. Most staff appreciate the OAIC's flexible work environment.

s47C

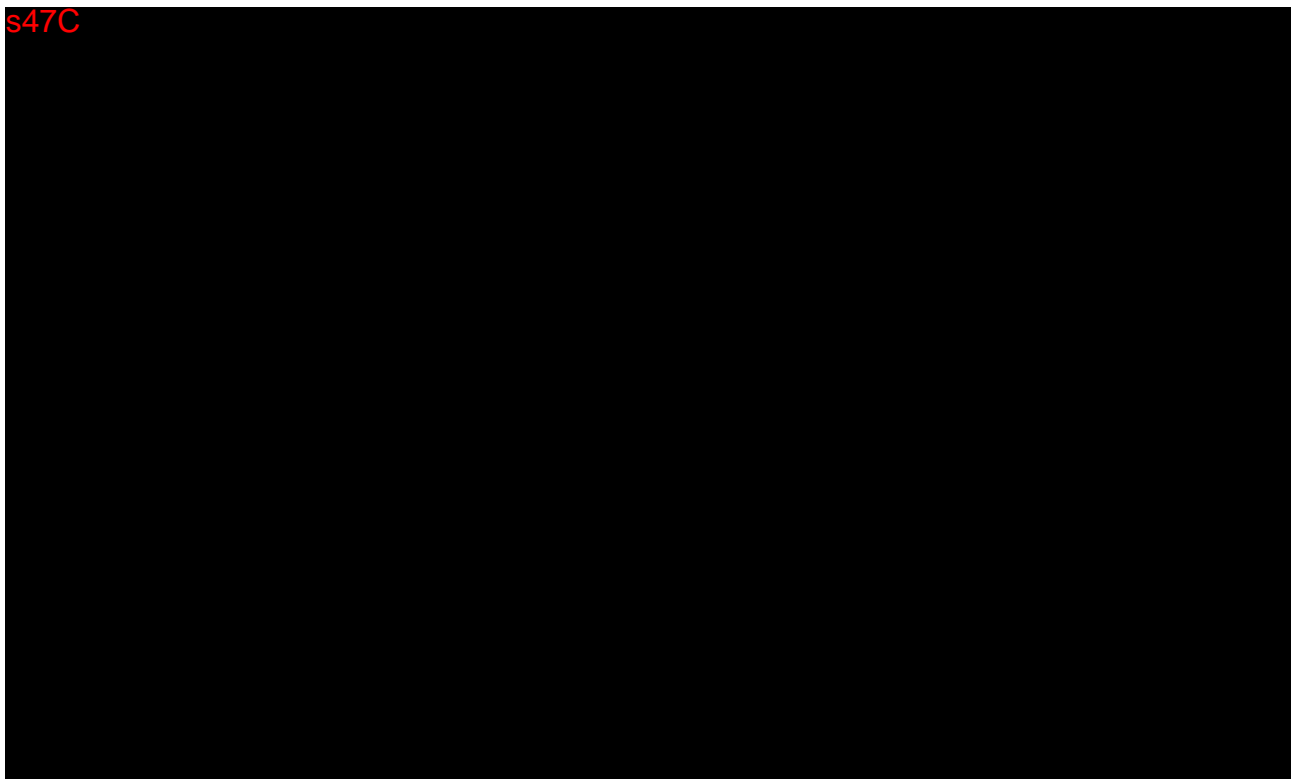


SOURCING EXTERNAL CAPABILITIES

- In recent years, the OAIC has substantially increased its spending on external legal support, from \$1.1 million in FY20 to \$5.7 million in FY23, as the agency has focused more on enforcement. s47C



s47C



s47C

7.1 Workforce capability and skills

Significant workforce transformation over the past few years has made it challenging to build and retain corporate memory

The OAIC's workforce has undergone major changes over the past three years, with a significant increase in FTE (from 105 in 2020 to 162 in 2023) and the move towards a permanent hybrid working model. Before 2020, most staff worked in the OAIC's Sydney office; now they are more widely spread across the country. The OAIC's geographic footprint by branch is shown in Figure 53.

Figure 53 | FTE by location and branch

Location	Corporate	Dispute Resolution	FOI	Major Investigations	Regulation and Strategy	Executive	Total
ACT	5	1	5	–	1	1	12
NSW	18	41	16	9	21	1	106
NT	–	–	1	–	–	–	1
Qld	7	2	3	–	3	1	17
SA	5	3	–	–	6	–	14
Tas	–	1	–	1	1	–	3
Vic	10	3	1	–	4	1	19
WA	–	1	2	–	–	–	3
Total	45	51	28	10	35	4	173

Source: OAIC-supplied data as at September 2023

At the same time as the OAIC's workforce has become larger and more geographically dispersed, the agency has experienced high levels of turnover across all branches over the past two financial years, as shown in Table 11. The OAIC's digital platforms have therefore been critical in enabling collaboration between teams and in onboarding new staff.

Table 11 | Staff attrition rate by branch

Branch	2021-22 (%)	2022-23 (%)
Dispute Resolution	33	20
Regulation and Strategy	38	16
Freedom of Information	58	36
Corporate	54	39
Corporate (Legal Services)	38	42
Executive	14	22
Total	40	25

Source: data provided by OAIC

The agency's workforce has higher proportions of female and part-time workers, and those from non-English speaking backgrounds, relative to APS averages. See Appendix G for further details of key workforce metrics for the agency, relative to APS averages.

OAIC staff on average had a lower median length of service and had a higher exit rate of ongoing employees in 2022-23 relative to APS averages. This is particularly the case among more junior employees, which has resulted in two distinct cohorts of staff at the agency. Close to half of the leadership team have spent a large part of their career at the agency, whereas more junior staff have typically spent significantly less time there and in the APS generally.

Taken together, the above factors have posed challenges in recent years related to building and retaining corporate memory and know-how about core functions.

s47C

Figure 55 | Feedback from OAIC staff about their connections to work

Purpose	Leadership	Inclusion
Employee connection to the organisation’s mission, purpose and strategy	Employee perceptions of vision, commitment and support of the organisation’s leaders	Employee sense of belonging and perceived safety in bringing whole of self to work

- 80 per cent of staff are proud to work for the OAIC.
- 89 per cent feel committed to the OAIC’s goals.
- Staff identified the following sources of pride:
 - commitment and dedication to the values of upholding privacy and FOI
 - interesting work that delivers a positive community impact
 - working with smart, dedicated colleagues in a respectful and collegiate manner.

- The results of the APS Census indicate that the majority of OAIC staff are happy with the leadership of their immediate supervisor.
- The APS Census revealed staff generally have a positive attitude towards their immediate SES manager.
- Staff perceptions about the leadership of the OAIC’s broader SES cohort are less positive than in 2022 – although the OAIC’s results are still better than Census benchmarks.

- 86 per cent of staff feel that the OAIC supports and actively promotes an inclusive workplace culture – an increase of 10 per cent from the 2022 APS Census results.

- s47C [Redacted]
- s47C [Redacted]

s47C [Redacted]

s47C

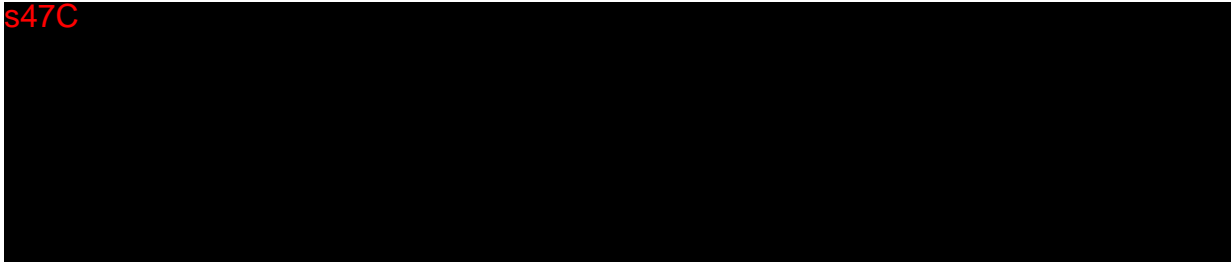
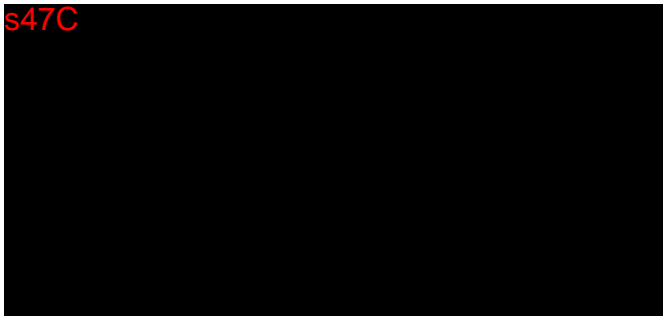


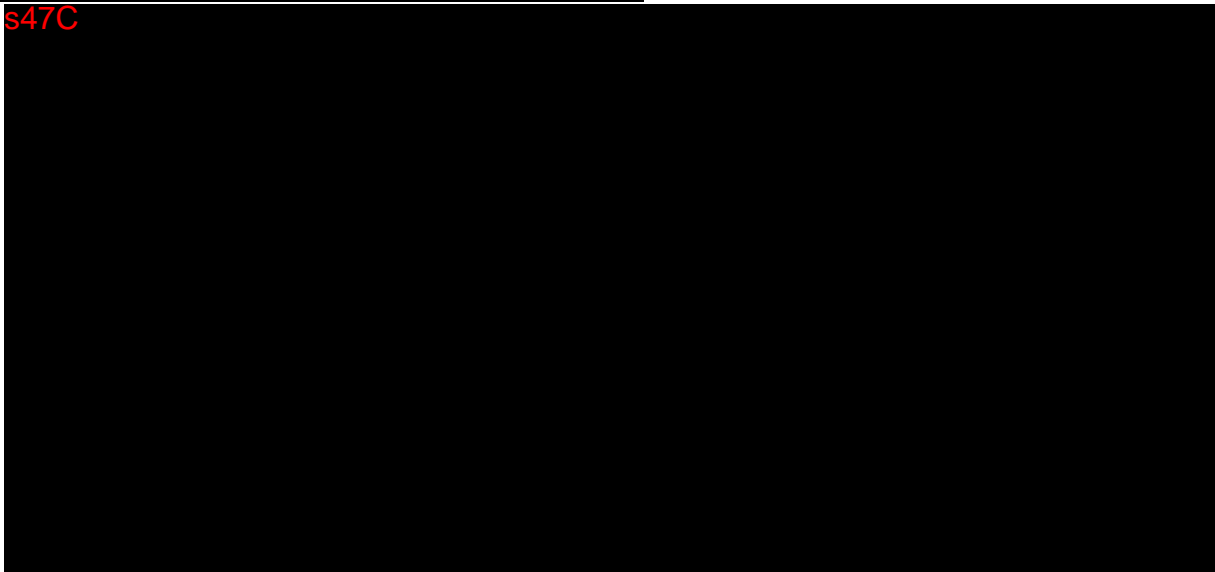
Figure 57 | Feedback from OAIC staff about the employee experience

Wellbeing	Infrastructure
<p>The focus on work-related safety and creation of a culture fostering wellbeing</p>	<p>The physical and digital resources available for employees to perform their roles</p>
<ul style="list-style-type: none"> • The OAIC scores well on APS Census questions related to promoting and communicating wellbeing. • s47C [Redacted] • The proportion of staff who agreed or strongly agreed that they felt burnt out by their work increased in the 2023 APS Census results. • In the 2023 results, the instances of staff who said they always or often find their work stressful also increased. 	<ul style="list-style-type: none"> • Only 38 per cent of OAIC staff who responded to the APS Census agreed that their workgroup has the tools and resources they need to perform well – substantially below the APS benchmark and other similar agencies. <p>s47C [Redacted]</p>

s47C



s47C



s47C

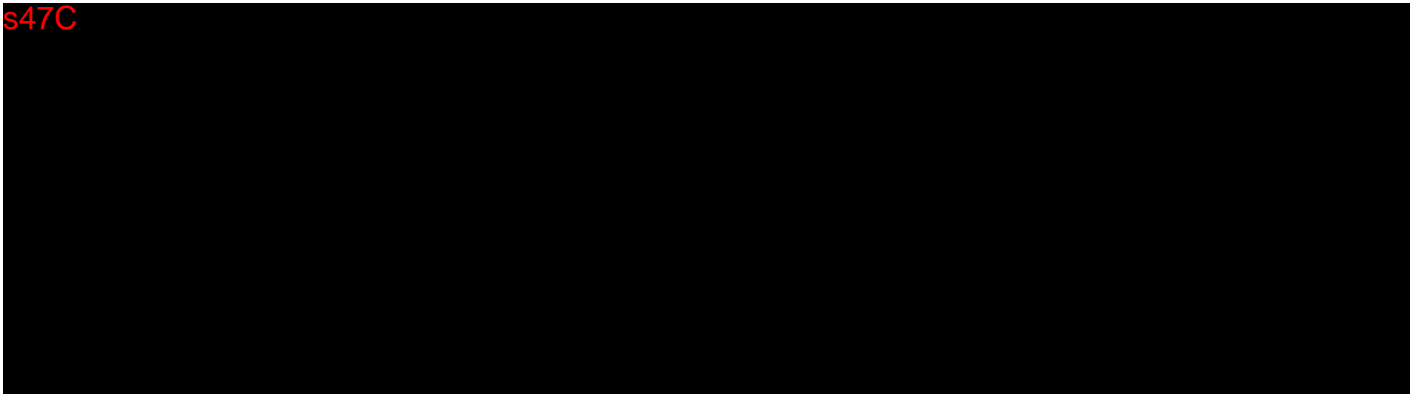
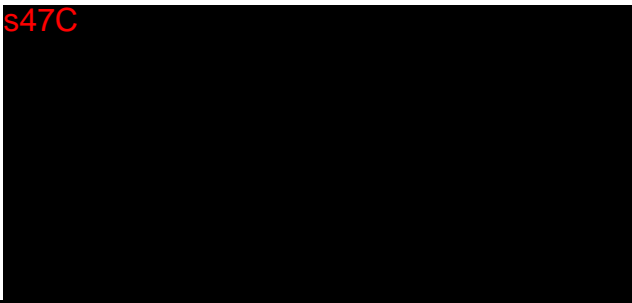


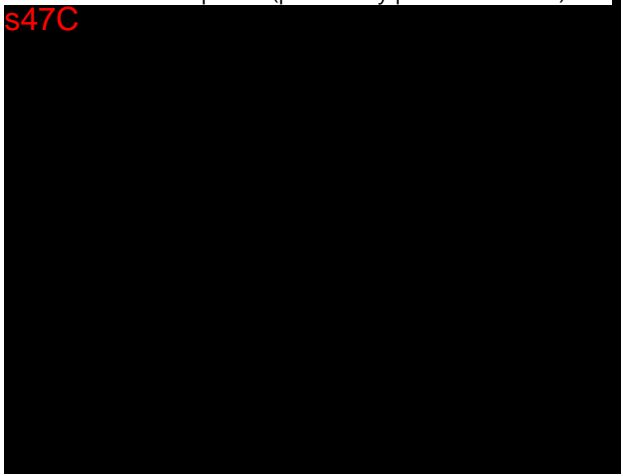
Figure 58 | Feedback from OAIC staff about how they are rewarded and recognised

Compensation	Conditions
The fixed and variable remuneration for employees	Work settings, including flexibility and work-life balance

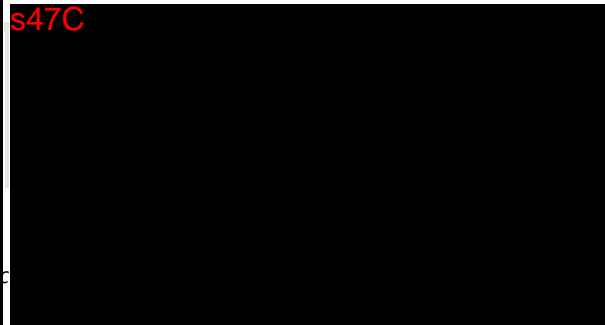
- Only 41 per cent of OAIC staff feel they are fairly remunerated (for example, salary and superannuation) for the work they do – well below all APS Census benchmarks.
- Current OAIC pay scales are in the lower third of APS agencies. This makes it hard for the OAIC to compete with other agencies, other jurisdictions (particularly the NSW Government) and private sector companies (particularly private law firms).



s47C



- 43 per cent of APS Census respondents said their workloads are well above capacity (well above all Census benchmarks).



7.4 Sourcing external capabilities

The OAIC currently relies on external legal providers to undertake a range of core activities

In recent years, the OAIC has substantially increased its spending on external legal support, from \$1.1 million in FY20 to \$5.7 million in FY23, as the agency has shifted focus to enforcement and increased its litigation activities.

Some activities currently completed or facilitated by external legal providers include:

- repeatable, non-specialised work such as document review is completed by legal secondees
- document and evidence storage (a capability that the OAIC currently lacks due to systems limitations)
- witness examination recordings for assessments and major investigations, to ensure that recordings are held locally and according to OAIC timeframes.

s47C



8 Processes and systems

The extent to which processes and systems are efficient and contemporary will play a critical role in the OAIC's ability to respond effectively and efficiently to the likely continuing growth in the volume and complexity of its core statutory work. This chapter assesses the agency's current processes and systems, and identifies opportunities to refine key processes in ways that should yield significant efficiencies and enable the agency to deliver on its updated strategic plan (see chapter 4).

Figure 61 | Relevant questions from the Terms of Reference

- How can the OAIC best respond to the likely continuing growth in the volume and complexity of its core statutory work?
- How can resource allocation be optimised to maximise efficiency and support the OAIC's statutory functions?

s47C



Table 12 | Processes analysed in the Strategic Review

PRIVACY PROCESSES	FOI PROCESSES
<ul style="list-style-type: none"> • Privacy complaints • Data breach notifications • CIs • Privacy assessments • CDR assessments 	<ul style="list-style-type: none"> • IC Reviews • FOI complaints • CIs

8.1 The OAIC's current processes and systems

Key processes and functions are derived from the OAIC's statutory responsibilities

The OAIC's core statutory functions are the management of the Privacy Act across the public and private sectors and oversight of the operation of the FOI Act.⁶¹ The most significant processes in terms of collective resourcing are those associated with privacy complaints and IC reviews (as discussed further in chapter 2). There is no statutory timeframe for completion of these processes.

The five-stage privacy complaints process involves up to four teams

Privacy complaints follow a process performed by four separate teams: Early Resolution, Conciliation, Investigation and Determination. Each team completes a version of the stages that are relevant to their individual roles in the process, as outlined in Figure 65. The Early Resolution team receives and registers complaints and attempts to resolve the most straightforward matters. If early resolution isn't possible, the complaint is transferred to the Conciliation or Investigation team, depending on the specific circumstances. The matter is then progressed before ultimately being resolved through a determination, if appropriate. Similar to IC reviews, many privacy complaints are resolved before reaching a determination and this can be because:

- They are assessed to be invalid (for example because the information at the centre of the complaint does not fall within the definition of 'personal information' as per the legislation), or
- the complainant hasn't contacted the relevant organisation or agency that mishandled their information before lodging a complaint with the OAIC.

⁶¹ OAIC, What we do, <https://www.oaic.gov.au/about-the-OAIC/what-we-do>

Figure 65 | Privacy complaints case process



Source: OAIC privacy complaint process workflows

IC reviews can pass through up to three stages

IC reviews follow a process that is largely dictated by the procedural requirements outlined in Part VII of the FOI Act. This includes levels of delegation to clear and complete process steps, as well as specific steps that must be undertaken during an IC review. This process can cover up to three stages – as outlined in Figure 66. Not all cases require the full three stages – a material share are closed before reaching the decision and finalisation stage. This can be for reasons including:

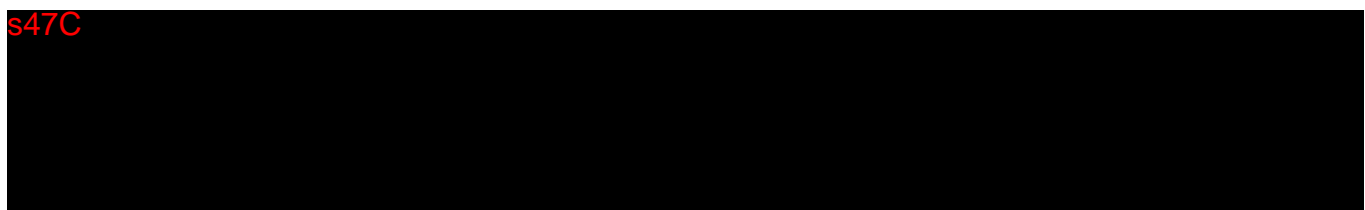
- the matter is deemed not to be an IC review (for example, if the time for making a decision on a request for access to a document has expired and an applicant has not been given a notice of decision.⁶²)
- the application is declined (for example, if the review is deemed to be lacking in substance, misconceived, not made in good faith, vexatious or frivolous), or
- the applicant withdraws their application.

Figure 66 | IC review case process



Source: OAIC IC review process workflows

s47C



⁶² OAIC, FOI Guidelines, <https://www.oaic.gov.au/freedom-of-information/freedom-of-information-guidance-for-government-agencies/foi-guidelines/part-3-processing-and-deciding-on-requests-for-access#deemed-decisions>

9 Resourcing and resource allocation

As an independent statutory agency, the OAIC is resourced through government appropriations to oversee government information policy functions, access to government-held information and promote data protection in the public and private sectors. This chapter examines the OAIC's current resourcing. It considers whether resourcing is sufficient and applied efficiently, and recommends changes to better enable the agency to achieve its purpose and future functionality.

Figure 72 | Relevant questions from the Terms of Reference

- To what extent is the OAIC's resourcing suitable to achieve its purpose and future functionality?
- How can resource allocation be optimised to maximise efficiency and support the OAIC's statutory functions?

Figure 73 | Summary of key findings

- The OAIC's resourcing has increased substantially in recent years to support the growth in workload and the resulting increase in staff. s47C [REDACTED] The agency's total resourcing (ongoing and terminating funding) has increased from \$10 million to \$46 million over the past ten years. This includes a 117 per cent increase in ongoing funding over the same period.
- This additional funding has come with a range of additional responsibilities. The bulk of this funding has been provided to allow the OAIC to deliver specific additional activities or functions (for example, My Health Record regulation, CDR, Digital ID and specific investigations).

s47C

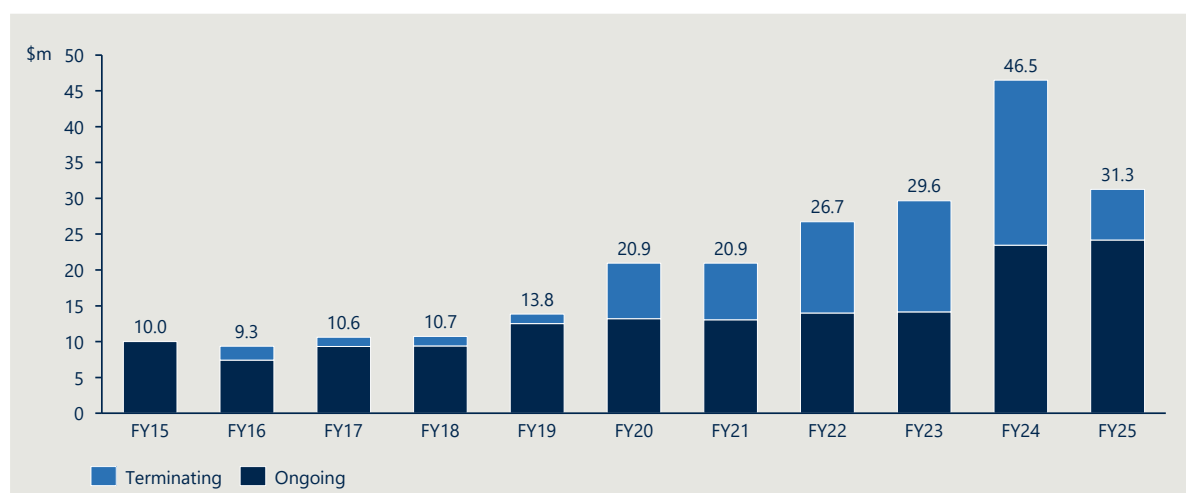
9.1 Current resourcing levels

The OAIC's total resourcing (ongoing and terminating funding) has increased significantly over the past ten years, from \$10 million to \$46 million, enabling the agency to hire staff to manage its growing workload. This includes a 117 per cent increase in ongoing funding over the same period, and a considerable funding increase since 2019 for both ongoing base and terminating functions. The growth reflects the increase in the OAIC's workload and responsibilities, as outlined in chapter 2. This includes ongoing funding for supporting the introduction and privacy function of CDR across three sectors of the economy, terminating funding for managing privacy functions of new government initiatives (Digital ID and My Health Record), and the commencement of major investigations into Optus, Medibank and Latitude.

s47C

⁶⁵ The Review benchmarked the internal and external OAIC's legal functions against the average internal legal expenditure share of total expenditure by ACCC, ASIC, AUSTRAC, APRA and ATO between 2017-18 and 2021-22 as outlined in the [Commonwealth Legal Services Expenditure Report](#).

Figure 76 | OAIC resourcing profile



Source: Budget Measures: Budget Paper 2 2022-23 (March), Budget Measures: Budget Paper 2 2022-23 (October), Budget Measures: Budget Paper 2 2023-24, OAIC Portfolio Budget Statement 2023

The increase in the OAIC's resourcing has enabled the agency's workforce headcount to grow from 79 in 2010 to 162 in 2023. With these resources, the OAIC has been funded to undertake new responsibilities and achieve many of its performance measures.

Terminating funding measures accounted for half of the OAIC's total funding in 2023-24, as outlined in Table 13. These measures include funding for short-term functions and functions such as major investigations that currently have no ongoing base funding.

Table 13 | Current OAIC terminating measures

Measure	Description	Budget allocation	FY Terminating
Next Steps for Digital ID	To provide ongoing privacy assurance for the Digital ID program	\$1.1 million for one year	2023-24
My Health Record	To regulate the privacy aspects of the My Health Record system	\$4.8 million over two years	2024-25
CDR Enhancement	To support the continued operation of CDR in the banking, energy and non-bank lending sectors	\$3.3 million over two years	2024-25
Stronger privacy enforcement (terminating portion)	To support a standalone Privacy Commissioner, enhance data and analytics capability, and progress enforcement and investigations actions	\$10.7 million over two years (part of a \$44.3 million measure)	2026-27
Privacy and social media	To undertake its privacy and regulatory functions, including in relation to social media and other platforms	\$17 million over two years	2023-24
Optus	To investigate and respond to the Optus data breach	\$5.5 million over two years	2023-24

Source: Budget Measures: Budget Paper 2 2022-23 (March), Budget Measures: Budget Paper 2 2022-23 (October), Budget Measures: Budget Paper 2 2023-24

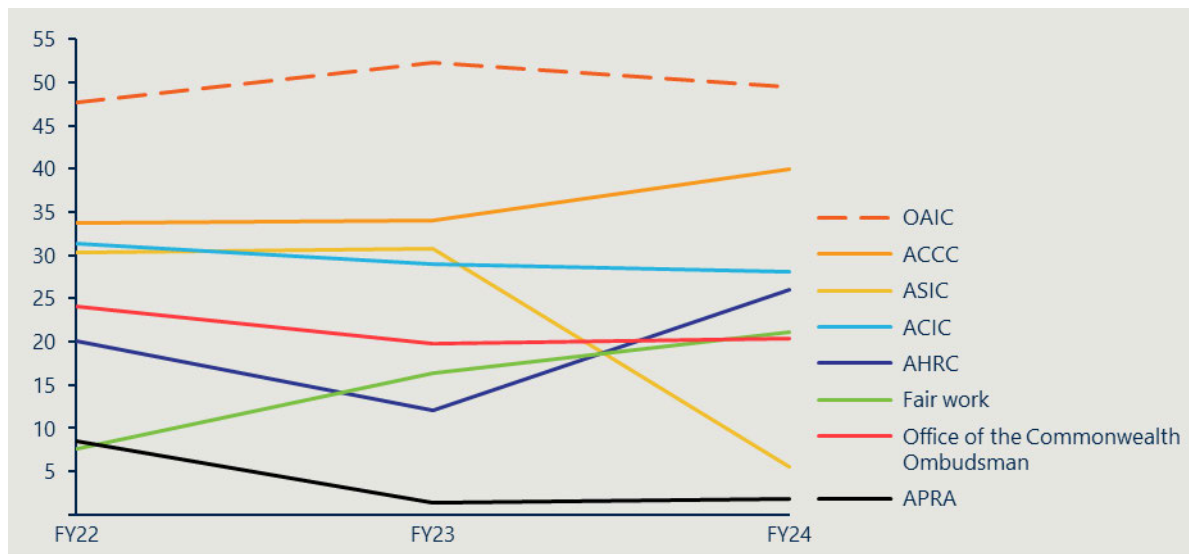
The OAIC’s Major Investigations Branch is currently funded through a specific Optus investigation budget measure and other stronger privacy enforcement funding to facilitate the Medibank, Australian Clinical Labs and Latitude Financial investigations. These measures are scheduled to terminate in June 2024.

[Redacted]

The OAIC has a relatively high proportion of terminating funding when compared to other regulators – as illustrated in Figure 77.

[Redacted]

Figure 77 | Percentage of terminating budget measures for similar government regulators



Source: Portfolio Budget Statements 2023-24 and Budget Measures: Budget Paper 2 2022-23 (March), Budget Measures: Budget Paper 2 2022-23 (October), Budget Measures: Budget Paper 2 2023-24

s47C

[Redacted]


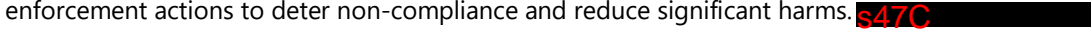
s47C

[Redacted]

s47C



The Australian Cyber Security Strategy notes that the acceleration of cyber attacks will lead to more frequent and large-scale data breaches containing personal information.⁷² As the regulator of privacy in Australia, the OAIC is best placed to investigate and respond to these breaches, with stronger, more timely enforcement actions to deter non-compliance and reduce significant harms. s47C



s47C



⁷² Australian Cyber Security Strategy, Department of Home Affairs, 2023.

Appendix B Details of the Strategic Review

This Appendix sets out the details of the Strategic Review including its Terms of Reference, data sources and stakeholders engaged.

B.1 Terms of Reference for the Strategic Review

A strategic review of the Office of the Australian Information Commissioner (OAIC) will ensure the OAIC is well positioned to deliver on its statutory functions as the national privacy and information access regulator into the future.

Scope

The reviewer should consider, report, and make recommendations about how the OAIC can ensure it is best positioned to deliver on its functions as the national privacy and information access regulator and respond to future challenges. Recommendations should cover:

- the extent to which the OAIC's
 - organisational capability,
 - structure,
 - governance, and
 - resourcing
 - are suitable to achieve the OAIC's purpose and future functionality, or require amendment;
- how resource allocation can be optimised to maximise efficiency and support the OAIC's statutory functions;
- how the OAIC can best respond to the likely continuing growth to the volume and complexity of its core statutory workload;
- how to ensure the effectiveness of the OAIC as a regulator in responding to changing technology, the growth of the digital economy and increasing cyber-crime; and
- the role of the OAIC in providing advice and reports to government about privacy, information access and information management.

Contextual information

The reviewer must have regard to relevant contextual matters, about which the OAIC will provide the reviewer with relevant background, including:

- potential changes to the functions of the OAIC arising from the Government's response to the Privacy Act Review;
- the operation of FOI laws;
- evolving community expectations about privacy and information access, and expectations that the OAIC will take a strong enforcement posture.

Recommendations

The reviewer must identify recommendations that can be implemented within the existing legislative framework, but may make recommendations that require legislative change where the reviewer considers necessary.

Activities

As a minimum, the reviewer should examine relevant documents and data, conduct interviews with OAIC executives, staff, and key external stakeholders, and examine the capabilities and arrangements of a selection of analogous agencies in Australia and elsewhere.

Timeframe

Interim report by **22 January 2024**. Final report by **19 February 2024**.

B.2 Review data sources

Review Data Sources

The Strategic Review considered a wide range of data sources, as summarised below.

Source	Description
Resolve case activity data for IC reviews and privacy complaints	<ul style="list-style-type: none"> All cases completed in FY2022-23 Informed the process mining analysis
OAIC Financial reports	<ul style="list-style-type: none"> Internal budgets including monthly financial statements, internal budget history and government resourcing
OAIC Staff	<ul style="list-style-type: none"> Staff interviews Workshops Focus groups
Legislation	<p>Including:</p> <ul style="list-style-type: none"> Privacy Act FOI Act AIC Act PGPA Act
Process Workflows	<ul style="list-style-type: none"> OAIC process workflow documentation for IC reviews, privacy complaints, CII (FOI and Privacy), NDBs, FOI complaints and Privacy and CDR assessments Tested and validated with OAIC staff
Document Review	<ul style="list-style-type: none"> Review of over 150 OAIC documents including policy, guidance and risk documents, senate estimates briefs, previous reports and analysis. Statistical information including staff headcount, APS survey responses. This review also included publicly available documentation including annual reports, corporate plans, online resources and guidelines.

B.3 Stakeholder engagement

B.3.1 Engagement with OAIC staff

Engagement with OAIC staff included interviews, workshops and focus groups held over the course of the project. Many staff were engaged multiple times as part of the Strategic Review.

Type of Engagement	Staff Engaged
Executive interviews and workshops	<ul style="list-style-type: none"> All members of the OAIC executive – individual or small group interviews Several workshops with OAIC executive team
Staff Workshops	<p>Engagement with 85 staff across all OAIC branches:</p> <ul style="list-style-type: none"> Corporate Branch Major Investigations Branch Dispute Resolution Branch FOI Branch Regulation and Strategy Branch Regulation and Strategy (CDR) Branch
Focus Groups	<ul style="list-style-type: none"> 25 staff from all branches were represented (many of these staff had been previously engaged through the workshops)
Process Mapping interviews	<ul style="list-style-type: none"> Interviews with Assistant Commissioners, Directors and Assistant Directors across the OAIC

s47C

Appendix C Overview of the OAIC's functions and roles

The OAIC has a range of statutory functions under several pieces of legislation. In chapter 2, the OAIC's functions are mapped as critical, strategic and supporting. Table 18 provides additional detail about the OAIC's statutory functions, the area they relate to, whether they are mandatory or discretionary under the legislation, and any specific requirements that apply in respect of how or when the OAIC may or must exercise them. The below table is not intended to be exhaustive but covers key statutory functions performed by the OAIC.

Table 18 | OAIC's statutory functions

Function	Legislative requirement	Area	Type	Requirements
IC review	<i>Freedom of Information Act 1982 - Part VII</i>	FOI	Mandatory	The Commissioner must make a decision in relation to an IC review under s 55K. The procedure is outlined in Division 6 of the FOI Act.
Privacy complaint	<i>Privacy Act 1988 - s 36</i>	Privacy	Mandatory	The Commissioner may or must decide not to investigate in certain circumstances outlined in s 41 of the Privacy Act.
Assess FOI complaints	<i>Freedom of Information Act 1982 - s 69</i>	FOI	Mandatory	The IC must investigate a complaint made under s 70.
Administer the NDB Scheme	<i>Privacy Act 1988 - Part IIIC</i>	Privacy	Mandatory	The OAIC must receive and process notifications of eligible data breaches (s 26WK). If the Commissioner believes there has been an eligible data breach then the Commissioner may direct the entity to prepare a statement to the impacted individuals (s 26WR).
Assess Extension of Time applications	<i>Freedom of Information Act 1982 - s 15AC</i>	FOI	Mandatory	The IC must decide whether an extension of time application will be accepted (s 15AB).
Vexatious applicant declaration applications	<i>Freedom of Information Act 1982 - s 89K</i>	FOI	Mandatory	The IC must declare whether a person is judged to be a vexatious applicant (s 89K).
Administer the Information Publication Scheme	<i>Freedom of Information Act 1982 - Part 2, s 7A</i>	FOI	Mandatory	The IC must review the operation of the scheme in each agency (s 8F).

Function	Legislative requirement	Area	Type	Requirements
Monitor and manage the privacy and confidentiality functions (CDR)	<i>Competition and Consumer Act 2010 - Part IVD</i>	CDR	Mandatory	The IC must promote compliance with the privacy safeguards (s 56EQ).
Approve code development	<i>Competition and Consumer Act 2010 - Part IVD</i>	CDR	Mandatory	The IC must analyse and report about an instrument proposing to designate a sector (s 56AF).
Ensure proper financial management and reporting	<i>Public Governance, Performance and Accountability Act 2013</i>	NA	Mandatory	The IC is the accountable authority and must abide by the duties (including those under s 36 relating to budgeting) outlined in the PGPA Act.
Adhere to public service employment standards	<i>Public Service Act 1999</i>	NA	Mandatory	The IC is the accountable authority and must abide by the duties outlined in the Public Service Act.
Ensure workplace health and safety compliance	<i>Work Health Safety Act 2011</i>	NA	Mandatory	The IC is the accountable authority and must abide by the duties outlined in the WHS Act.
Produce regulatory guidance for privacy legislation	<i>Privacy Act 1988 - Part IV s 28</i>	Privacy	Discretionary	The Commissioner may publish guidelines under s 28.
Perform strategic functions relating to information management in government	<i>Australian Information Commissioner Act 2010 - s 7</i>	Information Management	Discretionary	The IC is empowered to report to the Minister on information management in government under s 7.
Conduct CDR assessments	<i>Competition and Consumer Act 2010 - s 56ER</i>	CDR	Discretionary	The IC may conduct an assessment relating to the management and handling of CDR data.
Initiate privacy investigations	<i>Privacy Act 1988 - s 40(2)</i>	Privacy	Discretionary	The Commissioner may, on their own initiative, investigate an act or practice.
Conduct FOI investigations	<i>Freedom of Information Act - s 69</i>	FOI	Discretionary	The IC may investigate an action taken by an agency in the performance of functions, or the exercise of powers, under the FOI Act.
Conduct FOI monitoring	<i>Australian Information Commissioner Act 2010 - s 8</i>	FOI	Discretionary	The Commissioner is empowered to monitor compliance by agencies with the FOI Act.

Function	Legislative requirement	Area	Type	Requirements
Providing information, advice, assistance and training on matters relevant to the operation of the FOI Act	<i>Australian Information Commissioner Act 2010 - s 7</i>	FOI	Discretionary	The IC is empowered to report to the Minister on information management in government under s 7.
Making reports and recommendations to the Minister about proposals for legislative change or administrative action	<i>Australian Information Commissioner Act 2010 - s 8</i>	FOI	Discretionary	The IC is empowered to make reports and recommendations to the Minister about proposals for legislative change or administrative action under s 8.
Prepare FOI guidelines	<i>Freedom of Information Act 1982 - s 93A</i>	FOI	Discretionary	The IC is empowered to issue guidelines under s 93A of the FOI Act.
Develop CDR regulatory guidance	<i>Competition and Consumer Act 2010 - s 56EQ</i>	CDR	Discretionary	The IC may publish guidelines under s 56EQ.
CDR monitoring for small businesses and individuals	<i>Privacy Act 1988 - s 28A</i>	CDR	Discretionary	The Commissioner is empowered to monitor the security and accuracy of information held by an entity under s 28A.
Engage in information management policy development	<i>Australian Information Commissioner Act 2010 - s 7</i>	Information Management	Discretionary	The IC is empowered to report to the Minister on information management in government under s 7.
Provide expert advice on privacy to government agencies and other entities involved in Digital ID development	<i>Privacy Act 1988 - s 28B</i>	Privacy	Discretionary	The IC may publish guidelines under s 28B.
Provide guidance to healthcare providers on best practices for managing personal information within the My Health Record system	<i>My Health Records Act 2012 - s 111</i>	Privacy	Discretionary	The IC must formulate guidelines in relation to My Health Record.
Develop research and educate the public on privacy (e.g. Australian Community Attitudes to Privacy Survey)	<i>Privacy Act 1988 - s 28</i>	Privacy	Discretionary	The Commissioner may undertake educational programs for the purposes of promoting the protection of individual privacy.
Provide education on the privacy requirements of CDR	<i>Competition and Consumer Act 2010 - s 56EQ</i>	CDR	Discretionary	The Commissioner may undertake educational programs for the purposes of promoting the protection of individual privacy.

Function	Legislative requirement	Area	Type	Requirements
Provide education and outreach on information management	<i>Australian Information Commissioner Act 2010 - s 7</i>	Information Management	Discretionary	The IC is empowered to report to the Minister on information management in government under s 7.
Develop CDR guidelines and provide advice	<i>Privacy Act 1988 - s 28</i>	CDR	Discretionary	The IC may publish guidelines under s 56EQ.

Appendix D Privacy Act Review Impact Assessment

An impact assessment of the Privacy Act Review proposals on the OAIC is outlined below. The proposals are organised by whether the Government's response was to 'accept' or 'accept-in-principle' the recommendation. The 'impact' column refers to the assumed size of change in the OAIC's workload (regardless of direction) that would occur if a proposal were implemented. The 'OAIC Change' reflects Nous' high-level view of the shift in the OAIC's functions based on the proposal.

The Review completed an initial assessment of the Privacy Act Review proposals to understand which would impact the OAIC and the specific changes that might be required if the proposal was implemented. The assessment was then tested through engagements with OAIC staff and external stakeholders to understand the anticipated impact and potential change to the OAIC's current approach or execution of its functions relating to each of the proposals.

D.1 Proposals agreed

The impact assessment of the proposals that are agreed by Government is set out in Table 19.

Table 19 | Impact assessment of agreed proposals

Proposal
<p>Proposal 25.1 Create tiers of civil penalty provisions to allow for better targeted regulatory responses:</p> <p>(a) Introduce a new mid-tier civil penalty provision to cover interferences with privacy without a 'serious' element, excluding the new low-level civil penalty provision.</p> <p>(b) Introduce a new low-level civil penalty provision for specific administrative breaches of the Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties.</p>
<p>Proposal 25.9 Amend the annual reporting requirements in AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground of section 41.</p>
<p>Proposal 25.10 The OAIC should conduct a strategic internal organisational review with the objective of ensuring the OAIC is structured to have a greater enforcement focus.</p>
<p>Proposal 21.3 Enhance OAIC guidance in relation to APP 11 on what reasonable steps are to secure personal information. The guidance</p>

s47C

s47C

Proposal

that relates to cyber security could draw on technical advice from the Australian Cyber Security Centre.

Proposal 25.2 Amend section 13G of the Act to remove the word 'repeated' and clarify that a 'serious' interference with privacy may include: (a) those involving 'sensitive information' or other information of a sensitive nature; (b) those adversely affecting large groups of individuals; (c) those impacting people experiencing vulnerability; (d) repeated breaches; (e) wilful misconduct, and (f) serious failures to take proper steps to protect personal data.

The OAIC should provide specific further guidance on the factors that they take into account when determining whether to take action under section 13G.

Proposal 25.11 Amend subsection 41(dc) of the Act so that the Information Commissioner has the discretion not to investigate complaints where a complaint has already been adequately dealt with by an EDR scheme.

Proposal 28.1 Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.

Proposal 29.2 Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.

Proposal 5.1 Amend the Act to give power to the Information Commissioner to make an APP code where the Attorney-General has directed or approved that a code should be made: (a) where it is in the public interest for a code to be developed, and (b) where there is unlikely to be an appropriate industry representative to develop the code.

In developing an APP code, the Information Commissioner would: (a) be required to make the APP code available for public consultation for at least 40 days, and (b) be able to consult any person he or she considers appropriate and to consider the matters specified in any relevant guidelines at any stage of the code development process.

Proposal 13.2 Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities. This work should be done as part of a broader

s47C

Proposal

consideration by government of the regulation of biometric technologies.

Proposal 25.11 Amend subsection 41(dc) of the Act so that the Information Commissioner has the discretion not to investigate complaints where a complaint has already been adequately dealt with by an EDR scheme.

Proposal 28.1 Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.

Proposal 29.2 Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.

Proposal 5.1 Amend the Act to give power to the Information Commissioner to make an APP code where the Attorney-General has directed or approved that a code should be made: (a) where it is in the public interest for a code to be developed, and (b) where there is unlikely to be an appropriate industry representative to develop the code.

In developing an APP code, the Information Commissioner would: (a) be required to make the APP code available for public consultation for at least 40 days, and (b) be able to consult any person he or she considers appropriate and to consider the matters specified in any relevant guidelines at any stage of the code development process.

Proposal 13.2 Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities. This work should be done as part of a broader consideration by government of the regulation of biometric technologies.

Proposal 13.3 The OAIC should continue to develop practice-specific guidance for new technologies and emerging privacy risks. Practice-specific guidance could outline the OAIC's expectations for compliance with the Act when engaging in specific high-risk practices, including compliance with the fair and reasonable personal information handling test.

Proposal 17.1 Introduce, in OAIC guidance, a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information.

s47C

Proposal

Proposal 19.2 High-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Act. This should be supplemented by OAIC guidance.

Proposal 21.5 OAIC guidance in relation to APP 11.2 should be enhanced to provide detailed guidance that more clearly articulates what reasonable steps may be undertaken to destroy or de-identify personal information

Proposal 23.1 Consult on an additional requirement in subsection 5B(3) to demonstrate an 'Australian link' that is focused on personal information being connected with Australia.

Proposal 25.3 Amend the Act to apply the powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014 to investigations of civil penalty provisions in addition to the Information Commissioner's current investigation powers.

Proposal 25.4 Amend the Act to provide the Information Commissioner with the power to undertake public inquiries and reviews into specified matters on the approval or direction of the Attorney-General.

Proposal 25.5 Amend subparagraph 52(1)(b)(ii) and paragraph 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined: a declaration that the respondent must perform any reasonable act or course of conduct to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered by the complainant/those individuals. The OAIC should publish guidance on how entities could achieve this.

Proposal 25.6 Give the Federal Court and the Federal Circuit and Family Court of Australia the power to make any order it sees fit after a civil penalty provision relating to an interference with privacy has been established.

Proposal 28.4 Introduce a provision in the Privacy Act to enable the Attorney-General to permit the sharing of information with appropriate entities to reduce the risk of harm in the event of an eligible data breach. The provision would contain safeguards to ensure that only limited information could be made available for designated purposes, and for a time limited duration.

Proposal	s47C
<p>Proposal 5.2 Amend the Act to enable the Information Commissioner to issue a temporary APP code for a maximum 12-month period on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.</p>	
<p>Proposal 17.2 OAIC guidance on capacity and consent should be updated to reflect developments in supported decision-making.</p>	

D.2 Proposals agreed in-principle

The impact assessment of the proposals that are agreed-in-principle by Government is set out in Table 20.

Table 20 | Impact assessment of agreed-in-principle proposals

Proposal	s47C
<p>Proposal 6.1 Remove the small business exemption, but only after:</p> <ul style="list-style-type: none"> (a) an impact analysis has been undertaken to better understand the impact removal of the small business exemption will have on small business – this would inform what support small business would need to adjust their privacy practices to facilitate compliance with the Act (b) appropriate support is developed in consultation with small business (c) in consultation with small business, the most appropriate way for small business to meet their obligations proportionate to the risk, is determined (for example, through a code), and (d) small businesses are in a position to comply with these obligations. 	
<p>Proposal 6.2 In the short term:</p> <ul style="list-style-type: none"> (a) prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption, and (b) remove the exemption from the Act for small businesses that obtain consent to trade in personal information. 	
<p>Proposal 25.7 Further work should be done to investigate the effectiveness of an industry funding model for the OAIC.</p>	
<p>Proposal 25.8 Further consideration should be given to establishing a contingency litigation fund to fund any costs orders against the OAIC, and an enforcement special account to fund high cost litigation.</p>	

Proposal

Proposal 26.1 Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy. The model should incorporate the appropriate design elements discussed in this chapter.

Proposal 27.1 Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123. Consult with the states and territories on implementation to ensure a consistent national approach.

Proposal 7.1 Enhanced privacy protections should be extended to private sector employees, with the aim of:

(a) providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for

(b) ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information

(c) ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and

(d) notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm.

Further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including how privacy and workplace relations laws should interact. The possibility of privacy codes of practice developed through a tripartite process to clarify obligations regarding collection, use and disclosure of personal and sensitive information should also be explored.

Proposal 13.1 APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks.

(a) A Privacy Impact Assessment should be undertaken prior to the commencement of the high-risk activity.

(b) An entity should be required to produce a Privacy Impact Assessment to the OAIC on request. The Act should provide that a high privacy risk activity is one that is 'likely to have a significant impact on the privacy of individuals'. OAIC guidance should be developed which articulates factors that may indicate a high privacy risk, and provides examples of activities that will generally require a Privacy Impact Assessment to be completed. Specific high risk practices could also be set out in the Act.

Proposal 18.5 Introduce a right to de-index online search results containing personal information which is:

(a) sensitive information [e.g. medical history], or

(b) information about a child, or

s47C

Proposal

(c) excessively detailed [e.g. home address and personal phone number], or

(d) inaccurate, out-of-date, incomplete, irrelevant, or misleading.

The search engine may refer a suitable request to the OAIC for a fee. The right should be jurisdictionally limited to Australia.

Proposal 18.7 Individuals should be notified at the point of collection about their rights and how to obtain further information on their rights, including how to exercise them. Privacy policies should set out the APP entity's procedures for responding to the rights of the individual.

Proposal 18.9 An APP entity must take reasonable steps to respond to an exercise of a right of an individual. Refusal of a request should be accompanied by an explanation for the refusal and information on how an individual may lodge a complaint regarding the refusal with the OAIC.

Proposal 28.2

(a) Amend paragraph 26WK(2)(b) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, the entity must give a copy of the statement to the Commissioner as soon as practicable and not later than 72 hours after the entity becomes so aware, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours.

(b) Amend subsection 26WL(3) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity the entity must notify the individuals to whom the information relates as soon as practicable and where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases as soon as practicable.

(c) Require entities to take reasonable steps to implement practices, procedures and systems to enable it to respond to a data breach.

Proposal 4.1 Change the word 'about' in the definition of personal information to 'relates to'. Ensure the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance.

Proposal 4.2 Include a non-exhaustive list of information which may be personal information to assist APP entities to identify the types of information which could fall within the definition. Supplement this list with more specific examples in the explanatory materials and OAIC guidance.

Proposal 9.2 In consultation with industry, and the ACMA, the OAIC should develop and publish criteria for adequate media privacy standards and a template privacy standard that a media organisation may choose to adopt.

s47C

Proposal

Proposal 10.2 The list of matters in APP 5.2 should be retained. OAIC guidance should make clear that only relevant matters, which serve the purpose of informing the individual in the circumstances, need to be addressed in a notice. The following new matters should be included in an APP 5 collection notice:

- (a) if the entity collects, uses or discloses personal information for a high privacy risk activity – the circumstances of that collection, use or disclosure
- (b) that the APP privacy policy contains details on how to exercise any applicable Rights of the Individual, and (c) the types of personal information that may be disclosed to overseas recipients.

Proposal 10.3 Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.

Proposal 11.2 The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consents as part of any future APP codes.

Proposal 12.1 Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.

Proposal 12.2 In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account:

- (a) whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances
- (b) the kind, sensitivity and amount of personal information being collected, used or disclosed
- (c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency
- (d) the risk of unjustified adverse impact or harm
- (e) whether the impact on privacy is proportionate to the benefit
- (f) if the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child, and

s47C

Proposal

(g) the objects of the Act. The EM would note that relevant considerations for determining whether any impact on an individual's privacy is 'proportionate' and could include:

(i) whether the collection, use or disclosure intrudes upon the personal affairs of the affected individual to an unreasonable extent

(ii) whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits, and

(iii) any actions or measures taken by the entity to mitigate the impacts of the loss of privacy on the individual.

Proposal 12.3 The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained. The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should not apply to exceptions in APPs 3.4 and 6.2. The reference to a 'fair means' of collection in APP 3.5 should be repealed.

Proposal 13.4 Include an additional requirement in APP 3.6 to the effect that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3. OAIC guidelines could provide examples of reasonable steps that could be taken.

Proposal 15.2 Expressly require that APP entities appoint or designate a senior employee responsible for privacy within the entity. This may be an existing member of staff of the APP entity who also undertakes other duties.

s47C

Appendix G Key workforce metrics

Details of key workforce metrics for the OAIC relative to APS averages are summarised in Figure 97.

Figure 97 | Key workforce metrics as at 30 June 2023

Workforce metric	OAIC	APS Average
% female	74.3	60.4
% Indigenous	1.1	3.5
% with a disability	2.7	5.1
% non-English speaking background	22.4	15.8
% part-time (ongoing employees)	20.2	13.1
% at the APS classification level	48.6	69.1
Mean Age (years)	39.5	43.1
Median length of service in APS (years)	5.9	9.4
% who have worked in only one agency (ongoing employees)	39.9	67.9
% with a bachelor's degree or higher	81.9	67.3
Exit rate (ongoing employees)	14.1	13.5

Source: APSC, APS Employment Data 30 June 2023

Appendix H Resourcing Modelling Methodology

The Strategic Review evaluated the efficiency and effectiveness of the OAIC's current processes. The Review used a combination of quantitative and qualitative analysis as part of its assessment. The process analysis occurred over three main streams of work that were used to identify efficiency improvements and, where possible, corroborate findings:

1. Process mining
2. Process costing
3. Staff feedback

These three streams fed into the final analysis, completed by the Review to understand the effort and cost required to perform core processes.

Process mining was initially used to understand case data covering IC reviews and privacy complaints. This enabled the Review to understand broad themes related to the efficiency of current processes and the potential causes of backlogs.

Processes were then mapped to outline the current state. **47G**

To supplement the quantitative analysis, staff feedback was sought through focus groups where process barriers and opportunities were discussed. The opportunities were prioritised by staff according to the impact and effort assessed by staff.

Table 21 | Processes that were analysed by the Strategic Review by function

PRIVACY PROCESSES	FOI PROCESSES
<ul style="list-style-type: none"> • Privacy Complaints • Data Breach Notifications • Commissioner Initiated Investigations (CIIs) • Privacy Assessments • CDR Assessments 	<ul style="list-style-type: none"> • Information Commissioner Reviews • FOI Complaints • Commissioner Initiated Investigations (CIIs)

H.1 Process Mining

Process mining techniques were used for the analysis of IC reviews and privacy complaints. This style of analysis enabled the Strategic Review to identify differences in how process workflows are followed by staff, as well as the time taken to perform individual steps. **47G**

s47C

The data analysed covers all cases completed from July 2022 to October 2023. This included:

- 1,415 IC reviews
- 2,911 privacy complaints

The privacy complaints data covers 5,298 cases comprising 226 distinct activities performed across the period from 20 January 2018 to 13 November 2023.

The status of the cases received reflects the following:

- 2,886 number of complete cases (i.e. where a start and end event data could be found)
- 2,412 number of open cases (missing a start or end event)

The IC reviews data covers 3,539 reviews comprising 182 distinct activities performed across the period from 19 January 2018 to 13 November 2023.

The status of the reviews received reflects the following:

- 1,405 number of complete cases (i.e. where a start and end event data could be found)
- 2,134 number of incomplete (missing a start or end event)

The analysis covered the outcomes of each review/complaint type, length of time in system and the common paths followed. Process flow diagrams were developed to understand what steps were completed by staff when addressing reviews or complaints. From these findings, a set of process improvement hypotheses were outlined and tested with senior OAIC staff.

H.2 Process costing

The Review team assessed the cost of processes by combining process blueprints that outlined staff effort per process with case volume and staff cost data provided by the OAIC. The steps are outlined in further detail below.

47G [Redacted text block]

H.2.1 Process blueprints and staff effort allocations

The Strategic Review drafted end-to-end blueprints of key processes. **47G** [Redacted text block]











4 [Redacted text block]

H.3 Staff feedback

The Review team held focus groups with staff to collect feedback in relation to current processes. The focus groups included staff across all branches to gain a comprehensive understanding of common issues and opportunities related to processes.

The focus groups were held virtually with staff divided into three branch groups: Dispute Resolution Branch, FOI Branch, and the remaining branches were grouped together. The focus groups used Miro for online collaboration and staff added their thoughts covering process issues aligned to different categories of overarching process steps. Each focus group was attended by 8 staff who were experienced in the key processes performed by their branch.

Figure 101 | Focus group Miro board structure

	1 Receive or identify	2 Triage and allocate	3 Gather information	4 Action	5 Close
Issues					
Solutions					

Strategic Review – Interim Report

Office of the Australian Information Commissioner

22 January 2024



Nous Group acknowledges Aboriginal and Torres Strait Islander peoples as the First Australians and the Traditional Custodians of country throughout Australia. We pay our respect to Elders past, present and emerging, who maintain their culture, country and spiritual connection to the land, sea and community.

This artwork was developed by Marcus Lee Design to reflect Nous Group's Reconciliation Action Plan and our aspirations for respectful and productive engagement with Aboriginal and Torres Strait Islander peoples and communities.

Disclaimer:

*Nous Group (**Nous**) has prepared this report for the benefit of the Office of the Australian Information Commissioner (the **Client**).*

The report should not be used or relied upon for any purpose other than as an expression of the conclusions and recommendations of Nous to the Client as to the matters within the scope of the report. Nous and its officers and employees expressly disclaim any liability to any person other than the Client who relies or purports to rely on the report for any other purpose.

Nous has prepared the report with care and diligence. The conclusions and recommendations given by Nous in the report are given in good faith and in the reasonable belief that they are correct and not misleading. The report has been prepared by Nous based on information provided by the Client and by other persons. Nous has relied on that information and has not independently verified or audited that information.

© Nous Group

Contents

Executive summary.....	1
Recommendations	4
1 Overview of the Strategic Review	7
1.1 Strategic Review scope	8
1.2 Strategic Review governance	9
1.3 Strategic Review method and data sources	9
2 Overview of the OAIC.....	10
3 Drivers of change.....	18
3.1 Technological drivers of change	20
3.2 Social drivers of change.....	22
3.3 Political drivers of change.....	23
4 Strategy, regulatory posture and approach.....	28
4.1 Strategic plan	33
4.2 Regulatory posture	35
4.3 Regulatory approach.....	39
5 Governance	52
6 Organisational structure	61
7 Processes and systems	66
7.1 Limitations of the OAIC's current processes and systems.....	67
7.2 Opportunities to enhance processes and systems	72
8 Organisational capability	77
8.1 Workforce capability and skills	79
8.2 Employee experience	83
8.3 Culture and leadership	88
8.4 Sourcing external capabilities.....	91
9 Resourcing and resource allocation.....	92
9.1 Allocation of funding and effort.....	97
9.2 Efficient use of funding.....	99
9.3 Sufficiency of funding.....	100
Appendix A Terms of Reference for the Strategic Review.....	106
Appendix B Review data sources and methodology.....	108
Appendix C Stakeholder engagement.....	109
C.1 Engagement with OAIC staff	109
C.2 Engagement with external stakeholders.....	109
Appendix D Privacy Act Review Impact Analysis	110

D.1 Proposals agreed.....	110
D.2 Proposals agreed in-principle.....	115
Appendix E Possible governance models.....	123
Appendix F Possible structure models.....	126
Appendix G Key workforce metrics.....	130
Appendix H Resourcing Modelling Methodology.....	131

DRAFT

Acronyms, abbreviations and terminology

[Drafting Note: To be included in Final Report.]

DRAFT

Executive summary

The Strategic Review

The Office of the Australian Information Commissioner (OAIC) and the Attorney-General's Department engaged Nous Group to complete a Strategic Review of the OAIC. The purpose of the Strategic Review is to deliver an assessment of and recommendations on the operation, functions and governance of the OAIC. The Strategic Review included engagement with internal and external stakeholders, document review, data and comparative analysis. This report provides the recommendations on the Terms of Reference of the Strategic Review. In doing so, it provides recommendations on how to improve the functions of the OAIC, support the management of privacy and information regulation and aid the OAIC in an increasingly technologically dependent world.

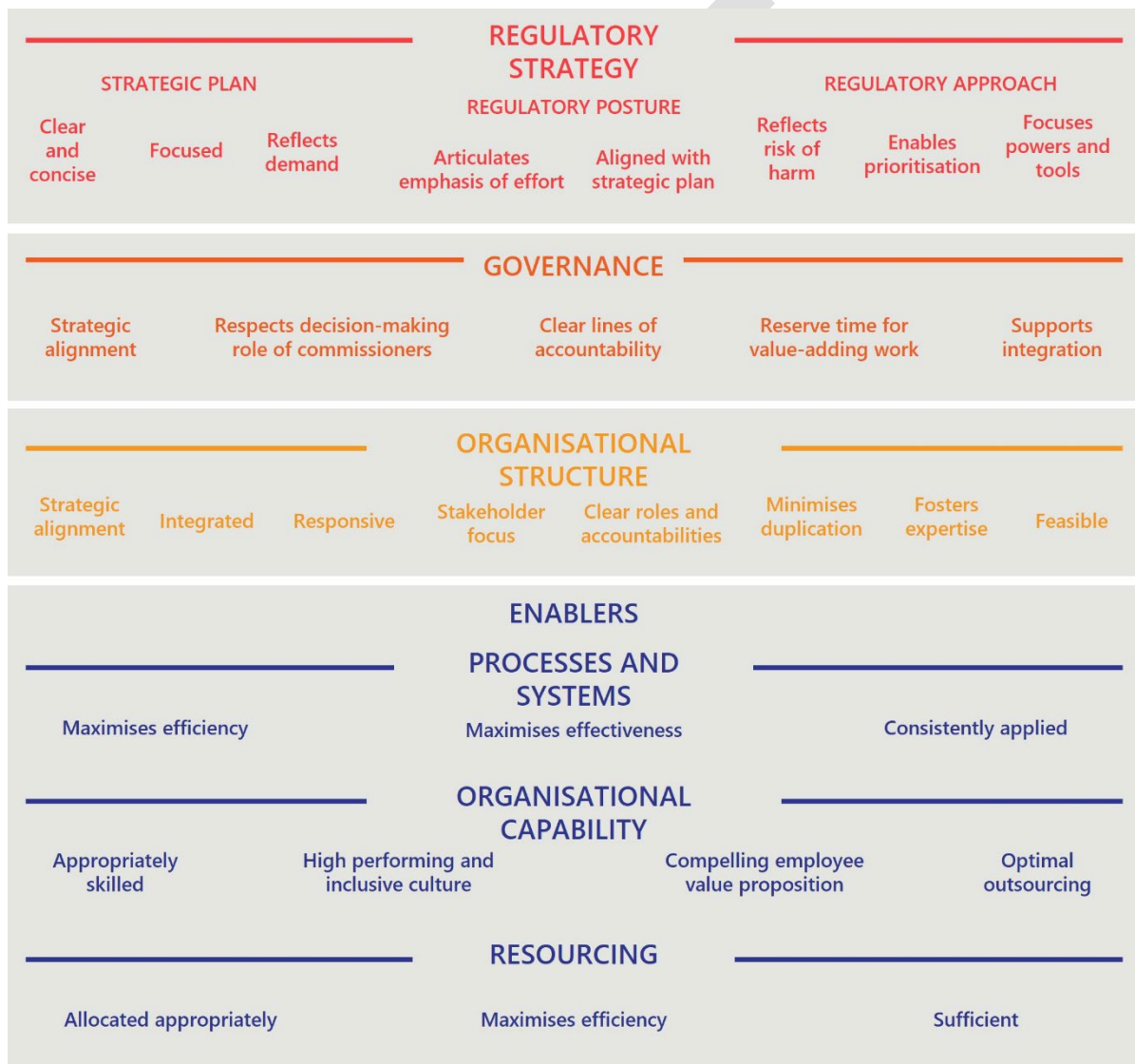
[Drafting Note: A 2-3 page summary narrative of the Strategic Review to be included in the Final Report, considering feedback provided on this Interim Report.]

Analytical framework for the Strategic Review

Many of the Terms of Reference are relevant to multiple elements of the OAIC’s operating model. As such, we developed an analytical framework to guide the Strategic Review that outlines the elements of the OAIC’s operating model that we have considered. The framework also articulates criteria for each element based on our research and analysis. The framework is focused on the specific areas of the Strategic Review specified in the Terms of Reference, and uses Nous’ organisational architecture framework to address the core organisational features and enablers. These criteria are used throughout the Strategic Review report as criteria to test the suitability of the current state to and guide what the ideal future state will be.

The analytical framework is shown in Figure 1.

Figure 1 | Review analytical framework



Structure of this report

This document is the Interim Report of the Strategic Review. The Interim Report will be refined and updated to reflect feedback received and further engagement with the OAIC executive to become the Final Report, which will be delivered on 5 February 2024.

A summary of how the Strategic Review Terms of Reference map to the elements of our analytical framework and the corresponding Chapters of this report is set out in Table 1.

Table 1 | Report structure

Terms of Reference	Relevant analytical framework elements	Report reference
The extent to which the OAIC's <ul style="list-style-type: none"> organisational capability structure governance resourcing are suitable to achieve the OAIC's purpose and future functionality, or require amendment	Drivers of change	Chapter 3
	Organisational capability	Chapter 8
	Organisational structure	Chapter 6
	Governance	Chapter 5
	Resourcing	Chapter 9
How resource allocation can be optimised to maximise efficiency and support the OAIC's statutory functions	Processes and systems	Chapter 7
	Resourcing	Chapter 9
How the OAIC can best respond to the likely continuing growth to the volume and complexity of its core statutory workload	Drivers of change	Chapter 3
	Strategy, regulatory posture and approach	Chapter 4
	Processes and systems	Chapter 7
	Organisational capability	Chapter 8
	Resourcing	Chapter 9
How to ensure the effectiveness of the OAIC as a regulator in responding to changing technology, the growth of the digital economy and increasing cyber crime	Drivers of change	Chapter 3
	Strategy, regulatory posture and approach	Chapter 4
The role of the OAIC in providing advice and reports to government about privacy, information access and information management	Strategy, regulatory posture and approach	Chapter 4

1 Overview of the Strategic Review

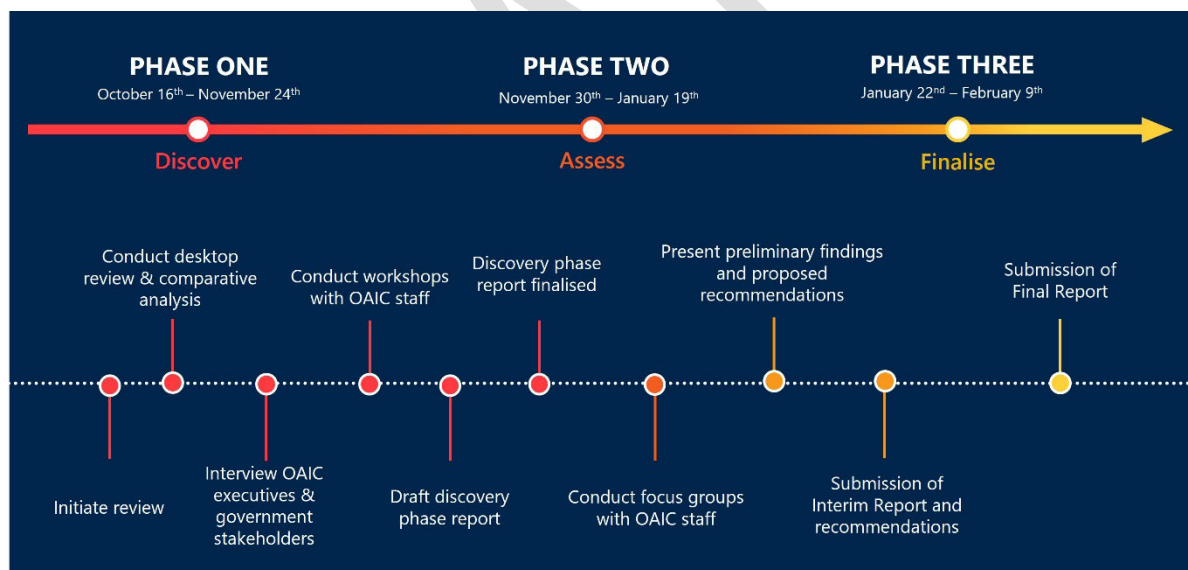
This Chapter provides an overview of the scope, governance, and data sources for the Strategic Review.

The Office of the Australian Information Commissioner (OAIC) and the Attorney-General's Department engaged Nous Group (Nous) to undertake a Strategic Review of the OAIC. The Strategic Review is intended to assess the OAIC's operations, functions and governance and makes recommendations about how the OAIC can ensure it is well positioned to deliver on its functions as the national privacy and information access regulator and respond to future changes.

The Strategic Review comes as the data, information and privacy system is becoming increasingly challenging and attracting greater attention from government and business. This brings the effectiveness of Australia's national privacy and information access systems, including OAIC's performance as the primary regulator of those systems, into the spotlight.

The Strategic Review was conducted over a 15-week period from October 2023 to February 2024. The timelines and key milestones for the Strategic Review are shown in Figure 3.

Figure 3 | Timelines for the Strategic Review



1.1 Strategic Review scope

The key elements of the terms of reference are outlined in Figure 4. The full Terms of Reference for the Strategic Review can be found in Appendix A.

Figure 4 | Scope of the of the Strategic Review as per the Terms of Reference

The reviewer should consider, report, and make recommendations about how the OAIC can ensure it is best positioned to deliver on its functions as the national privacy and information access regulator and respond to future challenges. Recommendations should cover:

1. the extent to which the OAIC's
 - a. organisational capability
 - b. structure
 - c. governance
 - d. resourcing
2. are suitable to achieve the OAIC's purpose and future functionality, or require amendment
3. how resource allocation can be optimised to maximise efficiency and support the OAIC's statutory functions
4. how the OAIC can best respond to the likely continuing growth to the volume and complexity of its core statutory workload
5. how to ensure the effectiveness of the OAIC as a regulator in responding to changing technology, the growth of the digital economy and increasing cyber crime
6. the role of the OAIC in providing advice and reports to government about privacy, information access and information management.

This Strategic Review occurred in parallel to several other reforms and announcements that will have a bearing on the OAIC's future priorities and operating model. These include the release of the report from the Senate Inquiry into the operation of Commonwealth FOI laws and the announcement of the appointment of the new Freedom of Information Commissioner and Privacy Commissioner. The release of the Government's response to the Privacy Act Review and the acceptance of the review recommendations in principle also preceded the start of this Strategic Review by several weeks.

It is important to note that there are several considerations or questions that were not in scope for the Strategic Review. Some these are outlined in Figure 5 below.

s47C



1.2 Strategic Review governance

This Strategic Review has been overseen by the OAIC Strategic Review Steering Group (SRSB) which is comprised of senior representatives from the OAIC, the Attorney-General's Department and the Department of Finance. The SRSB was responsible for:

- Reviewing the terms of reference for the Strategic Review, which were endorsed jointly by the OAIC Commissioners and AGD Secretary.
- Engaging with the reviewer (Nous) during the course of the Strategic Review to ensure that relevant matters are considered.
- Providing feedback to the reviewer in relation to draft review report.
- Considering outcomes of Strategic Review and providing advice on potential next steps.

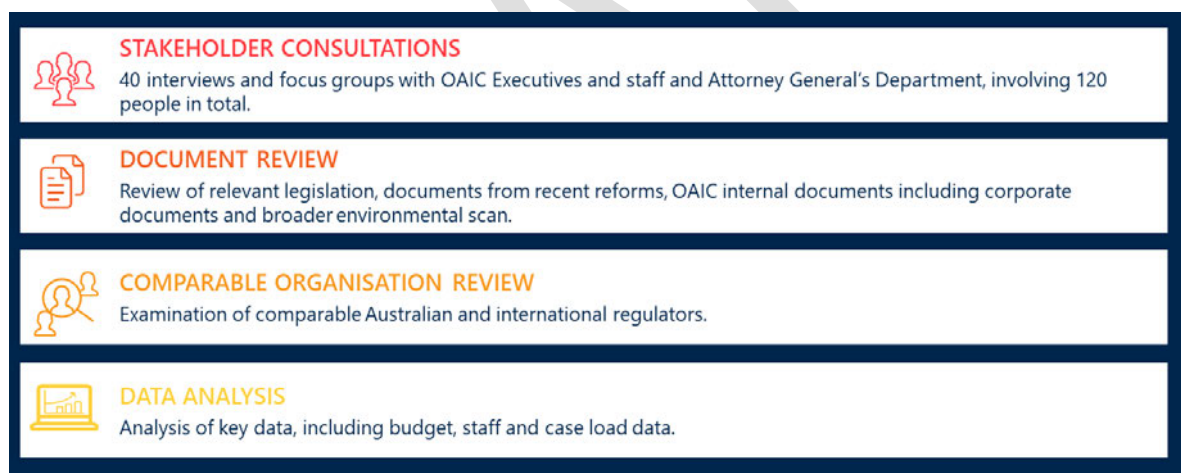
1.3 Strategic Review method and data sources

The Strategic Review drew on a wide range of data sources which are summarised in Figure 6.

See Appendix B for a detailed overview of the Strategic Review methodology and data sources.

See Appendix C for further details of the stakeholders that the Strategic Review team engaged.

Figure 6 | Overview of key data sources for the Strategic Review



2 Overview of the OAIC

This Chapter provides a summary overview of the OAIC. It outlines relevant context, including legislative responsibilities and functions, a snapshot of recent demand and performance, and key events that have impacted the OAIC's operations.

Figure 7 | Relevant questions from the Terms of Reference

- How can the OAIC best respond to the likely continuing growth to the volume and complexity of its core statutory workload?

s47C

- The OAIC has continued to see high and growing demand for its services. The agency has received increasing numbers of applications for IC reviews and privacy complaints. As cases have grown faster than they have been resolved, the case backlog has risen in the OAIC's IC review jurisdiction.
- The OAIC has met most but not all performance measures in the last financial year. Key areas where the OAIC could improve further to achieve its performance measures are in relation to the time taken to finalise IC reviews, CIIs and NDBs.

s47C

The OAIC is Australia's national privacy and information access regulator. Established in 2010 under the *Australian Information Commissioner Act 2010* (AIC Act), the OAIC is an independent statutory agency, within the Attorney-General's portfolio, that regulates the *Privacy Act 1988* (Privacy Act) and *Freedom of Information Act 1982* (FOI Act).

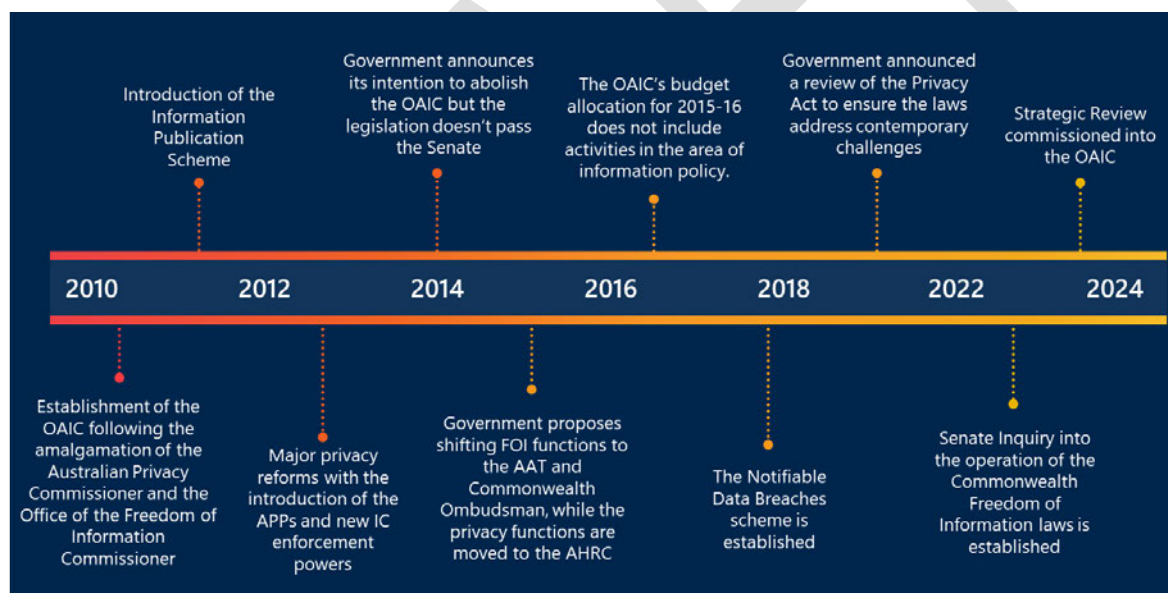
The OAIC has a range of functions under other legislation, such as the *Competition and Consumer Act 2010* (in relation to the Consumer Data Right), the *My Health Records Act 2012* and the *Privacy (Credit Reporting) Code 2014*. The OAIC regulates both Australian Government entities and officials (in relation to both freedom of information and privacy) and the private sector (in relation to privacy).

Since its establishment, the OAIC has experienced significant changes which has required the agency to adapt and expand to respond to evolving needs and challenges in privacy protection and information management. These changes include proposals by previous Governments to abolish the OAIC and transfer its functions to other areas of government.

The OAIC's remit has grown with major reforms to the Privacy Act, requiring the OAIC to exercise new functions, and respond to growing demand for FOI matters.

These key developments and reforms are outlined in Figure 9.

Figure 9 | Timeline of key events



The OAIC is responsible for protecting privacy and information access rights, and managing information policy in Australia

Through its regulation of privacy and information access under the Privacy Act and the FOI Act, the OAIC supports effective government, a strong Australian economy and human rights. Australia's national interest requires that the OAIC is well placed to perform this role. This is a challenging ask of the agency as the privacy and FOI landscape is constantly evolving and the OAIC must be at the forefront of the Government's response to whole-of-society future challenges.

The OAIC's roles matter to Australians, and they matter to the Government. Eighty-four per cent of Australians want more control or choice over the collection and use of their personal data.¹ Over 90 per cent of Australians believe that it is important that they have a right to access government information.²

¹ OAIC, Australian Community Attitudes to Privacy Survey, August 2023, p 18

² Information and Privacy Commission and Woolcott, Cross Jurisdictional Information Access Study, June 2023, p 6

The Attorney-General's Statement of Expectations for the OAIC acknowledges the OAIC's 'invaluable work' as it re-orientes elements of its mandate.

s47C

new information gathering powers in the Notifiable Data Breach (NDB) scheme and improving information sharing and enforcement powers. The FOI Commissioner role was also left vacant from 2015 to mid-2021, while the Privacy Commissioner and Information Commissioner roles have been filled as a dual appointment of a single individual since 2015. The decision to appoint three individuals to all three commissioner roles was only made in 2023 and will take effect from February of 2024.

The OAIC's remit has also expanded in recent years. In addition to its core privacy and freedom of information functions, the OAIC has obligations under 36 different Acts. In recent years, *Competition and Consumer (Consumer Data Right) Rules 2020*, the Notifiable Data Breaches scheme, and regulation of the COVIDSafe app were added to OAIC's remit.

s47C

The former Government proposed abolishing the OAIC in 2014 as part of its 'smaller government' agenda, with a proposal to move its functions to other agencies. The legislation to dissolve the OAIC lapsed in the Senate at the end of 2014.

More recently, in 2023 the Senate completed an inquiry into the operation of the Commonwealth FOI laws. It has highlighted the critical role of the OAIC in overseeing and administering these laws. It has also raised questions about the effectiveness, efficiency and challenges faced by the OAIC in fulfilling its mandate in the context of growing demands for transparency in government.

s47C

The OAIC can exercise its functions with a range of discretion according to legislation. Key functions such as assessing privacy complaints and IC reviews must be broadly performed in line with demand for these functions, while others including investigations and assessments can be applied in a more targeted and strategic manner.

The OAIC has many roles for an agency of its size, reflecting the approximately 36 different pieces of legislation that fall within its remit. As a result, the agency's priorities and resourcing allocation regularly needs to be revisited and assessed for its appropriateness.

The Strategic Review team developed a framework for mapping the OAIC's current roles by the following three categories:

- **CRITICAL** | Mandatory functions required by legislation forming the core responsibilities of the OAIC to meet its privacy and FOI obligations.
- **STRATEGIC** | All other activities related to privacy and FOI that the OAIC is empowered to exercise by legislation, including functions it is required to deliver for non-legislative reasons.
- **SUPPORTING** | All other functions that, while not directly involved in the regulatory process, are vital for the OAIC to operate.

The functions that fall under each category across the OAIC's core regulatory remit is shown in Figure 10 overleaf.

Figure 10 | The OAIC's key functions and roles

	CRITICAL	STRATEGIC	SUPPORTING
PRIVACY	<ul style="list-style-type: none"> Assess privacy complaints Administer the Notifiable Data Breaches scheme Approve code development 	<ul style="list-style-type: none"> Initiate privacy investigations Conduct privacy assessments Produce regulatory guidance for privacy legislation Develop research and educate the public on privacy (e.g. Australian Community Attitudes to Privacy Survey) 	
FOI	<ul style="list-style-type: none"> Assess IC reviews Assess FOI complaints Assess extension of time applications Assess vexatious applicant declaration applications Administer the Information Publication Scheme 	<ul style="list-style-type: none"> Conduct FOI investigations Conduct FOI monitoring Prepare FOI guidelines Provide advice and training on matters relevant to operation of the FOI Act 	
CDR	<ul style="list-style-type: none"> Monitor and manage the privacy and confidentiality functions of CDR 	<ul style="list-style-type: none"> Conduct CDR assessments Develop CDR regulatory guidance CDR monitoring for small businesses and individuals Develop CDR guidelines and provide advice 	
INFORMATION		<ul style="list-style-type: none"> Engage in information management policy development Perform strategic functions relating to information management in Government 	
OTHER	<ul style="list-style-type: none"> Adhere to public service employment standards Ensure proper financial management and reporting Ensure workplace health and safety compliance 	<ul style="list-style-type: none"> Provide expert advice on privacy to government agencies and other entities involved in Digital ID development Provide guidance to healthcare providers on best practices for managing personal information within the My Health Record system 	<ul style="list-style-type: none"> Conduct people management and development Engage in data management and analytics Provide administrative and support services Conduct communication and engagement Create content and manage publication Manage technology systems Conduct procurement and resource management

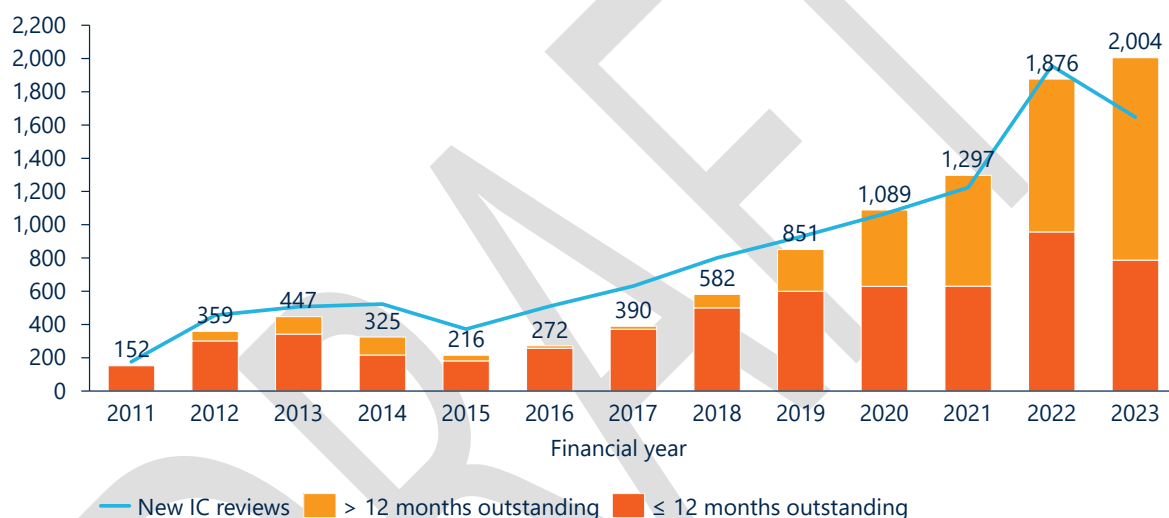
The OAIC has continued to see high and growing demand for its services

The number of Information Commissioner (IC) reviews (see Figure 11 below) and privacy complaints (see Figure 12 overleaf) received by the OAIC has increased since its establishment. As cases have grown faster than they have been resolved, the case backlog – as measured by the number of cases unresolved for over 12 months – has risen, and this has been most pronounced in the OAIC’s IC review jurisdiction.

The OAIC has received increasing numbers of applications for IC review of FOI decisions

The consistent increase in IC reviews on hand is due to the OAIC’s backlog of IC reviews, increasing complexity of IC reviews seeking information relating to third party individuals or national security matters, and where matters are voluminous or raise multiple and overlapping exemption claims. Growth in the number of new IC review applications received and applications outstanding is shown in Figure 11.

Figure 11 | Information Commissioner reviews



Source: OAIC Annual Report 2013-14, OAIC Annual Report 2018-19, OAIC Annual Report 2022-23

The number of privacy complaints has increased over time

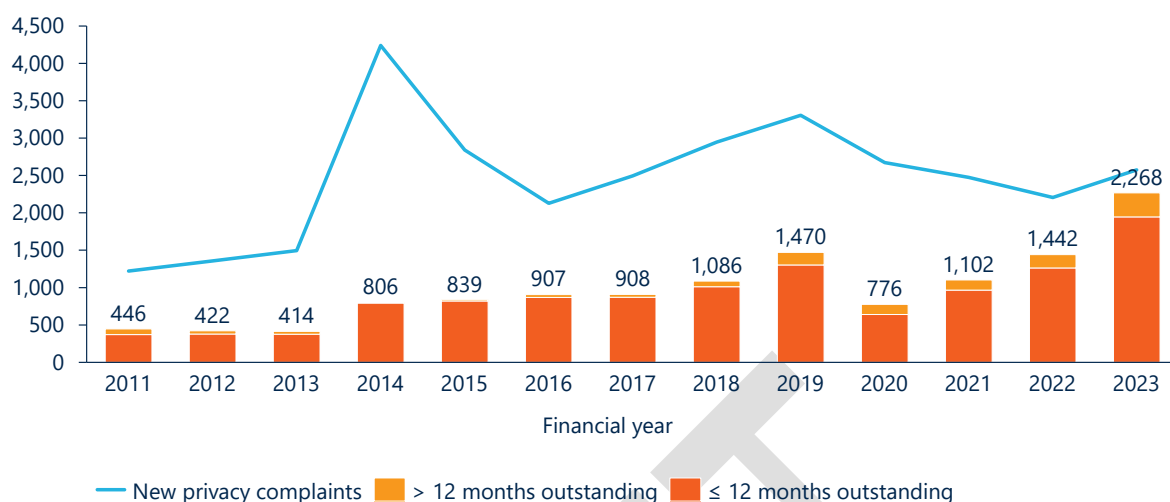
Privacy complaints to the OAIC have increased by 34 per cent in 2022-23 compared to 2021-22, but are below the 2014 peak.³ Complaints have steadily grown since 2011, as shown in Figure 12 overleaf. The increase in complaints relative to 2011 can largely be explained by a combination of increased public awareness of data privacy rights and greater use of digital services that handle personal data. Growing privacy awareness has added to the complexity of the complaints that the OAIC is asked to investigate.

A series of recent high-profile data breaches have also elevated public concern about the handling of data, leading to a large uptick in privacy complaints over the last financial year.⁴

³ The significant increase in privacy complaints in 2014-15 reflects approximately 1,000 complaints following an immigration data breach where the Department of Home Affairs published, in error, a detention report on its website that contained embedded personal information.

⁴ The recent high-profile Optus and Medibank data breaches have drawn attention to the handling of personal information.

Figure 12 | Privacy complaints



Source: OAIC Annual Report 2013-14, OAIC Annual Report 2018-19, OAIC Annual Report 2022-23

The OAIC has met most but not all performance measures in the last financial year

The OAIC's Performance Measurement Framework outlines the agency's approach to evaluating its effectiveness in promoting and upholding privacy and information access rights, based on specific measures contained in its Corporate Plan and Portfolio Budget Statement.

Figure 13 below shows how the OAIC performed last FY against the subset of performance measures that relate to how efficiently the agency is performing its core roles. The OAIC met or was close to meeting all of the targets for five of the six performance measures.

Figure 13 | OAIC Key Performance Outcomes 2022-23

Performance measure	Target	Result	Outcome
1.2.1 Time taken to finalise privacy complaints	80% of privacy complaints finalised within 12 months	84%	✓
1.2.2 Time taken to finalise privacy and FOI Commissioner-initiated investigations (CIIs)	80% of CIIs finalised within 8 months	68%	✗
1.2.3 Time taken to finalise Notifiable Data Breaches (NDBs)	80% of NDBs finalised within 60 days	77%	✗
1.2.4 Time taken to finalise My Health Record notifications	80% of My Health Record notifications finalised within 60 days	100%	✓
1.2.5 Time taken to finalise Information Commissioner (IC) reviews of FOI decisions made by agencies and Ministers	80% of IC reviews finalised within 12 months	78%	✗
1.2.6 Time taken to finalise FOI complaints	80% of FOI complaints finalised within 12 months	94%	✓

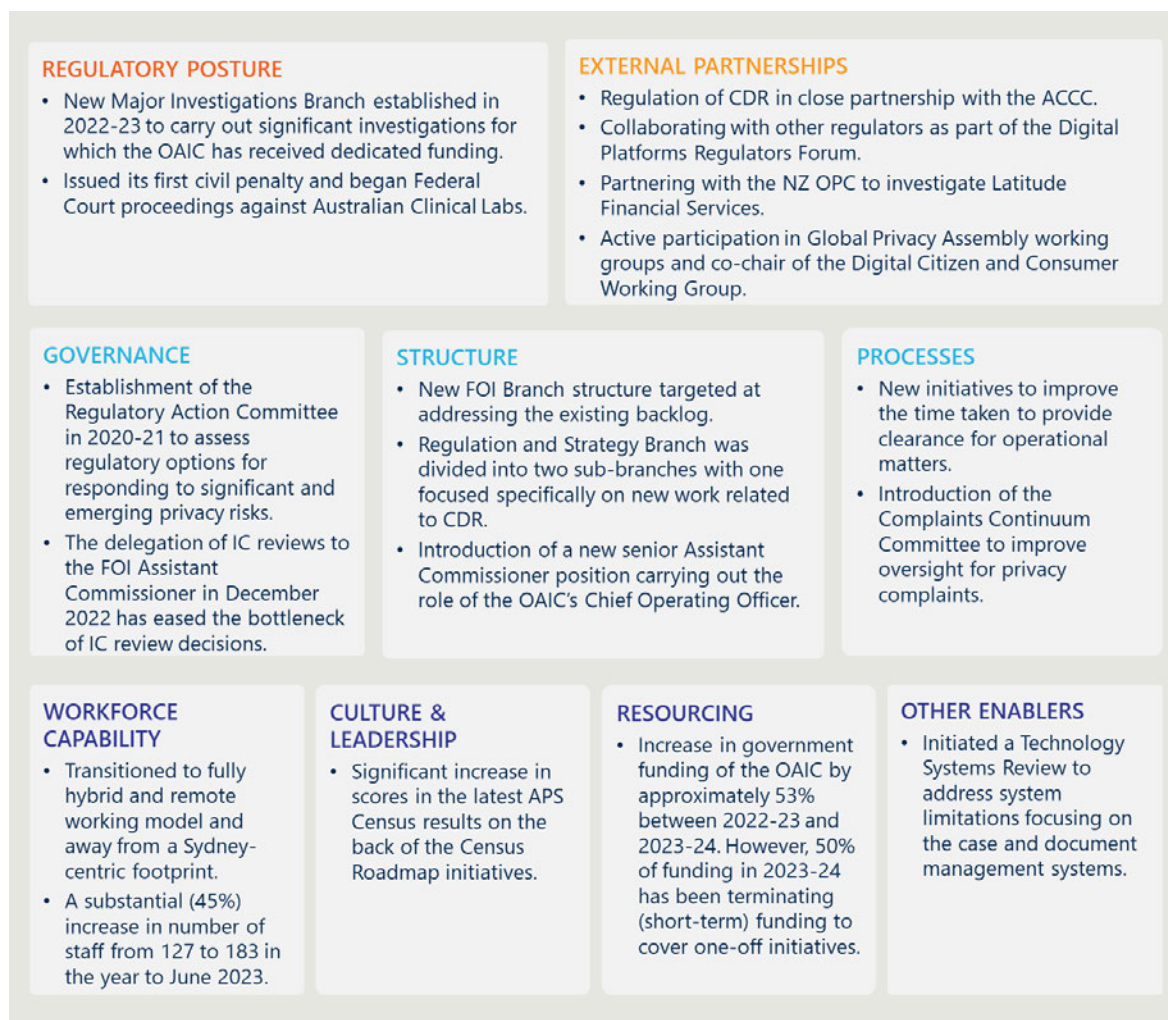
✓ Achieved ✗ Not achieved

Source: OAIC Annual Report 2022-23

The OAIC has implemented a series of initiatives in response to its evolving operating environment and greater size and scope

The OAIC has made substantial changes across all elements of its operating model in the past few years in response to changing demands in an evolving external landscape. Some of these key changes are shown in Figure 14 below.

Figure 14 | Overview of recent reforms to the OAIC's operating model



3 Drivers of change

A range of economic, technological, social and political drivers will play a key role in influencing demand for the OAIC's work and its effectiveness as a regulator. This Chapter explores these drivers in detail and considers some of the likely implications for the OAIC's future regulatory strategy and elements of its operating model. This Chapter provides important context for the findings and recommendations throughout this Strategic Review report.

Figure 15 | Relevant questions from the Terms of Reference

- How can the OAIC best respond to the likely continuing growth to the volume and complexity of its core statutory workload?
- How can the OAIC remain effective as a regulator in responding to changing technology, the growth of the digital economy and increasing cyber crime?

Figure 16 | Summary of key findings

Technological drivers of change

- Further developments in artificial intelligence (AI) will have a profound impact on personal privacy. In response, the OAIC will need to develop regulatory guidance and enforce stricter controls on data sharing.
- New technologies that collect personal information will challenge traditional definitions of personal information. For example, biometric authentication and profiling systems continually collect vast amounts of data and are becoming increasingly common. The OAIC's regulatory guidance will need to keep pace with these changes and provide clarity on emerging technologies and their potential impact on privacy.
- Data breaches are becoming larger in scale and more frequent alongside growth in the digital economy and increasingly sophisticated cyber attacks. In response, the OAIC will need to play a significant role ensuring organisations that collect personal information secure it effectively.
- Cybercrime is becoming more sophisticated and widespread, raising the risks to personal data security. The OAIC will need to contribute to Government cyber security efforts and raise awareness through education initiatives.

Social drivers of change

- Societal expectations of individual privacy protection are changing. Most Australians are now highly aware of their privacy rights due to recent large-scale data breaches and understand the importance of personal information security.
- Changes in societal expectations reflect a desire for government to do more to uphold privacy and information access rights. The vast majority of Australians would like government agencies to act and do more to protect their personal information, including through legislative change. These expectations will likely drive an increased workload for the OAIC to uphold privacy protections.

Political drivers of change

- The Government's expectations of the OAIC have evolved in response to increasing privacy harms. The OAIC is expected to take an approach that balances education of regulated

entities that supports voluntary compliance with enforcement to promote public confidence in the regulatory activities of the agency.

- Significant legislative and policy reforms and reviews – particularly the Privacy Act Review – will place greater demand on the OAIC. The proposed reforms from the Privacy Act Review will broaden the OAIC's enforcement powers and require updated regulatory guidance.
- Suggested reforms from the FOI Senate Inquiry may require increased engagement with agencies to prioritise its efforts to develop guidance and build the capacity of decision-making agencies.
- In other areas of the OAIC's remit, expansions in scope and changes in legislation for CDR and Digital ID will also require an updated regulatory posture and guidance.

The volume and complexity of the OAIC's core statutory workload is expected to increase in the coming years

Technological, social and political trends are expected to place increased demand – to varying degrees – on the key functions performed by the OAIC. The impact of these trends on the OAIC's functions is summarised at a macro level in Figure 17.

The OAIC's privacy functions are where the most significant impacts will be felt as digital transformation across sectors leads to vast amounts of data being hosted online increasing the potential for large scale data breaches and associated enforcement action.

s47C



s47C



3.1 Technological drivers of change

Technological shifts will lead to a growing expectation for enforcement action by the OAIC

As the digital transformation of our economy continues, the volume of data managed by entities regulated by the OAIC will expand and the methods used to process this data will become more complex.

Rapid advances in artificial intelligence (AI) and machine learning will lead to dramatically more sophisticated data processing techniques, placing pressure on the OAIC to develop mechanisms for data validation and guidelines.⁷ Data breaches are becoming larger and more common with the expansion of personal data being exchanged through digital platforms and increased rates of cyber crime.

The key technological shifts that will impact the OAIC in the coming years are outlined in Figure 18.

Figure 18 | Technological drivers of change and implications for the OAIC

Driver	Description	Evolving risk landscape
Growing use of AI	<ul style="list-style-type: none"> Developments in AI will have a profound impact on personal privacy. Generative AI and large language models can collect personal data by making semi-hidden information more visible through reidentification, challenging the effectiveness of traditional privacy protections. AI tools can also combine personal information with misleading information which will pose a new type of threat to individual privacy. 	<ul style="list-style-type: none"> Without greater regulatory guidance on the use of personal information in AI and enforcement of AI-related privacy breaches, there is the potential for the large-scale erosion of individual privacy. The risk is growing as reflected by the fact that 68 per cent of Australian businesses have already implemented AI technologies and a further 23 per cent are planning to implement them in the next 12 months.
New technologies that collect personal information	<ul style="list-style-type: none"> New types of information are being collected that challenge traditional definitions of personal information. Biometric authentication and profiling systems continually collect vast amounts of data. This increases the volume of data to be protected while also introducing potentially new forms of personal information that will need to be regulated. 	<ul style="list-style-type: none"> Personal information could be hacked and misused without consequence if new technologies continue to be used to collect this information without updates to the definition of personal information and guidance from the OAIC on emerging technologies. New technologies are collecting large volumes of personal information, with 95 per cent of

⁷ It is currently unclear what regulator or regulatory scheme will address emerging issues linked to AI safety and AI ethics. Absent a dedicated AI regulator, OAIC is well positioned to have a role in ensuring harms from AI are minimised while benefits are maximised.

Driver	Description	Evolving risk landscape	Implications for the OAIC
Larger and more frequent data breaches	<ul style="list-style-type: none"> Data breaches are becoming larger in scale and more frequent alongside growth in the digital economy and increasingly sophisticated cyber attacks. Breaches are increasingly occurring in the health and financial services sectors. Increasing amounts of data are expected to be collected in these sectors, including as part of the expansion of My Health Record. 	<p>Australians reporting use of at least one biometric security technology in 2022.</p> <ul style="list-style-type: none"> If data breaches are left unchecked and not investigated thoroughly, risk of identity theft and fraud will increase and there will be a loss of public trust in digital services and institutions. The risk posed by these breaches is large and growing, with significant data breaches resulting in millions of Australians having their information stolen and leaked on the dark web in 2022. The most recent data shows that around 70 per cent of breaches are the result of malicious or criminal attacks. 	s47C
Increasing cyber crime	<ul style="list-style-type: none"> Cybercrime is becoming more sophisticated and widespread, raising the risks to personal data security. Phishing, ransomware attacks and other forms of malicious activities are aimed at illegally accessing and exploiting personal data. 	<ul style="list-style-type: none"> Without regulatory action, increasing cybercrime will lead to more significant financial and personal losses from cyber attacks. There were 94,000 cyber crime reports in 2022-23, reflecting an increase of 23 per cent from the previous financial year. Australians lost over \$3 billion to scams in 2022. This is an 80 per cent increase on total losses recorded the prior year. 	s47C

3.2 Social drivers of change

Societal expectations of individual privacy protection are changing

In recent years, there has been a shift in technology usage where individuals increasingly provide their personal information on digital platforms, while simultaneously expecting enhanced intervention from the OAIC to safeguard their data.

A significant share of Australians are now highly aware of their privacy rights and the importance of personal information security as reflected by the OAIC's Australian Community Attitudes to Privacy Survey. Awareness has grown following recent large-scale data breaches that refocused attention on online privacy and forced individuals to reflect on how their personal information is stored, managed and shared online. The survey showed that approximately two-thirds (64 per cent) of Australians have experienced at least one issue with how their personal information has been handled within the past 12 months.

Changes in societal expectations are contributing to a desire for government to do more to uphold privacy and information access rights

Social expectations concerning privacy and access to government information are shifting. This is reflected in the trajectory of privacy complaints and FOI submissions which continue to grow. A significant share of Australians are highly aware of their privacy rights.⁸ With greater public awareness of privacy rights, it is likely that this awareness will drive increases in enquiries and complaints to be addressed by the OAIC. When significant privacy breaches occur, there will also be a greater expectation of government intervention that will also place pressure on the OAIC in its enforcement capacity.

Similarly, there is increasing public awareness about the right to access information held by public entities.⁹ This awareness will likely see more individuals exercise this right, increasing the volume of Information Commissioner reviews and FOI complaints. Societal expectations reflect that the public want more action to prevent government entities from delaying public requests for information or dealing with these requests inadequately.

Expectations for greater privacy protection will likely drive an increased workload for the OAIC

The latest Australian Community Attitudes to Privacy Survey found that 62 per cent of Australians view the protection of their personal information as a major concern but only 32 per cent feel in control of their data privacy. As a result, expectations of the OAIC and broader government action are growing – 89 per cent of Australians would like government agencies to act and do more to protect their personal information, including through legislative change.¹⁰

⁸ [Australian Community Attitudes to Privacy Survey 2023](#)

⁹ [Australian Government Information Access Survey 2023](#)

¹⁰ [Australian Community Attitudes to Privacy Survey 2023](#)

3.3 Political drivers of change

The Government's expectations of the OAIC have evolved in response to increasing privacy harms

In the latest Ministerial Statement of Expectations published in March 2023, the Government outlined the principles expected of the OAIC in its regulation of privacy and FOI matters.¹¹ The Government expects the OAIC to take an approach that balances education of regulated entities that supports voluntary compliance with enforcement to promote public confidence in the regulatory activities of the agency. The OAIC is also expected to focus on regulatory activities that address harms arising from the use of digital platforms in particular, reflecting the growing risk posed by these platforms.

The pressing nature of the issues at hand has seen Government consult with key stakeholders and develop plans for action. The new Australian Cyber Security Strategy is a key example and will see the OAIC play a role contributing to a range of actions to strengthen Australia's cyber security, including to support the uplift of data governance and security across the economy.¹² The Government has also recently consulted on safe and responsible AI, drawing on the expertise of the OAIC and other bodies on the impact of AI in relation to privacy.¹³

s47C



¹¹ [Ministerial Statement of Expectations \(2023\)](#)

¹² [2023 Cyber Security Strategy](#)

¹³ [Safe and responsible AI in Australia consultation: Australian Government's interim response](#)

The proposed reforms from the Privacy Act Review will broaden the OAIC’s enforcement powers and require updated regulatory guidance

The Privacy Act Review proposals enhance privacy protections in a range of ways that will lead to a step change in the OAIC’s effort. These proposals are outlined in Figure 19. Many of the recommendations are expected to be implemented over the coming years.

Figure 19 | Overview of key Privacy Act recommendations agreed by Government

Proposal	Goal
Proposal 25.10 The OAIC should conduct a strategic internal organisational review with the objective of ensuring the OAIC is structured to have a greater enforcement focus.	Greater enforcement focus
Proposal 25.9 Amend the annual reporting requirements in AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground of section 41.	Increased transparency
Proposal 28.1 Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.	
Proposal 25.1 Create tiers of civil penalty provisions to allow for better targeted regulatory responses.	
Proposal 25.2 Amend section 13G of the Act to remove the word ‘repeated’ and clarify what a ‘serious’ interference with privacy may include.	Risk-based enforcement approach
Proposal 25.11 Amend subsection 41(dc) of the Act so the Information Commissioner has the discretion not to investigate complaints where a complaint has already been dealt with by an EDR scheme.	

The recommendations outlined in Figure 19 focus on the proposals that have been agreed by Government. Those that have been agreed in-principle and will likely have a significant impact on the OAIC are detailed in Figure 20. These recommendations are subject to further consideration, including stakeholder consultation and impact analysis. A detailed analysis outlining the potential changes to the OAIC from the proposed reforms is contained in Appendix D.

Figure 20 | Overview of key Privacy Act recommendations agreed in-principle by Government

Change	Reform proposals		Type of work	Impact ¹⁴
Enhanced enforcement powers	Proposals 25.1, 25.2, 25.4, 25.5 and 25.10: Introduction of new civil penalty provisions, public inquiry powers and structure to have a greater enforcement focus.	s47C	Ongoing	s47C

s47C

Change	Reform proposals	s47C	Type of work	Impact ¹⁴								
Data security and privacy guidance enhancement ¹⁵	Proposals 21.3, 21.5, 28.1 and 28.4: Enhanced guidance on data security, breach responses, and cross-agency cooperation in enforcement.		s47C	Ongoing	s47C							
Organisational and operational reforms	Proposals 25.6, 25.9 and 25.11: Greater cooperation with other bodies and introduction of new reporting requirements.			s47C		Ongoing	s47C					
Automated decision-making and emerging technology regulation	Proposals 13.2, 13.3, 19.1 and 19.2: Development of guidance for new technologies, privacy impact assessments, and automated decision-making processes.					s47C		One off	s47C			
Increased transparency in data handling	Proposals 23.1 and 23.5: Enhanced transparency requirements for overseas data flows and entities' data handling practices.							s47C		One off	s47C	
Vulnerability and consent guidance**	Proposals 17.1 and 17.2: Development of guidance on handling data of vulnerable individuals and consent processes.									s47C		One off

s47C

s47C

s47C

Figure 21 | Overview of potential reforms from the FOI Senate Inquiry

Area	Suggested Reforms	OAIC Impact	Type of work	Impact ¹⁶
Education, monitoring and guidance	The OAIC prioritises efforts to develop guidance and strengthen pathways for people accessing personal information outside of FOI.	s47C		
The OAIC's functions	Move IC review functions and the FOI Commissioner to the Commonwealth Ombudsman's Office or remove IC reviews and allow applicants to appeal directly to the Administrative Appeals Tribunal (AAT).			
Culture	There should be an independent external review of the culture of the OAIC.			

s47C

s47C

4 Strategy, regulatory posture and approach

The extent to which the OAIC's strategy, regulatory approach and posture are clear, modern and risk-based will be critical to the OAIC's ability to respond to the likely continuing growth of its workload and be an effective regulator of information rights into the future. This chapter outlines the current state and provides recommended changes that the OAIC could make to improve its strategy, regulatory posture and approach to enable it to best respond to changes to demand on its workload and the external environment.

Figure 24 | Relevant questions from the Terms of Reference

- How can the OAIC best respond to the likely continuing growth to the volume and complexity of its core statutory workload?
- How can the OAIC remain effective as a regulator in responding to changing technology, the growth of the digital economy and increasing cyber crime?
- What is the role of the OAIC in providing advice and reports to Government about privacy, information access and information management?

s47C



Effective regulation is supported by a clear regulatory strategy. A regulatory strategy typically comprises a regulator's strategic plan, regulatory posture and approach. Each of these elements is explored further in Figure 27 below.

Figure 27 | Overview of elements of regulatory strategy

Element	Overview
Strategic plan	<p>A strategic plan sets out the overarching purpose and vision and what a regulator seeks to achieve, including:</p> <ul style="list-style-type: none"> • Regulatory purpose articulating who the regulator is, what it does and for whom. This should be derived from its legislative mandate and organisational context. • Regulatory vision identifying the regulator's desired future. • Strategic objectives identifying specific, longer horizon goals the regulator seeks to achieve.
Regulatory posture	<p>Regulatory posture describes where the regulator will focus its effort. Regulators need to decide what percentage of their activities will react to instances of non-compliance and what percentage will proactively attempt to promote compliance. Some decisions around where to place regulatory emphasis are enshrined in the legislation administered by the regulator, but many involve considering the external operating environment and organisational priorities.</p> <p>Regulatory posture also involves deciding where a regulator sits on the regulatory spectrum. For example, a regulator can focus at the education and information end of the spectrum – seeking to change behaviour (make regulated entities compliant) through engagement, education etc. Or it can focus its effort at the enforcement end of the spectrum – taking targeted action against wrongdoers that directly address noncompliance and act as a deterrent to others.</p>
Regulatory approach	<p>Regulatory approach is how the regulator uses its regulatory tools and powers to achieve its strategic plan and posture. Regulatory approach is made up of:</p> <ul style="list-style-type: none"> • How a regulator prioritises matters. • How a regulator exercises its regulatory functions in respect of the matters it prioritises. <p>A risk-based approach focuses resources and efforts on the risks associated with non-compliance with rules, rather than the rules themselves. It is based on the notion that it is impossible to avoid all risks and that regulatory tools and powers should aim to effectively manage risks. One of the Regulator Performance (RMG 128) principles for best practice regulator performance is being 'risk based and data driven'.</p>

The analytical framework for the Strategic Review articulates the criteria that we have used to assess the effectiveness and appropriateness of the OAIC's current regulatory strategy for the OAIC. These criteria and the associated tests are outlined in detail in Figure 28 below.

Figure 28 | Tests of effective regulatory strategy

Criteria	Test
Strategic plan	
Clear and concise	<ul style="list-style-type: none"> Can the community, staff, regulated entities easily understand what the OAIC is seeking to achieve?
Focused	<ul style="list-style-type: none"> Does the strategic plan set the focus and direction of where the OAIC puts its attention and how it uses its regulatory powers and tools?
Regulatory posture	
Articulates emphasis of effort	<ul style="list-style-type: none"> Does the regulatory posture describe where effort is focused and where the OAIC sits on the regulatory spectrum?
Reflects demand	<ul style="list-style-type: none"> Is the regulatory posture reflective of current and future demand and expectations on the OAIC?
Aligned with strategic plan	<ul style="list-style-type: none"> Are regulatory tools and powers consistently being used to further the objectives in the strategic plan?
Regulatory approach	
Reflects risk of harm	<ul style="list-style-type: none"> Does the regulatory approach identifying the greatest risks the OAIC is seeking to address?
Enables prioritisation	<ul style="list-style-type: none"> Does the regulatory approach prioritise high-risk matters with the greatest potential for harm?
Focuses powers and tools	<ul style="list-style-type: none"> Does the regulatory approach outline which powers and tools to apply to address that risk?

4.1 Strategic plan

The OAIC's strategic plan outlines its purpose and strategy to uphold information rights

The OAIC's current strategic plan outlines its purpose and strategy to uphold information rights. **s47C**

Figure 29 | Summary overview of the OAIC's current strategic plan

Purpose	Promote and uphold privacy and information access rights.			
Vision	To increase public trust and confidence in the protection of personal information and access to government-held information.			
Strategy	Prevent privacy harm and uphold the community's access to information rights in the areas of greatest impact and concern.			
Key activities	Influence and uphold privacy and information access rights frameworks.	Advance online privacy protection for Australians.	Encourage and support proactive release of government information.	Take a contemporary approach to regulation.
Success measures	The OAIC's regulatory outputs are timely.	The OAIC's activities support innovation and capacity for Australian businesses to benefit from using data, while minimising privacy risks for the community.	The OAIC's activities support government agencies to provide quick access to information requested and at the lowest reasonable cost, and proactively publish information of interest to the community.	The OAIC's approach to its regulatory role is consistent with better practice principles.
Enablers	Continuous improvement and building trust.	Adopting a risk-based and data-driven approach.	Collaboration and engagement.	

Source: OAIC's Corporate Plan 2023-24

s47C

4.2 Regulatory posture

s47C



- A new Major Investigations Branch was established in 2022-23 to carry out significant investigations. The OAIC currently has 3 open investigations against large companies Optus, Medlab and Medibank in relation to significant data breaches. The OAIC commenced its first civil proceedings in 2020 against Facebook and issued further proceedings against ACL in 2023. Both proceedings are on foot in the Federal Court.
- The OAIC conducted a Commissioner initiated investigation and follow up into Department of Home Affairs' compliance with FOI processing timeframes in 2020. The investigation found shortfalls and made recommendations which have been implemented and have significantly improved the Department's FOI policy, procedures and outcomes for applicants.

s47C



s47C

- 62 per cent of respondents to the Community Attitudes to Privacy Survey 2023 do not know how to protect their personal information and see it is a major concern in their life. 89 per cent would like government agencies to act and do more to protect their personal information. Expectations of government intervention require a stronger enforcement posture including more assessments and investigations.
- Witnesses to the FOI Senate Inquiry called for a more responsive FOI culture among agencies and increased OAI guidance. Witnesses submitted that agency delay and impunity for breaches of FOI timeframes causes significant frustration and impacts work of stakeholders including journalists and organisations seeking documents to advise refugees. A stronger enforcement approach to improve compliance by FOI agencies would promote a more responsive FOI culture. FOI agencies and witnesses see benefit in OAI guidance material on how agencies can build a culture of proactive

disclosure and strengthen pathways for accessing personal information outside the FOI regime. Expectations of witnesses and FOI agencies require a stronger enforcement and education posture.

s47C



4.3 Regulatory approach

There are two key elements in the OAIC’s current regulatory approach – its regulatory priorities and its regulatory action policies. Each of these elements are discussed in turn below. We then move to a discussion about the OAIC’s recommended future regulatory approach.

4.3.1 Regulatory priorities

The OAIC has publicly articulated its regulatory priorities

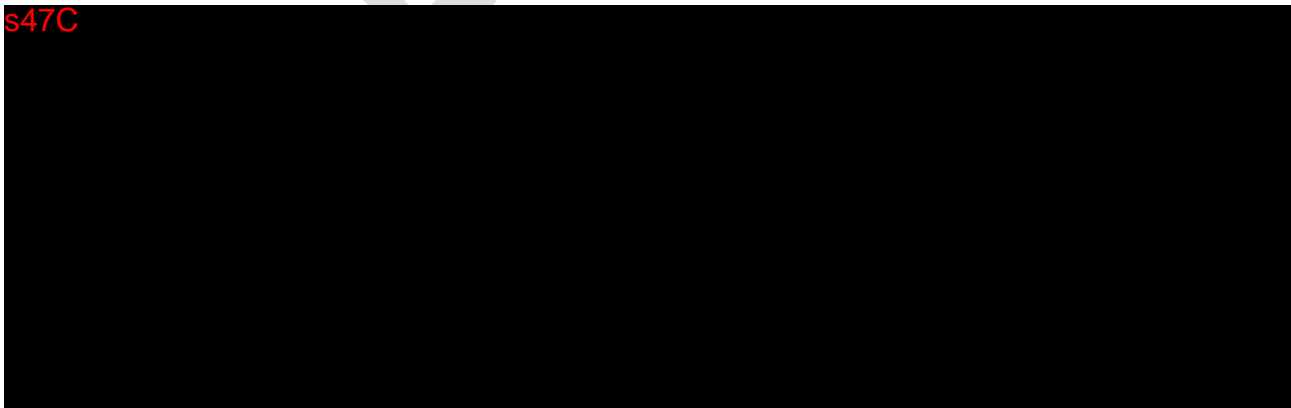
The OAIC has published regulatory priorities in 2022-23 to guide where to direct resources, set out in Figure 31. The OAIC uses these regulatory priorities to ‘ensure that the OAIC’s resources are focused on the prevention of privacy harm and upholding the community’s access to information rights in the areas of greatest impact and concern’.¹⁷

Figure 31 | OAIC’s regulatory priorities

Regulatory Priorities	
1. Online platforms, social media and high privacy impact technologies	Harms which impact on individuals’ choice and control, through opaque information practices or terms and conditions of service. Technologies and business practices that record, monitor, track and enable surveillance, and the use of algorithms to profile individuals in ways they may not understand or expect, with adverse consequences.
2. Security of personal information	Serious failures to take reasonable steps to protect information or report. Risks and mitigations have previously been publicised by the OAIC. Finance and health sectors.
3. Consumer Data Right	Coordinated compliance and enforcement activities by the OAIC and the ACCC. Ensuring that the fundamental privacy safeguards provided by the system are upheld by participants to protect consumers’ information.
4. Proactive disclosure of government-held information	The need for agencies to make timely decisions and proactively disclose information to support an efficient access to information regime.

Source: OAIC’s [Regulatory Approach](#)

s47C



¹⁷ Source: OAIC’s [Regulatory Approach](#)

5 Governance

Governance will be an important enabler for the OAIC to achieve its purpose and future functionality. This Chapter provides an outline of the Strategic Review's findings relating to governance. It outlines current governance arrangements and provides recommended changes that the OAIC could make to enable its governance arrangements to best achieve its purpose and future functionality.

Figure 35 | Relevant questions from the Terms of Reference

- To what extent is the OAIC's governance suitable to achieve its purpose and future functionality?

s47C



- The Strategic Review considered governance criteria, comparable models and legislative requirements to develop and refine options with the OAIC executive. The relevant legislative requirements, including the AIC Act, the Privacy Act, the FOI Act, the Public Service Act and the PGPA Act, have also been considered.

s47C



s47C

The analytical framework for the Strategic Review articulates five criteria for the OAIC's governance arrangements, as set out in Figure 38. These criteria have been tested and refined with the OAIC's executive.

These criteria have been used by the Strategic Review team to test the suitability of the OAIC's current governance arrangements and inform recommendations related to the agency's future governance arrangements.

Figure 38 | Assessing the suitability of the OAIC's governance

Criteria	Test
Strategic alignment	To what extent do governance arrangements align and enable the OAIC's overarching strategy?
Respects decision-making role of commissioners	To what extent are the decision-making roles of each of the Commissioners respected?
Show clear lines of accountability	Are there clear lines of accountability for each Commissioner and the governance structures that support them, in respect of the OAIC's remit?
Reserve Commissioner time for value-adding work	To what extent is the Commissioners' time reserved for value-adding work (i.e. decision-making and external facing work, not operations)?
Supports integration	To what extent do governance arrangements support an integrated OAIC?

The OAIC's governance in recent years has been calibrated to several different Commissioner arrangements

The AIC Act provides for a three Commissioner model that includes the Australian Information Commissioner (Information Commissioner), a Privacy Commissioner and an FOI Commissioner. The Information Commissioner is also the agency head for the purposes of the *Public Service Act 1999* (Public Service Act) and is the accountable authority for the purposes of finance law provided under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

The Information Commissioner holds a unique role among the three Commissioners as agency head and accountable authority. As Agency Head the Information Commissioner has the employer powers and as accountable authority the Information Commissioner is responsible for the way in which the OAIC must be governed to promote the proper use of public resources and achieve the OAIC's purposes and financial sustainability.

The OAIC's current governance arrangements have been developed over time to meet the needs of the different Commissioner models it has operated within. In recent years, the Information Commissioner has also delivered the Privacy Commissioner role and for a long period between 2014 and 2021 the FOI Commissioner role was vacant, with the Australian Information Commissioner also carrying out those functions. Between 2021 and early 2024 three different people have carried out the FOI Commissioner role, with only one of these formally appointed to the role.

The OAIC's current governance arrangements include a number of committees which advise the Information Commissioner in relation to operational and strategic matters and statutory decision-making:

- The **Executive Committee** supports the Information Commissioner to achieve the strategic objectives of the OAIC by ensuring Executive focus on privacy and FOI priorities. The committee is chaired by the Australian Information Commissioner and membership consists of OAIC Commissioners and SES-level staff members.
- The **Operations Committee** ensures Executive oversight in the management of the OAIC and several subcommittees (Health, Safety and Wellbeing Committee, Security Governance Committee, Information Governance Committee, OAIC Consultative Forum). The committee is chaired by the OAIC Deputy Commissioner and membership consists of SES-level staff members.
- The **Audit and Risk Committee** provides advice to the Information Commissioner on the appropriateness of the OAIC's financial reporting, performance measurement, system of risk oversight and management, and systems of internal control.
- The **Regulatory Action Committee** advises the Information Commissioner on suitable regulatory responses to significant privacy risks.

The OAIC will soon be returning to a three Commissioner model. In May 2023 the Government announced the appointment of standalone Freedom of Information and Privacy Commissioners, increasing the permanent number of statutory information officers from one to three. The formal appointment of these two new Commissioners was announced in November 2023 and they will commence at the OAIC in February 2024.

s47C



6 Organisational structure

A fit-for-purpose structure will be a critical enabler for the OAIC's future effectiveness. This Chapter describes the OAIC's current structure and assesses its alignment with the best practice criteria in our analytical framework. The Chapter also outlines a number of potential structural options that the OAIC could adopt going forward in response to several key drivers of change.

Figure 40 | Relevant questions from the Terms of Reference

- To what extent is the OAIC's structure suitable to achieve its purpose and future functionality?

Figure 41 | Summary of key findings

- The OAIC's current structure focuses firstly on the division between privacy and FOI work and then by the necessary functions associated with each regulated area. This structure reflects the OAIC's extensive growth in staff and areas regulated over the past 10 years.
- The OAIC has made structural changes in recent years to support an increased enforcement focus. This includes standing up the Major Investigations Branch in October 2022, to facilitate large scale investigations in a focused and direct manner.

s47C

s47C

The analytical framework for the Strategic Review articulates seven best practice criteria and tests that have been used to assess the appropriateness of the OAIC's current organisational structure and to design potential new structural options. These criteria have been tested and refined with OAIC's Executive, and are outlined in Figure 43.

Figure 43 | Assessing the suitability of the OAIC's structure

Criteria	Test
Alignment to strategy	To what extent does the OAIC's structure enable it to achieve its strategic priorities?
Integrated approach	Does the structure enable a 'one OAIC' approach to integrated, end-to-end regulation and facilitate a smooth and collaborative workflow between teams?
Responsiveness	To what extent does the OAIC's structure enable efficient and effective response (including decision-making) to high-risk matters, and more broadly?
Focus on stakeholders	To what extent does the OAIC's structure enable effective engagement and communication with stakeholders, meeting evolving needs and expectations?
Clear roles and accountabilities	To what extent does the OAIC's structure enable clear definitions of staff members' positions, reporting lines, and ensure responsibilities (including handover points) are clearly assigned, with accountability for achieving desired outcomes?
Minimises duplication	To what extent does the OAIC's structure minimise inefficient duplication of effort?
Expertise	To what extent does the OAIC's structure foster regulated area expertise across the agency?

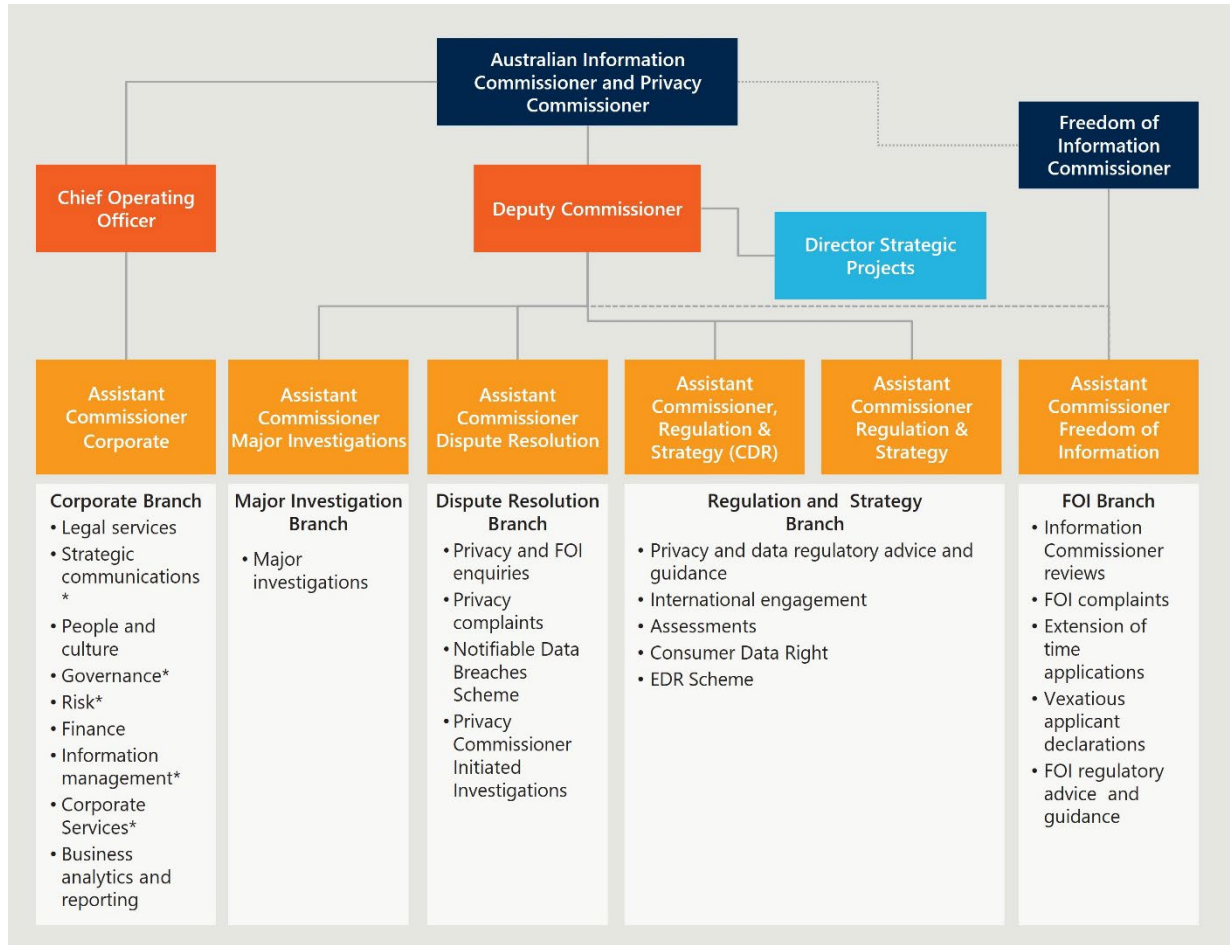
The OAIC's current structure is organised by regulated area with some functional elements

The OAIC's current structure divides the agency into branches by regulated area and corporate functions. Figure 44 provides a high-level overview of this structure and the functions completed by each branch, which are split by regulated area and by the type of action completed.

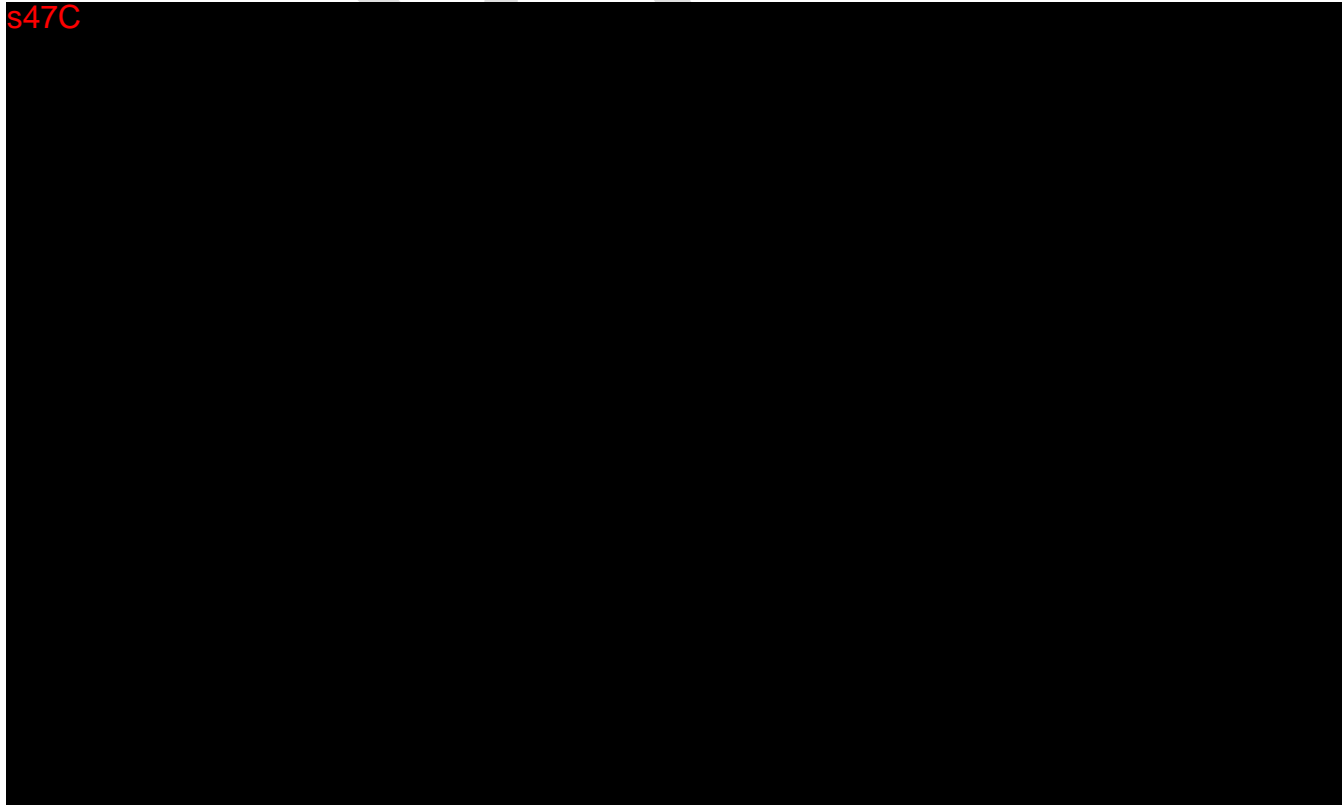
This structure focuses firstly on the division between privacy and FOI work and then by the necessary functions associated with each regulated area. This structure reflects the OAIC's extensive growth in staff and areas regulated over the past 10 years.

Privacy and FOI, and their associated branches, are structured quite differently. FOI is organised into a single branch and privacy split across four branches: Major Investigations, Dispute Resolution, Regulation and Strategy and Regulation and Strategy (CDR). The four privacy branches have overlapping areas of function with Major Investigations covering large scale privacy CIs and NDBs and the two Regulation and Strategy branches split by CDR associated functions and Privacy (non-CDR functions). In the current structure all non-corporate branches report to the Deputy Commissioner, with corporate branches reporting to the Chief Operating Officer (COO).

Figure 44 | The OAIC’s current organisational structure



s47C



7 Processes and systems

The extent to which the OAIC's processes and systems are efficient and contemporary will play a critical role in the OAIC's ability to respond effectively and efficiently to the likely continuing growth to the volume and complexity of its core statutory workload. This Chapter assesses the OAIC's current processes and systems and identifies opportunities to further refine key processes in ways that should yield significant efficiencies and enable the agency to deliver on its updated strategic plan (see Chapter 4).

Figure 46 | Relevant questions from the Terms of Reference

- How can the OAIC best respond to the likely continuing growth to the volume and complexity of its core statutory workload?
- How can resource allocation be optimised to maximise efficiency and support the OAIC's statutory functions?

s47C



s47C

The analytical framework for the Strategic Review articulates three criteria for the OAIC's processes and systems, as set out in Figure 49. These criteria have been used to test the suitability of the OAIC's processes and systems and develop our recommendations.

Figure 49 | Assessing the suitability of the OAIC's processes and systems

Criteria	Test
Maximises efficiency	To what extent do the OAIC's processes and systems support the efficient delivery of its functions?
Maximises effectiveness	To what extent do the OAIC's processes and systems enable the achievement the agency's intended outcomes and performance metrics?
Consistently applied	To what extent are OAIC's processes and systems well documented, understood across the agency and consistently applied?

7.1 Limitations of the OAIC's current processes and systems

The OAIC's key processes and functions are derived from its statutory responsibilities

The core statutory functions of the OAIC are the management of the Privacy Act across the public and private sectors and oversight of the operation of the FOI Act.¹⁹ The OAIC's most significant processes in terms of collective resourcing required are those associated with IC reviews and privacy complaints (as discussed further in Chapter 2 of this report).

¹⁹ OAIC, What we do, <https://www.oaic.gov.au/about-the-OAIC/what-we-do>

8 Organisational capability

This Chapter provides an outline of the Strategic Review's findings relating to the OAIC's organisational capability. Attracting and retaining the right skills and capabilities and fostering an inclusive and high performing culture will play a critical role in whether the OAIC can successfully deliver on its regulatory strategy.

Figure 55 | Relevant questions from the Terms of Reference

- To what extent are the OAIC's organisational capabilities suitable to achieve its purpose and future functionality?

Figure 56 | Summary of key findings

Workforce capability and skills

- The OAIC's workforce has undergone significant changes over the last three years, with a significant increase in size (from 105 in 2020 to 162 in 2023), the move towards a permanent hybrid working model and a transition from a predominantly Sydney based workforce to one that is dispersed across the country. The agency has also experienced high levels of turnover across all branches over the last two financial years.
- These factors have posed challenges related to the building and retention of corporate memory and know-how related to the OAIC's core functions.
- The profile of skills across the OAIC will need to evolve as the agency responds to rapidly evolving technological drivers of change and moves towards a greater focus on enforcement to address harm arising from privacy breaches and education/guidance. The agency will likely need to build and acquire skills and capabilities related to cyber security, AI, data analytics, forensic investigations, and engaging with and educating industry.

s47C

- The OAIC's remuneration is low compared with many other agencies and well behind equivalent state government or private sector roles – particularly in the legal and technology sectors. The OAIC therefore needs to compete in the labour market on other factors such as

purpose and workplace conditions. Most staff appreciate the OAIC's flexible work environment.

s47C

Sourcing external capabilities

- In recent years the OAIC has substantially increased its spending on external legal support, from \$1.1 in FY20 to \$5.7 million in FY23, as the agency has shifted to a more enforcement centred focus. s47C

s47C

The analytical framework for the Strategic Review articulates four criteria for the OAIC's organisational capabilities, as set out in Figure 58. These criteria have been used to test the suitability of the OAIC's organisational capabilities and develop our recommendations.

Figure 58 | Assessing the suitability of the OAIC's organisational capabilities

Criteria	Test
Appropriately skilled	Does the OAIC have the right number and type of capabilities and skills that it needs to effectively and efficiently deliver on its regulatory strategy?
Compelling employee value proposition	To what extent does the OAIC have a compelling value proposition for current and prospective staff?
High performing and inclusive culture	Does the OAIC have a high performing and inclusive culture?
Optimal out-sourcing	Is the OAIC's procuring external capabilities under appropriate circumstances?

8.1 Workforce capability and skills

The OAIC's workforce has transformed significantly over the last few years which has resulted in challenges related to building and retaining corporate memory

The OAIC's workforce has undergone significant changes over the last three years, with a significant increase in FTE (from 105 in 2020, to 162 in 2023) and the move towards a permanent hybrid working model. The two changes combined have resulted in a change from most staff being co-located in the OAIC's Sydney office to a workforce that lives and works across the country. The OAIC's geographic footprint by branch is shown in Figure 59 below.

Figure 59 | FTE by location and branch

Location	Corporate	Dispute Resolution	FOI	Major Investigations	Regulation and Strategy	Executive	Total
ACT	5	1	5		1	1	12
NSW	18	41	16	9	21	1	106
NT			1				1
QLD	7	2	3		3	1	17
SA	5	3			6		14
TAS		1		1	1		3
VIC	10	3	1		4	1	19
WA		1	2				3
Total	45	51	28	10	35	4	173

Source: OAIC supplied data as at September 2023

At the same time as OAIC's workforce has become larger and more geographically dispersed, the agency has experienced high levels of turnover across all branches over the last two financial years, as shown in Table 6 below. The OAIC's digital platforms have therefore been critical in enabling collaboration between teams and the onboarding of new staff.

Table 6 | Attrition rate for all staff by branch

Branch	2021–22	2022–23
Dispute Resolution	33%	20%
Regulation and Strategy	38%	16%
Freedom of Information	58%	36%
Corporate	54%	39%
Corporate (Legal Services)	38%	42%
Executive	14%	22%
Total	40%	25%

Source data provided by OAIC

The agency's workforce has a higher proportion of female, NESB, part-time staff relative to the APS average. See Appendix G for further details of key workforce metrics for the agency relative to APS averages.

OAIC staff on average have a lower median length of service relative to the APS average and a higher exit rate of ongoing employees in 22/23. This is particularly the case for more junior staff, which has resulted in two distinct cohorts of staff in the OAIC. Many of the OAIC's leadership team have spent a large part of their career at the agency. Whereas more junior staff have typically spent significantly less time in the OAIC and the APS.

Taken together, all the above factors have posed challenges in recent years related to the building and retention of corporate memory and know-how related to the OAIC's core functions.

s47C

8.2 Employee experience

s47C



Figure 61 | Feedback from OAIC staff about their connections to work

Purpose	Leadership	Inclusion
<p>Employee connection to the organisation's mission, purpose and strategy.</p> <p>s47C</p>	<p>Employee perceptions of vision, commitment and support of the organisation's leaders.</p> <ul style="list-style-type: none">• The results from the APS Census indicate that the majority of OAIC staff are happy with the leadership of their immediate supervisor.• The APS Census results for staff's immediate SES manager are also positive.• Staff perceptions about how the OAIC's broader SES cohort are less positive and are slightly less positive than 2022 – although the OAIC's results are still better than all of the Census benchmarks. <p>s47C</p>	<p>Employee sense of belonging and perceived safety in bring whole-of-self to work.</p> <ul style="list-style-type: none">• 86 per cent of staff feel that the OAIC supports and actively promotes an inclusive workplace culture – an increase of 10 per cent from the 2022 APS Census results.
<p>s47C</p>		
<p>s47C</p>		
<p>s47C</p>		

s47C

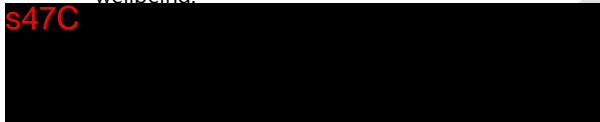


Figure 63 | Feedback from OAIC staff about their employment experience

Wellbeing	Infrastructure
The focus on work-related safety and creation of a climate fostering wellbeing	The physical and digital resources available for employees to perform their roles.

- The OAIC scores well on APS Census questions related to promoting and communicating wellbeing.

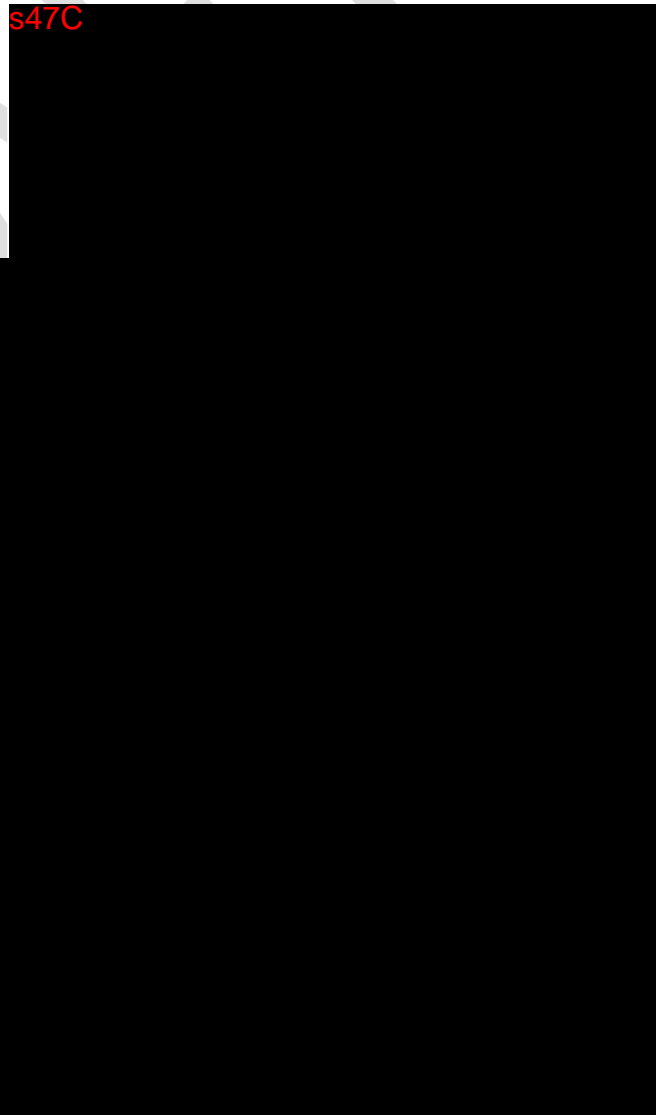
s47C



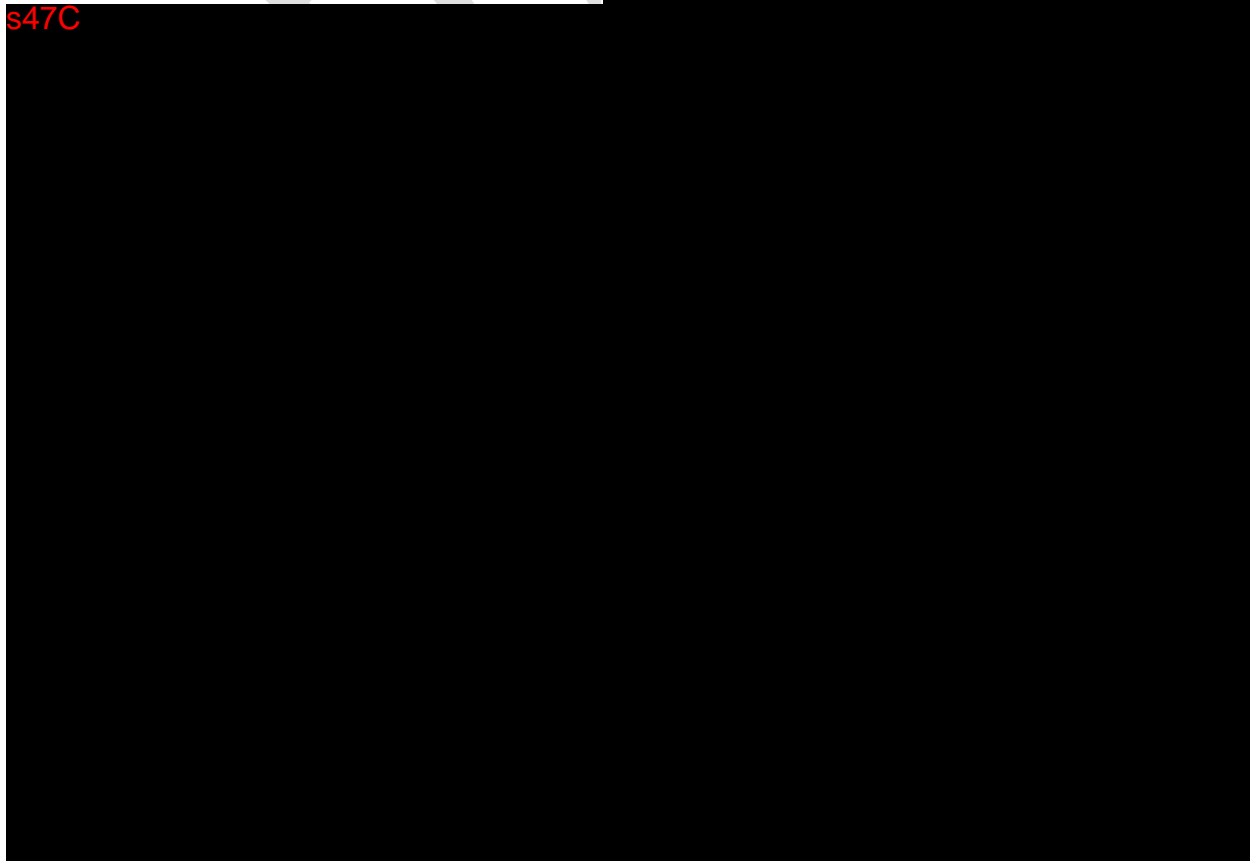
- The proportion of staff that agree or strongly agree that they feel burned out by their work increased in the 2023 APS Census results.
- The frequency with which staff always or often find their work stressful also increased in the 2023 results.

- Only 38 per cent of OAIC staff that responded to the APS Census agreed that their workgroup has the tools and resources they need to perform well – substantially below the APS benchmark and other similar agencies.

s47C



s47C



The OAIC struggles to compete with other employers on the basis of salary

The OAIC's remuneration is low compared with many other agencies and well behind equivalent state government or private sector roles – particularly in the legal and technology sectors. The OAIC therefore needs to compete in the labour market on other factors such as purpose and workplace conditions.

s47C

Figure 64 | Feedback from OAIC staff about how they are rewarded and recognised

Compensation	Conditions
<p>The fixed and variable remuneration for employees.</p> <ul style="list-style-type: none">• Only 41 per cent of OAIC staff feel that they are fairly remunerated (e.g. salary, superannuation) for the work that they do – well below all of the APS Census benchmarks.• The OAIC current pay scales are in the lower third of APS agencies – which makes it hard for the agency to compete with other agencies, other jurisdictions (particularly the NSW Government) and with private sector companies (particularly private law firms).• s47C	<p>Work settings, including flexibility and work-life balance.</p> <ul style="list-style-type: none">• There is strong support for and uptake of flexible working across the OAIC, with 79 per cent of staff working away from the office or work from home (+22 greater than the APS average).• s47C• s47C• 43 per cent of APS Census respondents said that their workloads are well above capacity (well above all other Census benchmarks).

s47C

8.4 Sourcing external capabilities

The OAIC currently relies on external legal providers to undertake a range of core activities

In recent years the OAIC has substantially increased its spending on external legal support, from \$1.8 million in 2019 to \$7.4 million in 2023, as the agency has shifted to a more enforcement centred focus and increased its litigation activities.

s47C



9 Resourcing and resource allocation

As an independent statutory agency under the Attorney-General's Department portfolio, the OAIC is resourced through government appropriations to oversee government information policy functions, access to government held information and promote data protection in the public and private sectors. This Chapter provides an outline of the Strategic Review's findings relating to resourcing of the OAIC. It outlines the current state and provides recommendations about changes that the Government and the OAIC could make to optimise resource allocation and enable the OAIC to deliver its future regulatory strategy more effectively and efficiently.

Figure 67 | Relevant questions from the Terms of Reference

- To what extent is the OAIC's resourcing suitable to achieve its purpose and future functionality?
- How can resource allocation be optimised to maximise efficiency and support the OAIC's statutory functions?

Figure 68 | Summary of key findings

- The OAIC's resourcing has increased substantially in recent years to support the growth in workload and resulting increase in staff however ^{s47C} [REDACTED]. The agency's total resourcing (ongoing and terminating funding) has increased from \$10 million to \$46 million over the past ten years. This includes a 234 per cent increase in ongoing funding over the same period.
- This additional funding has come with a range of additional responsibilities. The bulk of this funding has been provided to allow the OAIC to deliver specific additional activities or functions. (E.g. My Health Record regulation, CDR, Digital ID, specific investigations etc.)

s47C

s47C

The Strategic Review employed the criteria and tests outlined in Figure 70 below to assess the appropriateness of the OAIC's resourcing and resource allocation and to develop our recommendations about related to future changes.

Figure 70 | Assessing the suitability of the OAIC's resourcing

Criteria	Test
Allocated appropriately	Is the OAIC appropriately balancing funding and resource allocation across its statutory functions?
Maximises efficiency	Is the OAIC using its funding as efficiently as possible?
Sufficient	To what extent is the OAIC's resourcing suitable to achieve its purpose and future functionality?

The OAIC's resourcing has increased substantially in recent years, enabling the agency to hire staff to manage its growing workload

The OAIC's total resourcing (ongoing and terminating funding) has increased significantly over the past ten years from \$10 million to \$46 million. This includes a 234 per cent increase in ongoing funding over the same period. This growth reflects the increase in workload and responsibilities of the OAIC as outlined in Chapter 2, including the management of privacy functions of new government initiatives (Digital ID and My Health Record), supporting the introduction and privacy function of CDR across three sectors of the economy, and the commencement of major investigations into Optus, Medibank and Latitude.

s47C

Figure 71 below outlines the funding profile of the OAIC over the past decade, and shows the considerable funding increase the OAIC has received since 2019 for both ongoing base and terminating functions.

Figure 71 | OAIC resourcing profile



Source: Budget Measures: Budget Paper 2 2022-23 (March), Budget Measures: Budget Paper 2 2022-23 (October), Budget Measures: Budget Paper 2 2023-24, OAIC Portfolio Budget Statement 2023

The increase in the OAIC's resourcing has supported the growth of staff from 79 in 2010 to 162 in 2023. With these resources, the OAIC has been able to undertake new responsibilities and achieve many of its performance measures.

Terminating funding measures accounted for half of the OAIC's total funding in 2023-24, outlined further in Table 7 below. These measures include short-term functions and functions such as major investigations that currently have no ongoing base funding attached.

Table 7 | Current OAIC terminating measures

Measure	Description	Budget allocation	FY Terminating
Next Steps for Digital ID	To provide ongoing privacy assurance for the Digital ID program	\$1.1 million for 1 year	2023-24
My Health Record	To regulate the privacy aspects of the My Health Record system	\$4.8 million over 2 years	2024-25
CDR Enhancement	To support the continued operation of CDR in the banking, energy and non-bank lending sectors	\$3.3 million over 2 years	2024-25

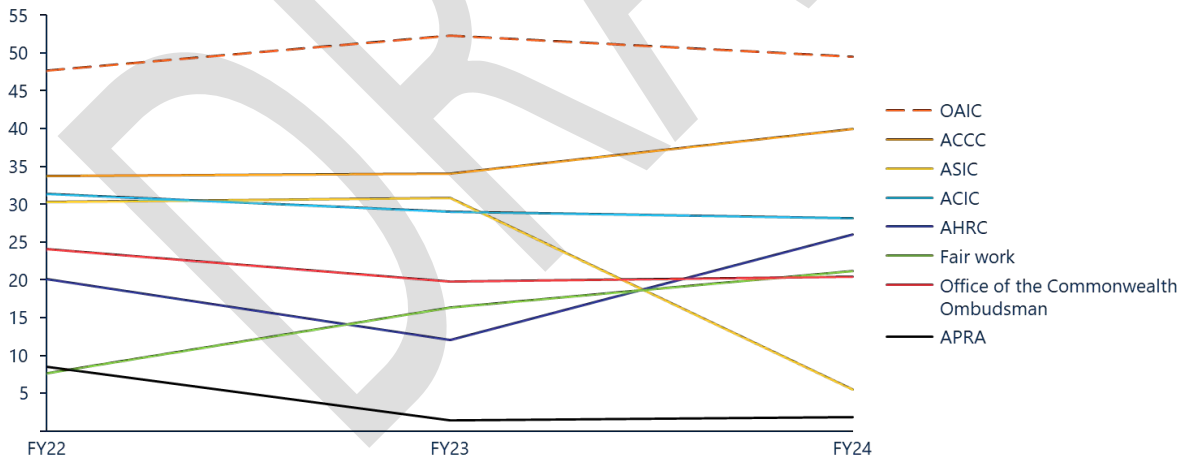
Measure	Description	Budget allocation	FY Terminating
Stronger privacy enforcement (non-ongoing portion)	To support a standalone Privacy Commissioner, enhance data and analytics capability and progress enforcement and investigations actions.	\$10.7 million over 4 years (part of the \$44.3 million measure)	2026-27
Privacy and social media	To undertake its privacy and regulatory functions including in relation to social media and other platforms	\$17 million over 2 years	2023-24
Optus	To investigate and respond to the Optus data breach.	\$5.5 million over 2 years	2023-24

Source: Budget Measures: Budget Paper 2 2022-23 (March), Budget Measures: Budget Paper 2 2022-23 (October), Budget Measures: Budget Paper 2 2023-24

The OAIC’s Major Investigations Branch is currently funded through the specific Optus investigation budget measure and other stronger privacy enforcement funding to facilitate the Medibank, ACL and Latitude investigations. Due the expected completion of these terminating measures, the Major Investigations Branch is only funded until June 2024. s47C

The OAIC has a relatively high proportion of terminating funding when compared to other regulators – as illustrated in Figure 72 below. s47C

Figure 72 | Percentage of terminating budget measures for like government regulators



Source: Portfolio Budget Statements 2024-23 and Budget Measures: Budget Paper 2 2022-23 (March), Budget Measures: Budget Paper 2 2022-23 (October), Budget Measures: Budget Paper 2 2023-24

s47C



s47C



The OAIC's external legal expenditure has increased alongside greater enforcement activity, rising from an average of approximately \$1 million over the past 3 years to \$7.25 million in 2023-24. This spending has been used to support major investigations and litigation, including the Optus data breach investigation and litigation in relation to Medlab and Medibank.

s47C



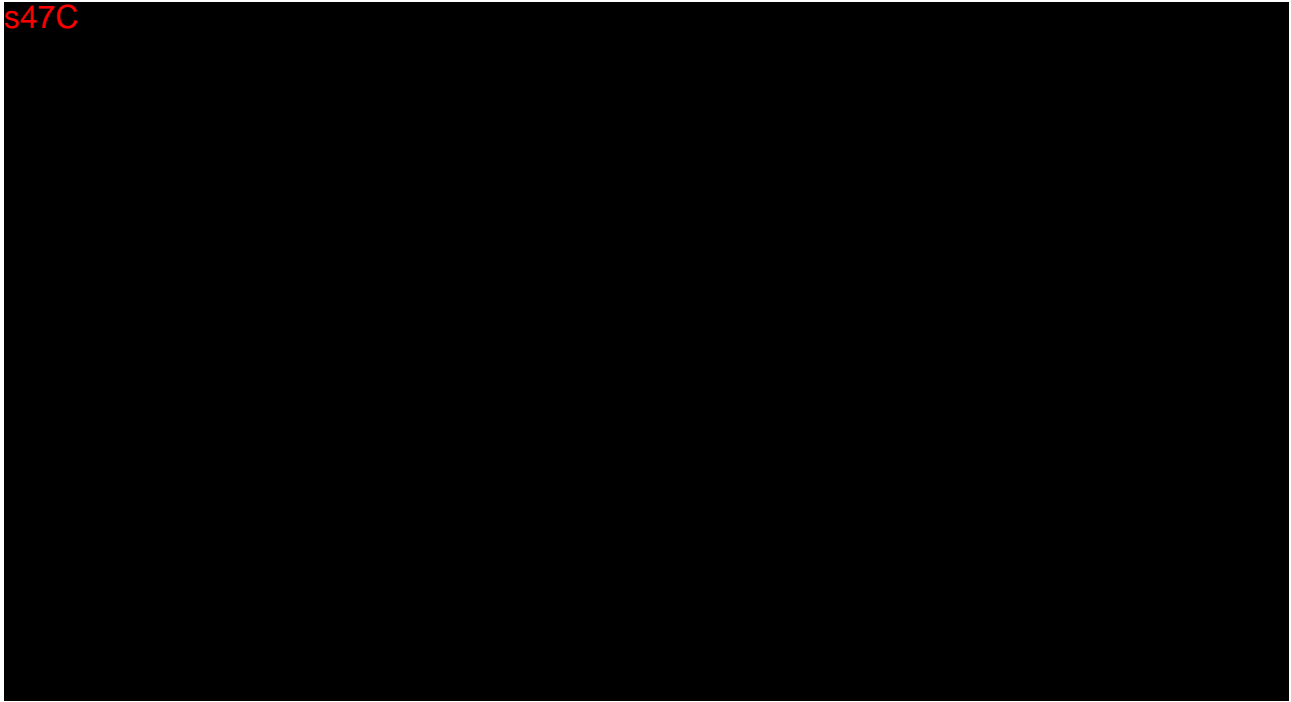
s47C



s47C

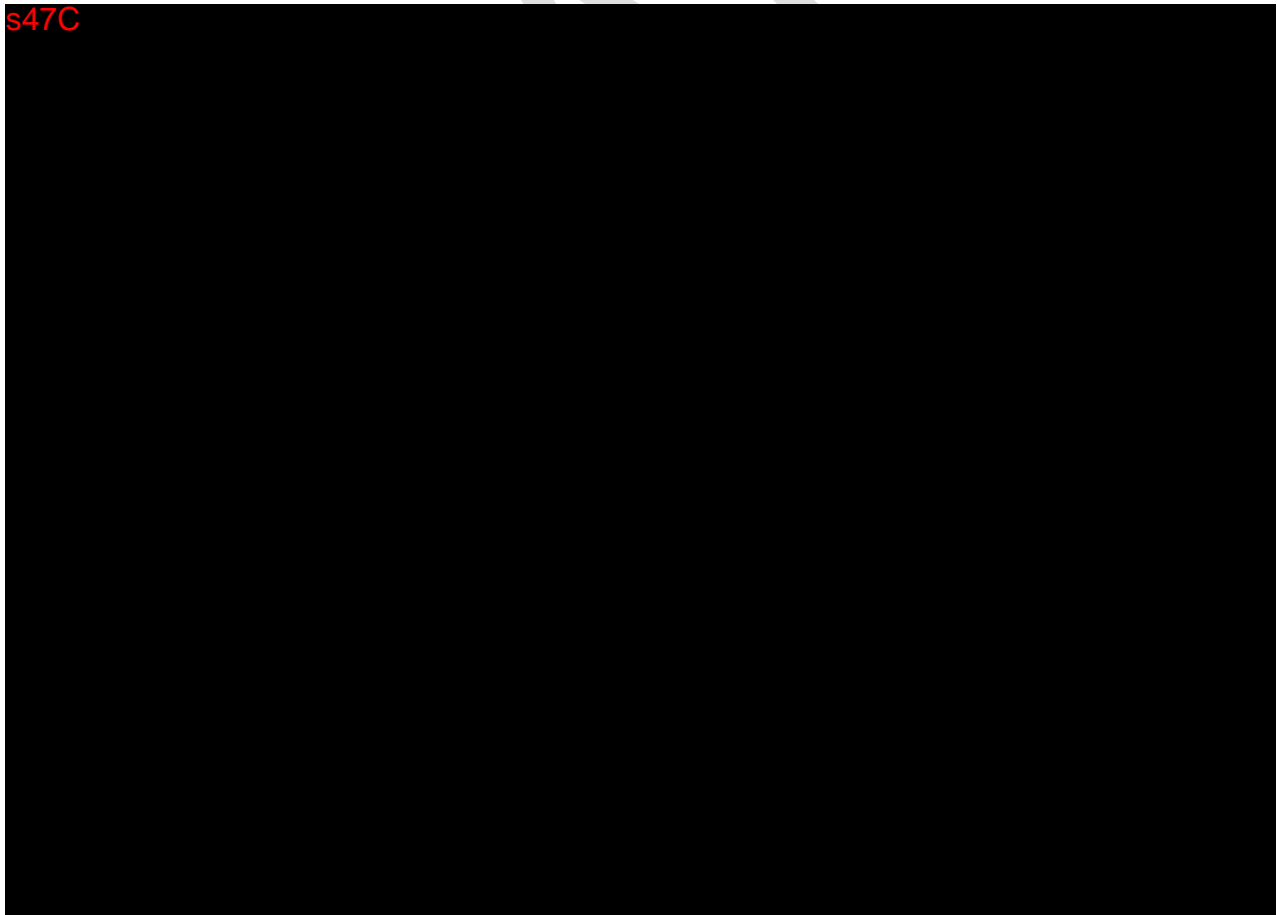


s47C



The Australian Cyber Security Strategy recently noted that the acceleration of cyber attacks will lead to more frequent and large-scale data breaches containing personal information.²⁶ As the regulator of privacy in Australia, the OAIC is best placed to investigate and respond to these breaches.

s47C



²⁶ Australian Cyber Security Strategy, Department of Home Affairs, 2023

Appendix A Terms of Reference for the Strategic Review

A strategic review of the Office of the Australian Information Commissioner (OAIC) will ensure the OAIC is well positioned to deliver on its statutory functions as the national privacy and information access regulator into the future.

Scope

The reviewer should consider, report, and make recommendations about how the OAIC can ensure it is best positioned to deliver on its functions as the national privacy and information access regulator and respond to future challenges. Recommendations should cover:

- the extent to which the OAIC's
 - organisational capability,
 - structure,
 - governance, and
 - resourcing
- are suitable to achieve the OAIC's purpose and future functionality, or require amendment;
- how resource allocation can be optimised to maximise efficiency and support the OAIC's statutory functions;
- how OAIC can best respond to the likely continuing growth to the volume and complexity of its core statutory workload;
- how to ensure the effectiveness of the OAIC as a regulator in responding to changing technology, the growth of the digital economy and increasing cybercrime; and
- the role of the OAIC in providing advice and reports to government about privacy, information access and information management.

Contextual information

The reviewer must have regard to relevant contextual matters, about which the OAIC will provide the reviewer with relevant background, including:

- potential changes to the functions of the OAIC arising from the Government's response to the Privacy Act Review;
- the operation of FOI laws;
- evolving community expectations about privacy and information access, and expectations that OAIC will take a strong enforcement posture.

Recommendations

The reviewer must identify recommendations that can be implemented within the existing legislative framework, but may make recommendations that require legislative change where the reviewer considers necessary.

Activities

As a minimum, the reviewer should examine relevant documents and data, conduct interviews with OAIC executives, staff, and key external stakeholders, and examine the capabilities and arrangements of a selection of analogous agencies in Australia and elsewhere.

Timeframe

Interim report by **15 January 2024**. Final report by **5 February 2024**.

DRAFT

Appendix B Review data sources and methodology

[Drafting Note: To be included in Final Report]

DRAFT

Appendix C Stakeholder engagement

C.1 Engagement with OAIC staff

[Drafting Note: To be included in Final Report]

C.2 Engagement with external stakeholders

[Drafting Note: To be included in Final Report]

DRAFT

Appendix D Privacy Act Review Impact Analysis

D.1 Proposals agreed

An impact assessment of the Privacy Act Review proposals on the OAIC is outlined in the table below and overleaf. **s47C**

Proposal	Government Response
<p>Proposal 25.1 Create tiers of civil penalty provisions to allow for better targeted regulatory responses:</p> <p>(a) Introduce a new mid-tier civil penalty provision to cover interferences with privacy without a 'serious' element, excluding the new low-level civil penalty provision.</p> <p>(b) Introduce a new low-level civil penalty provision for specific administrative breaches of the Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties</p>	Agree
<p>Proposal 25.9 Amend the annual reporting requirements in AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground of section 41.</p>	Agree
<p>Proposal 25.10 The OAIC should conduct a strategic internal organisational review with the objective of ensuring the OAIC is structured to have a greater enforcement focus.</p>	Agree
<p>Proposal 21.3 Enhance the OAIC guidance in relation to APP 11 on what reasonable steps are to secure personal information. The guidance that relates to cyber security could draw on technical advice from the Australian Cyber Security Centre.</p>	Agree

s47C

Proposal	Government Response
<p>Proposal 25.2 Amend section 13G of the Act to remove the word 'repeated' and clarify that a 'serious' interference with privacy may include: (a) those involving 'sensitive information' or other information of a sensitive nature; (b) those adversely affecting large groups of individuals; (c) those impacting people experiencing vulnerability; (d) repeated breaches; (e) wilful misconduct, and (f) serious failures to take proper steps to protect personal data.</p> <p>The OAIC should provide specific further guidance on the factors that they take into account when determining whether to take action under section 13G.</p>	Agree
<p>Proposal 25.11 Amend subsection 41(dc) of the Act so that the Information Commissioner has the discretion not to investigate complaints where a complaint has already been adequately dealt with by an EDR scheme.</p>	Agree
<p>Proposal 28.1 Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.</p>	Agree
<p>Proposal 29.2 Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.</p>	Agree

s47C

Proposal	Government Response
<p>Proposal 5.1 Amend the Act to give power to the Information Commissioner to make an APP code where the Attorney General has directed or approved that a code should be made: (a) where it is in the public interest for a code to be developed, and (b) where there is unlikely to be an appropriate industry representative to develop the code.</p> <p>In developing an APP code, the Information Commissioner would: (a) be required to make the APP Code available for public consultation for at least 40 days, and (b) be able to consult any person he or she considers appropriate and to consider the matters specified in any relevant guidelines at any stage of the code development process.</p>	Agree
<p>Proposal 13.2 Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities. This work should be done as part of a broader consideration by government of the regulation of biometric technologies.</p>	Agree
<p>Proposal 25.11 Amend subsection 41(dc) of the Act so that the Information Commissioner has the discretion not to investigate complaints where a complaint has already been adequately dealt with by an EDR scheme.</p>	Agree
<p>Proposal 28.1 Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.</p>	Agree
<p>Proposal 29.2 Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.</p>	Agree

s47C

Proposal	Government Response
<p>Proposal 5.1 Amend the Act to give power to the Information Commissioner to make an APP code where the Attorney General has directed or approved that a code should be made: (a) where it is in the public interest for a code to be developed, and (b) where there is unlikely to be an appropriate industry representative to develop the code.</p> <p>In developing an APP code, the Information Commissioner would: (a) be required to make the APP Code available for public consultation for at least 40 days, and (b) be able to consult any person he or she considers appropriate and to consider the matters specified in any relevant guidelines at any stage of the code development process.</p>	Agree
<p>Proposal 13.2 Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities. This work should be done as part of a broader consideration by government of the regulation of biometric technologies.</p>	Agree
<p>Proposal 13.3 The OAIC should continue to develop practice-specific guidance for new technologies and emerging privacy risks. Practice-specific guidance could outline the OAIC's expectations for compliance with the Act when engaging in specific high-risk practices, including compliance with the fair and reasonable personal information handling test.</p>	Agree
<p>Proposal 17.1 Introduce, in OAIC guidance, a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information.</p>	Agree

s47C

Proposal	Government Response
<p>Proposal 19.2 High-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Act. This should be supplemented by OAIC Guidance.</p>	Agree
<p>Proposal 21.5 The OAIC guidance in relation to APP 11.2 should be enhanced to provide detailed guidance that more clearly articulates what reasonable steps may be undertaken to destroy or de-identify personal information</p>	Agree
<p>Proposal 23.1 Consult on an additional requirement in subsection 5B(3) to demonstrate an 'Australian link' that is focused on personal information being connected with Australia.</p>	Agree
<p>Proposal 25.3 Amend the Act to apply the powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014 to investigations of civil penalty provisions in addition to the Information Commissioner's current investigation powers.</p>	Agree
<p>Proposal 25.4 Amend the Act to provide the Information Commissioner with the power to undertake public inquiries and reviews into specified matters on the approval or direction of the Attorney-General</p>	Agree
<p>Proposal 25.5 Amend subparagraph 52(1)(b)(ii) and paragraph 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined: a declaration that the respondent must perform any reasonable act or course of conduct to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered by the complainant/those individuals. The OAIC should publish guidance on how entities could achieve this.</p>	Agree
<p>Proposal 25.6 Give the Federal Court and the Federal Circuit and Family Court of Australia the power to make any order it sees fit after a civil penalty provision relating to an interference with privacy has been established.</p>	Agree

s47C

Proposal	Government Response
Proposal 28.4 Introduce a provision in the Privacy Act to enable the Attorney-General to permit the sharing of information with appropriate entities to reduce the risk of harm in the event of an eligible data breach. The provision would contain safeguards to ensure that only limited information could be made available for designated purposes, and for a time limited duration.	Agree
Proposal 5.2 Amend the Act to enable the Information Commissioner to issue a temporary APP code for a maximum 12-month period on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.	Agree
Proposal 17.2 OAIC guidance on capacity and consent should be updated to reflect developments in supported decision-making.	Agree

D.2 Proposals agreed in-principle

Proposal	Government Response
Proposal 6.1 Remove the small business exemption, but only after: (a) an impact analysis has been undertaken to better understand the impact removal of the small business exemption will have on small business - this would inform what support small business would need to adjust their privacy practices to facilitate compliance with the Act (b) appropriate support is developed in consultation with small business (c) in consultation with small business, the most appropriate way for small business to meet their obligations proportionate to the risk, is determined (for example, through a code), and (d) small businesses are in a position to comply with these obligations.	Agree in-principle

s47C

Proposal	Government Response
<p>Proposal 6.2 In the short term:</p> <p>(a) prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption, and</p> <p>(b) remove the exemption from the Act for small businesses that obtain consent to trade in personal information.</p>	Agree in-principle
<p>Proposal 25.7 Further work should be done to investigate the effectiveness of an industry funding model for the OAIC.</p>	Agree in-principle
<p>Proposal 25.8 Further consideration should be given to establishing a contingency litigation fund to fund any costs orders against the OAIC, and an enforcement special account to fund high cost litigation.</p>	Agree in-principle
<p>Proposal 26.1 Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy. The model should incorporate the appropriate design elements discussed in this chapter.</p>	Agree in-principle
<p>Proposal 27.1 Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123. Consult with the states and territories on implementation to ensure a consistent national approach.</p>	Agree in-principle

s47C

Proposal	Government Response
<p>Proposal 7.1 Enhanced privacy protections should be extended to private sector employees, with the aim of:</p> <p>(a) providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for</p> <p>(b) ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information</p> <p>(c) ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and</p> <p>(d) notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm.</p> <p>Further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including how privacy and workplace relations laws should interact. The possibility of privacy codes of practice developed through a tripartite process to clarify obligations regarding collection, use and disclosure of personal and sensitive information should also be explored.</p>	<p>Agree in-principle</p>

s47C

Proposal	Government Response
<p>Proposal 13.1 APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks.</p> <p>(a) A Privacy Impact Assessment should be undertaken prior to the commencement of the high-risk activity.</p> <p>(b) An entity should be required to produce a Privacy Impact Assessment to the OAIC on request. The Act should provide that a high privacy risk activity is one that is 'likely to have a significant impact on the privacy of individuals'. OAIC guidance should be developed which articulates factors that that may indicate a high privacy risk, and provides examples of activities that will generally require a Privacy Impact Assessment to be completed. Specific high risk practices could also be set out in the Act.</p>	Agree in-principle
<p>Proposal 18.5 Introduce a right to de-index online search results containing personal information which is:</p> <p>(a) sensitive information [e.g. medical history], or</p> <p>(b) information about a child, or</p> <p>(c) excessively detailed [e.g. home address and personal phone number], or</p> <p>(d) inaccurate, out-of-date, incomplete, irrelevant, or misleading. The search engine may refer a suitable request to the OAIC for a fee. The right should be jurisdictionally limited to Australia.</p>	Agree in-principle
<p>Proposal 18.7 Individuals should be notified at the point of collection about their rights and how to obtain further information on the rights, including how to exercise them. Privacy policies should set out the APP entity's procedures for responding to the rights of the individual.</p>	Agree in-principle
<p>Proposal 18.9 An APP entity must take reasonable steps to respond to an exercise of a right of an individual. Refusal of a request should be accompanied by an explanation for the refusal and information on how an individual may lodge a complaint regarding the refusal with the OAIC.</p>	Agree in-principle

s47C

Proposal	Government Response
<p>Proposal 28.2</p> <p>(a) Amend paragraph 26WK(2)(b) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, the entity must give a copy of the statement to the Commissioner as soon as practicable and not later than 72 hours after the entity becomes so aware, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours.</p> <p>(b) Amend subsection 26WL(3) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity the entity must notify the individuals to whom the information relates as soon as practicable and where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases as soon as practicable.</p> <p>(c) Require entities to take reasonable steps to implement practices, procedures and systems to enable it to respond to a data breach.</p>	Agree in-principle
<p>Proposal 4.1 Change the word 'about' in the definition of personal information to 'relates to'. Ensure the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance.</p>	Agree in-principle
<p>Proposal 4.2 Include a non-exhaustive list of information which may be personal information to assist APP entities to identify the types of information which could fall within the definition. Supplement this list with more specific examples in the explanatory materials and OAIC guidance.</p>	Agree in-principle
<p>Proposal 9.2 In consultation with industry, and the ACMA, the OAIC should develop and publish criteria for adequate media privacy standards and a template privacy standard that a media organisation may choose to adopt.</p>	Agree in-principle

s47C

Proposal	Government Response
<p>Proposal 10.2 The list of matters in APP 5.2 should be retained. OAIC guidance should make clear that only relevant matters, which serve the purpose of informing the individual in the circumstances, need to be addressed in a notice. The following new matters should be included in an APP 5 collection notice:</p> <p>(a) if the entity collects, uses or discloses personal information for a high privacy risk activity —the circumstances of that collection, use or disclosure</p> <p>(b) that the APP privacy policy contains details on how to exercise any applicable Rights of the Individual, and (c) the types of personal information that may be disclosed to overseas recipients.</p>	Agree in-principle
<p>Proposal 10.3 Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.</p>	Agree in-principle
<p>Proposal 11.2 The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consents as part of any future APP codes.</p>	Agree in-principle
<p>Proposal 12.1 Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.</p>	Agree in-principle

s47C

Proposal	Government Response
<p>Proposal 12.2 In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account:</p> <ul style="list-style-type: none"> (a) whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances (b) the kind, sensitivity and amount of personal information being collected, used or disclosed (c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency (d) the risk of unjustified adverse impact or harm (e) whether the impact on privacy is proportionate to the benefit (f) if the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child, and (g) the objects of the Act. The EM would note that relevant considerations for determining whether any impact on an individual's privacy is 'proportionate' and could include: <ul style="list-style-type: none"> (a) whether the collection, use or disclosure intrudes upon the personal affairs of the affected individual to an unreasonable extent (b) whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits, and (c) any actions or measures taken by the entity to mitigate the impacts of the loss of privacy on the individual. 	Agree in-principle
<p>Proposal 12.3 The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained. The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should not apply to exceptions in APPs 3.4 and 6.2. The reference to a 'fair means' of collection in APP 3.5 should be repealed.</p>	Agree in-principle

Proposal	Government Response
<p>Proposal 13.4 Include an additional requirement in APP 3.6 to the effect that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3. OAIC guidelines could provide examples of reasonable steps that could be taken.</p>	<p>Agree in-principle</p>
<p>Proposal 15.2 Expressly require that APP entities appoint or designate a senior employee responsible for privacy within the entity. This may be an existing member of staff of the APP entity who also undertakes other duties.</p>	<p>Agree in-principle</p>

s47C

Appendix G Key workforce metrics

Figure 82 | Key workforce metrics as at 30 June 2023

Workforce metric	OAIC	APS Average
% Female	74.3	60.4
% Indigenous	1.1	3.5
% with a disability	2.7	5.1
% NESB	22.4	15.8
% part-time (ongoing employees)	20.2	13.1
% at the APS classification level	48.6	69.1
Mean Age (years)	39.5	43.1
Median length of service in APS (years)	5.9	9.4
% who have worked in only one agency (ongoing employees)	39.9	67.9
% with a bachelors degree or higher	81.9	67.3
Exit rate (ongoing employees)	14.1	13.5

Source: APSC, APS Employment Data 30 June 2023

Appendix H Resourcing Modelling Methodology

[Drafting Note: To be included in Final Report.]

DRAFT