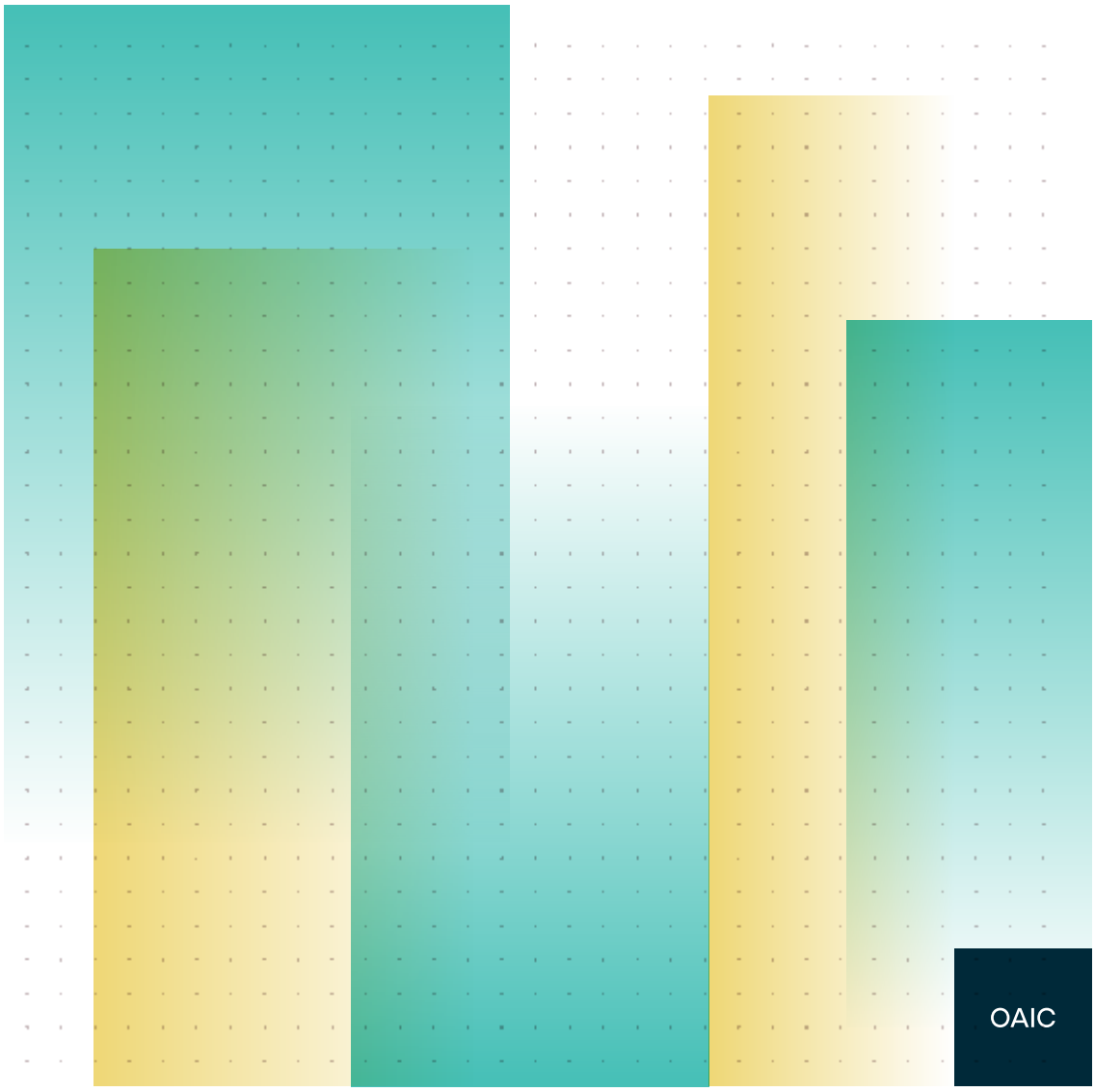
Australian Government

Office of the Australian Information Commissioner

Office of the Australian Information Commissioner

Annual Report 2018–19



Office of the Australian Information Commissioner

Annual Report 2018–19

ISSN 1839-5155

Creative Commons

Contact

Email: enquiries@oaic.gov.au
Website: oaic.gov.au
Phone: 1300 363 992

Mail: Director, Strategic Communications
Office of the Australian Information Commissioner
GPO Box 5218
SYDNEY NSW 2001

Our annual report is also available free of charge on our website at oaic.gov.au.

Non-English speakers

If you speak a language other than English and need help, please call the translating and interpreting service on 131 450 and ask for the Office of the Australian Information Commissioner on 1300 363 992.

Accessible formats

All our publications can be made available in a range of accessible formats. If you would like this report in an accessible format, please contact us.

Cover and design

Swell Design Group

Australian Government
Office of the Australian Information Commissioner

The Hon Christian Porter MP
Attorney-General
Parliament House
Canberra ACT 2600

Dear Attorney

I am pleased to provide to you, for presentation to the Parliament, the Office of the Australian Information Commissioner's (OAIC's) Annual Report 2018–19 for the year ending 30 June 2019.

This report has been prepared for the purposes of s 46 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), which requires that I prepare and provide an annual report to you for presentation to the Parliament.

Section 30 of the *Australian Information Commissioner Act 2010* (AIC Act) requires the Information Commissioner to prepare an annual report — under aforementioned s 46 of the PGPA Act — on the OAIC's operations, including a report on freedom of information matters (defined in s 31 of the AIC Act) and privacy matters (defined in s 32 of the AIC Act).

The freedom of information matters include a summary of the data collected from Australian Government ministers and agencies in relation to activities under the *Freedom of Information Act 1982*.

I certify that the OAIC has prepared a fraud risk assessment and fraud control plan. We also have a number of appropriate fraud prevention, detection, investigation, reporting and data collection mechanisms in place. The OAIC has taken all reasonable measures to minimise the incidence of fraud.

I certify that this report has been prepared in line with the *Public Governance, Performance and Accountability Amendments (Non-Corporate Commonwealth Entity Annual Reporting) Rule 2016*.

Yours sincerely

Angelene Falk
Australian Information Commissioner
Australian Privacy Commissioner

12 September 2019

Contents

Part 1
Overview

About the OAIC

The Office of the Australian Information Commissioner (OAIC) is an independent statutory agency within the Attorney-General's portfolio, established under the *Australian Information Commissioner Act 2010 (AIC Act)*.

Our key role is to meet the needs of the Australian community when it comes to the regulation of privacy and freedom of information. We do this by:

- ensuring proper handling of personal information under the *Privacy Act 1988 (Privacy Act) and other legislation*
- protecting the public's right of access to documents under the *Freedom of Information Act 1982* (FOI Act)
- performing strategic functions relating to information management within the Australian Government under the AIC Act.

Outcome and program structure

Our Portfolio Budget Statement describes the OAIC's outcome and program framework.

Outcome	Provision of public access to Commonwealth Government information, protection of individuals' personal information, and performance of information commissioner, freedom of information and privacy functions.
Program 1.1	Complaint handling, compliance and monitoring, and education and promotion.

Our annual performance statement details our activities, key deliverables and performance measures.

Purpose

Our purpose is to promote and uphold privacy and information access rights.

In the *OAIC Corporate Plan 2018–19* we determined we would be successful if we:

- assisted businesses and Australian Government agencies to understand their privacy obligations, and encouraged them to respect and protect the personal information they handle
- efficiently and effectively took action against suspected interferences with privacy to improve compliance with the Privacy Act
- helped the community to understand and feel confident to exercise their privacy and information access rights
- assisted Australian Government agencies to understand their freedom of information (FOI) obligations, and respect and promote access to government information
- efficiently and effectively carried out our regulatory functions under the FOI Act.

Commissioner's review

In our data-driven economy there is increasing recognition of the value of personal information. The past year's focus on digital platforms in Australia and overseas has brought home the scale of the issues we confront in safeguarding personal data. The importance of access to information in underpinning democracy and open and accountable government has also come to the fore this year in political and media discourse around the world.

Our role in promoting and upholding privacy and access to information rights sits at the centre of these debates on how to meet community expectations and ensure organisational accountability.

These are regulatory issues with global reach, and we are working with our international counterparts as part of a worldwide movement to hold organisations to account and enforce greater transparency. Getting privacy right is not only fundamental to creating greater community trust in the exchange of personal information, it also ensures government-held information is used for public benefit, informs evidence-based policy making and supports innovation.

In addressing these challenges nationally, we worked closely with the Australian Competition and Consumer Commission (ACCC) to consider whether existing privacy legislation is fit for purpose in the digital economy. Through my role on the Executive Committee of the International Conference of Data Protection and Privacy Commissioners, we worked globally towards interoperable regulatory frameworks and support cooperative regulatory action between jurisdictions. We are actively engaged with the Asia Pacific Privacy Authorities forum and Global Privacy Enforcement Network. We are also working with the Attorney-General's Department to implement the Asia-Pacific Economic Cooperation's cross-border privacy rules system in Australia. The global interoperability of privacy law supports a strong domestic economy and provides robust protections for the privacy rights of all Australians.

In March 2019, the Australian Government announced plans for online protections for personal information and increased penalties for its misuse. Additional funding has been provided to the OAIC to assist us in regulating privacy, particularly in the online environment, which will be a significant focus for us over the next three years. These changes would build upon the significant regulatory reforms implemented in 2018. The Notifiable Data Breaches (NDB) scheme was established in February last year to strengthen consumer protection and elevate the security posture of organisations and agencies who handle personal information. Over 2018–19 we received 1,160 data breach notifications, including 950 under the mandatory NDB scheme. During this reporting period, we have worked with notifying organisations to ensure data breaches were contained and rectified, affected individuals were informed so they can act swiftly, and that measures were put in place to prevent a reoccurrence.

In May 2019, we published the *Notifiable Data Breaches Scheme 12-Month Insights Report*, which provides a clear evidence base for regulated entities to prevent data breaches. Most breaches exploited a human factor, such as an employee being tricked into providing credentials that allow cyber intrusion into information and systems. We continued to highlight the need for employees to be supported through training, processes and technology to mitigate this known risk.

Significant areas of work for the OAIC in 2018–19 include our ongoing focus on the Australian Government Agencies Privacy Code and preparing for the Consumer Data Right in our regulatory role with the ACCC and the Data Standards Body. We also regulate the privacy aspects of the My Health Record system, which transitioned to an opt-out system at the start of 2019.

These developments, along with several high-profile data breaches brought to light by the NDB scheme and the European Union's General Data Protection Regulation, have contributed to increased awareness about obligations to protect personal information. They also added to the substance and complexity of many matters brought to us to investigate.

We continued to take an evidence-based and proportionate approach to exercising the range of regulatory tools available to us. In 2018–19 we assessed privacy practices in the finance, telecommunications and government sectors, as well as the digital health sector. We engaged regularly with businesses and Australian Government agencies on good privacy practice and provided advice on a wide range of matters such as credit reporting, government-related identifiers, digital identity systems, de-identification and data-matching. We also made detailed submissions on issues relating to national security, artificial intelligence, cooperative intelligent transport systems and telecommunications.

The privacy issues raised direct us to consider closely whether community expectations, and the current scope and settings of our Privacy Act, are aligned. These issues will also be considered as part of Government's response to the *Digital Platforms Inquiry report*.

International cooperation to strengthen public access to information is also critical. Through our engagement this year with the International Conference of Information Commissioners, we continued to promote the importance of global action on open government. We also continued our work as part of the Open Government Partnership Australia to develop the third National Action Plan to improve transparency in the public sector.

This year I was appointed as a founding member of the National Data Advisory Council, looking at ways to streamline the sharing and release of government data while ensuring the protection of privacy and confidentiality. This is one of many areas where personal data handling and information management considerations converge.

We remain committed to promoting the management and use of government-held information as a national resource for public purposes. As part of this work, in June 2019 we released a survey of government agencies' compliance with the Information Public Scheme (IPS). The results confirmed a continued commitment across government to the IPS's requirements and principles. However, a decline was observed in key areas of compliance compared to our first survey in 2012.

These findings are assisting both the OAIC and government agencies to identify improvements to support the proactive publication of government information.

Day to day, our skilled and dedicated staff continued to assist the community and regulated entities in providing information and resolving a growing number of privacy and FOI complaints and requests for Information Commissioner reviews.

We received 3,306 privacy complaints in 2018–19, an increase of around 12% on the previous financial year. We assisted 2,920 complainants in resolving these issues, nearly 6% more than in 2017–18. Complaints were resolved in an average time of 4.4 months. We also handled 17,445 privacy enquiries.

The number of FOI enquiries rose by almost half in 2018–19 to 2,881 and applications for Information Commissioner (IC) reviews of FOI requests grew by almost 16% to 925. We finalised 8% more IC reviews than in the previous year. IC review decisions continue to provide important guidance to agencies.

We also launched our new website for public feedback in June 2019. Its new architecture improves navigation and search functionality and features a wide range of updated information and advice, particularly for individuals.

Across our core functions, we continued to seek ways to improve our efficiency and effectiveness so we can meet the community's needs. Through our strategic priorities, we are working on behalf of the Australian community to achieve our long-term vision of increasing public trust and confidence in the protection of personal information and access to government-held information.

Angelene Falk
Australian Information Commissioner
Privacy Commissioner
20 August 2019

Our year at a glance

Privacy highlights*

We received

12% more
privacy complaints

2018–19
3,306
Total

2017–18
2,947
Total

Most complaints came from the following sectors

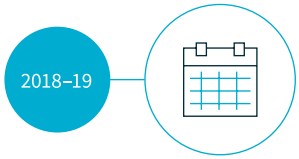
- 13% Finance (including superannuation)
- 12% Australian Government
- 10% Health service providers
- 7% Telecommunications
- 5% Retail
- 5% Online services

We finalised

6% more
privacy complaints

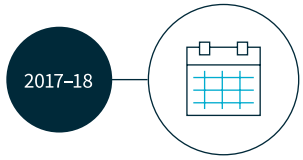
2018–19
2,920
Total

2017–18
2,766
Total



Average time taken to finalise a complaint was

4.4 months



Compared to the time taken last year of

3.7 months

* Percentages have been rounded to the nearest whole number.
End-of-year statistics may differ from quarterly publication statistics.

2018–19

95%

of all privacy complaints were finalised within 12 months of receipt

2017–18

97%

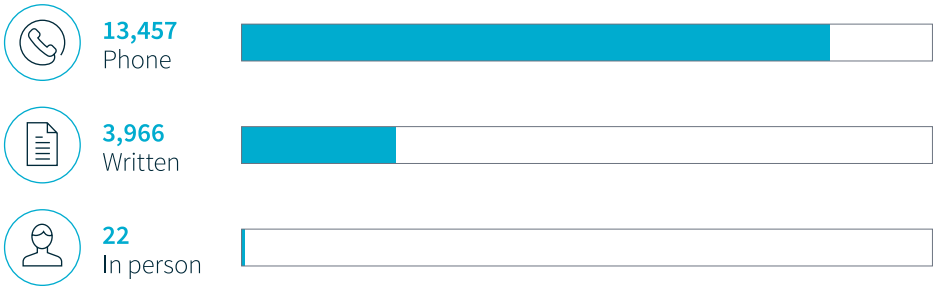
of all privacy complaints were finalised within 12 months of receipt

We handled

17,445
privacy enquiries

2017–18

10%
decrease
from 2017–18



We received

9% more*
notifications under the Notifiable Data Breaches (NDB) scheme

2018–19
950
Total

2017–18
305
Total

79%

of all notifications under the NDB scheme were finalised within 60 days

* Corrected to take account the NDB scheme only commenced on 22 February 2018.

FOI highlights*

We received

928

applications for Information Commissioner reviews of FOI requests

16%

a 16% increase

2018–19	2017–18
928 Total	801 Total

We finalised

73% of applications

for an Information Commissioner review within 12 months of receipt

The top five agencies involved in Information Commissioner reviews were:

1. Department of Home Affairs **(198)**
2. Department of Human Services **(104)**
3. Department of Veterans' Affairs **(47)**
4. Australian Federal Police **(46)**
5. Department of Defence **(44)**

We finalised

8% more

Information Commissioner reviews

2018–19	2017–18
659 finalised	610 finalised

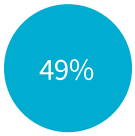
2018–19	2017–18
Average time taken to finalise an Information Commissioner review in 2018–19 was	**Average time taken to finalise an Information Commissioner review in 2017–18 was**
7.8 months	6.7 months

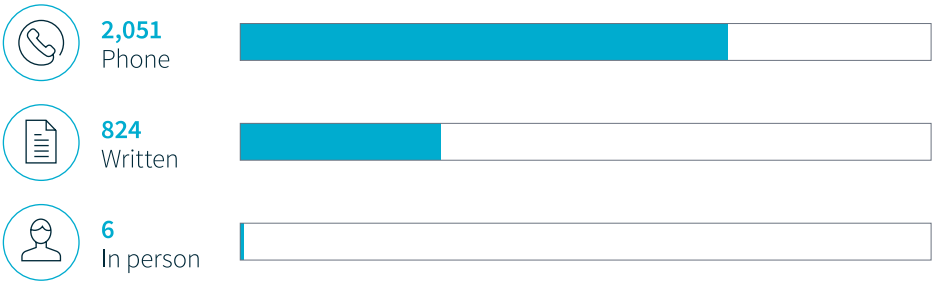
* Percentages have been rounded to the nearest whole number.

We handled

2,881

FOI enquiries which is a 49% increase on 2017–18

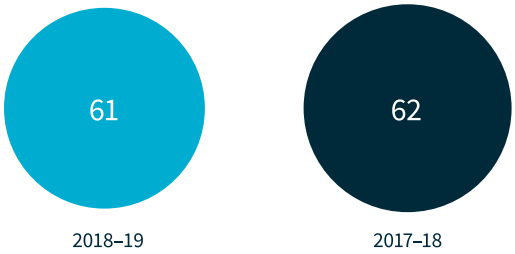


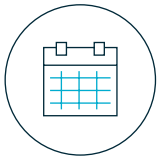


We received

61

FOI complaints which was a similar number to last year

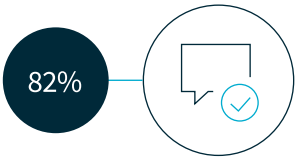




Average time taken to close FOI complaints was

7.2 months

compared to 5.8 months in 2017–18



82%

of FOI complaints were finalised within 12 months of receipt, compared to 83% in 2017–18

Our structure

The OAIC is headed by the Australian Information Commissioner, a statutory officer appointed by the Governor-General. The Commissioner has a range of powers and responsibilities outlined in the AIC Act, and also exercises powers under the FOI Act, the Privacy Act and other privacy-related legislation.

The Australian Information Commissioner is the agency head accountable for strategic oversight and the OAIC's regulatory, strategic, advisory and dispute resolution functions, as well as financial and governance reporting.

Angelene Falk was appointed by the Governor-General to the roles of Australian Information Commissioner and Privacy Commissioner on 16 August 2018.
She was acting Australian Information Commissioner and Privacy Commissioner from 24 March 2018 to 15 August 2018.

Angelene Falk

Angelene Falk has held senior positions in the OAIC since 2012, including serving as Deputy Commissioner from 2016 to March 2018.

Over the past decade, she has worked extensively with Australian Government agencies, across the private sector and internationally, at the forefront of addressing regulatory challenges and opportunities presented by rapidly evolving technology and potential uses of data. Her experience extends across industries and subject matter, including data breach prevention and management, data sharing, credit reporting, digital health and access to information.

She holds a Bachelor of Laws with Honours and a Bachelor of Arts from Monash University and a Diploma in Intellectual Property Law from Melbourne University.

Support to the Commissioner

The Commissioner is supported by an Executive team of three substantive Senior Executive Services (SES) positions, and expert staff, working within the Dispute Resolution, Regulation and Strategy, and Legal and Governance branches.

Generally, the Dispute Resolution branch is responsible for resolving privacy complaints, FOI Information Commissioner reviews, Commissioner initiated privacy and FOI investigations and the OAIC's public information service. The Regulation and Strategy branch provides guidance, examines and drafts submissions on proposed legislation, conducts assessments, and provides advice on inquiries and proposals that may have an impact on privacy. The Legal and Governance branch provides legal and corporate services and strategic communications functions.

Communication and collaboration

We used a range of networks and communication channels during this reporting period to raise awareness across businesses, government agencies and the public about privacy and information access rights and responsibilities.

We have highlighted some of these activities below and give more detail in Part 2.

Our networks

We hosted and participated in a number of domestic and international privacy and information access networks which provided opportunities to collaborate and share expertise with stakeholders.

Privacy Professionals Network

The Privacy Professionals Network (PPN) is for public and private sector privacy professionals. Its membership grew during this reporting period from 3,442 to 3,623 members.

We sent regular updates to PPN members on topics such as: agencies we recently recognised to handle particular privacy-related complaints (an external dispute resolution scheme); our recent submissions about privacy-related matters to the Australian Government or other entities; a new or updated resource on a topic of interest, such as the My Health Record system; and relevant national or international developments.

The majority of PPN events in 2018–19 were fully subscribed and provided PPN members with an opportunity to hear from experts and network with colleagues.

PPN events during this reporting period included:

- a presentation on privacy issues at the GRC Institute in Perth in November 2018
- a Privacy Awareness Week (PAW) business breakfast in Sydney in May 2019, where the Commissioner shared insights from the first 12 months of the NDB scheme
- a Privacy Authorities Australia panel discussion in Brisbane in April 2019, that focused on the challenges each jurisdiction faced and opportunities for cross-border collaboration.

Information Contact Officer Network

Our Information Contact Officer Network (ICON) for Australian Government FOI contact officers was given regular updates on topics such as: recent IC review decisions; a new or update resource on a topic of interest, such as updates to the FOI Guidelines; and relevant national or international developments.

At the end of this reporting period there were 527 ICON members.

We held two ICON information sessions in Canberra during this reporting period to update members on recent FOI activity, decision review trends and our priorities:

- In September 2018, the Commissioner and the Executive team were joined by representatives of the Department of the Prime Minister and Cabinet and the Department of Finance.
- In April 2019, our ICON session featured representatives of the National Archives of Australia and an introduction to the Open Australia Foundation's Right to Know website.

Consumer Privacy Network

The Consumer Privacy Network (CPN) furthers the privacy community's understanding of current privacy issues affecting consumers. Members were appointed for a two-year period:

- Australian Communications Consumer Action Network
- Australian Privacy Foundation
- Consumer Action Law Centre
- Consumer Credit Law Centre South Australia
- Consumers Health Forum of Australia
- Electronic Frontiers Australia Inc
- Financial Rights Legal Centre Inc (NSW)
- Internet Australia

- Legal Aid New South Wales
- Legal Aid Queensland
- The Foundation for Young Australians
- National LGBTI Health Alliance
- Federation of Ethnic Communities' Councils of Australia
- National Mental Health Consumer & Carer Forum.

Domestic networks

Privacy Authorities Australia

Privacy Authorities Australia (PAA) is a group of Australian privacy authorities who meet regularly to promote best practice and consistency of privacy policies and laws. We joined privacy representatives from all states and territories as a member of PAA.

Association of Information and Access Commissioners

This Australian and New Zealand network is for information access authorities who administer FOI legislation. In September 2018, we hosted a meeting of the Association of Information and Access Commissioners (AIAC) members at our office in Sydney.

International networks

Asia Pacific Privacy Authorities forum

The Asia Pacific Privacy Authorities (APPA) forum is the principal forum for privacy authorities in the Asia-Pacific region for exchanging ideas about privacy regulation, emerging technologies, and managing privacy enquiries and complaints.

Common Thread Network

This network brings together data protection and privacy authorities from Commonwealth countries.

Global Privacy Enforcement Network

The Global Privacy Enforcement Network is designed to facilitate cross-border cooperation in enforcing privacy laws.

International Conference of Data Protection and Privacy Commissioners

The largest and longest standing network for data protection and privacy authorities, the International Conference of Data Protection and Privacy Commissioners (ICDPPC) brings together organisations from around the world to provide leadership at international level in data protection and privacy.

The Commissioner was elected to the ICDPPC Executive Committee in October 2018 and is a co-chair of the ICDPPC Digital Citizen and Consumer Working Group.

International Conference of Information Commissioners

The International Conference of Information Commissioners (ICIC) comprises information commissioners and ombudsmen from around the world. The ICIC provides an opportunity for information commissioners, practitioners and advocates to exchange ideas, to identify emerging trends and challenges and to strengthen public access to information.

Events

During this reporting period, our Executive team and senior staff delivered speeches and presentations and took part in panel discussions at 36 external events, including:

- Australian Communications Consumer Action Network ACCANect National Conference, Sydney, September 2018
- Australian Information Security Association Cyber Conference, Melbourne, October 2018
- the keynote address for the International Association of Privacy Professionals Australia and New Zealand Summit, Melbourne, November 2018
- International Institute of Communications Digital Platforms seminar, Sydney, February 2019
- a panel discussion on 'Privacy and openness — is the balance right?' for the Australian Banking Association, Sydney, March 2019
- Australian Government Solicitor FOI and Privacy Forums, Canberra, November 2018 and May 2019
- Australian Insurance Law Association National Conference, Perth, November 2018
- a panel discussion on the 'Increasing importance of the interrelationship between information access and data protection, including open data' at the ICIC, Johannesburg, March 2019

- a panel discussion on 'Privacy — what patient and hospital information can be shared?' at the Australian Private Hospitals Association National Conference, Melbourne, March 2019
- a presentation on 'Trust in the data economy: the role of stakeholders' at the International Seminar on Personal Data, a G20 Summit Side Event, Tokyo, June 2019.

Privacy Awareness Week

Privacy Awareness Week (PAW) is an annual initiative of the APPA forum. It is held every year to promote and raise awareness of privacy issues and the importance of protecting personal information.

In 2019, PAW ran from 12 to 18 May, promoting a range of privacy priorities through the theme 'Don't be in the dark on privacy'. This message was supported by a digital campaign that directed businesses, agencies and consumers to useful resources and the PAW website.

Events included a sold-out business breakfast, attended by approximately 150 representatives from business and government. Members of the Executive team and senior staff also represented the OAIC at events throughout the week, including at the Australian Government Solicitor FOI and Privacy Forum in Canberra, the Deloitte Privacy Index launch in Sydney and an Information Integrity Solutions event in Melbourne.

A record number of organisations signed up as official supporters of PAW (500, up from 360 in 2017–18) and promoted the importance of good privacy practice to their stakeholders, customers and staff. PAW supporters were given a wide range of resources to share through internal and external communication channels, including posters, social media posts and digital assets; as well as the presentation's slides which included useful information for agencies on the Australian Government Agencies Privacy Code and the NDB scheme.

We also launched a new online game, Privacy Challenge, for PAW 2019 to raise public awareness of how to protect personal information in the digital and real-world environment. The Privacy Challenge features three different scenarios that explore a range of situations including smart phone security, social media privacy, credit reports and scams. The scenarios in this community e-learning resource were launched 2,678 times between 17 May to 30 June 2019.

Our ability to prevent, detect, deter and remedy relies on cooperation and collaboration, across regulatory regimes, across borders, with the community, business, government and academics.

This is central to our approach to regulating in the global economy: developing regulatory policy and guidance that takes account of global developments, creating interoperable regulatory frameworks, and cooperative international regulatory action.

Angelene Falk, Australian Information Commissioner and Privacy Commissioner, keynote address to the PAW Business Breakfast, 'Making privacy the priority: privacy and data protection in our interconnected world', 13 May 2019.

Paw snapshot

16,045
PAW website views

500
PAW supporters

865
PAW posts on social media

Right to Know Day

Our Right to Know Day campaign aimed to raise awareness about the public's right to access government-held information through a dedicated website, digital promotion and events in the lead up to international Right to Know Day on 28 September 2018.

The Right to Know website hosted a new series of FOI videos, event listings, resources and promotional materials. Our events to mark Right to Know Day included an ICON information session in Canberra on the role of the FOI practitioner in promoting accountability and transparency and a community event in Sydney on 27 September 2018 where our staff engaged with more than 500 people about access to information issues.

We also hosted a meeting of the AIAC from 20 to 21 September 2018, where members collaborated on a joint statement to promote Right to Know Day and the importance of open government.

Media and social media

Media interest in our work remained strong throughout 2018–19, reflecting continued community awareness of privacy and information access rights. Media coverage of personal information security issues was also driven by mandatory notifications of data breaches to affected individuals and the OAIC, and our regular statistical reports on the NDB scheme.

We responded to 238 media enquiries in 2018–19 (compared to 317 in 2017–18) from a range of mainstream, business and digital publications.

We actively promoted awareness of privacy and information access rights through the social media channels, increasing followers and page likes across Facebook and Twitter. We also regularly shared privacy and information access updates through our e-newsletter, which was relaunched in May 2019 as 'Information Matters' to a combined subscriber base of almost 7,800 people.

Facebook

Almost 60,000 people actively engaged with our campaign posts to promote awareness of privacy controls within the My Health Record system.

Page likes grew by almost 10% to 2886.

Twitter

More than 913,000 tweet impressions.

Followers grew by almost 10% to more than 5,200.

Webinars and podcasts

We partnered with the Royal Australian College of General Practitioners (RACGP) to present three webinars on the NDB scheme in February 2019, which attracted 222 attendees and 145 downloads. The webinars were part of a broader communications campaign with the RACGP to promote good privacy and personal information handling practices to their members.

For PAW 2019, we partnered with Wolters Kluwer to present a webinar on the NDB scheme that highlighted the findings and recommendations from our *Notifiable Data Breaches Scheme 12-Month Insights Report*. The webinar attracted almost 400 registrations, and 95% of attendees rated the session as 'excellent' or 'very good'.

> *This webinar has filled some gaps and clarified the major grey areas. The questions session gave a great opportunity to clarify any uncertainty. I am more confident in my knowledge now.*
>
> PAW webinar attendee

We also collaborated with Legal Aid NSW to create a podcast on consumer credit reporting issues for PAW, which has since been downloaded more than 250 times.

Part 2
Performance

Our annual performance statement

Introduction

I, Angelene Falk, as the accountable authority of the Office of the Australian Information Commissioner (OAIC), presents the 2018–19 annual performance statement of the OAIC, as required under paragraph 39(1)(a) of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). In my opinion, this annual performance statement is based on properly maintained records, accurately reflects the performance of the entity, and complies with subsection 39(2) of the PGPA Act.

Overall performance

During this reporting period, we worked to achieve 43 performance measures outlined in the *OAIC Corporate Plan 2018–19*. We met the target for 38 of these performance measures and we did not achieve four (one measure did not apply during this reporting period).

We:

- promoted and upheld privacy rights by achieving 30 of the 32 performance measures
- promoted and upheld information access rights by achieving 8 of the 11 performance measures (one measure did not apply during this reporting period).

Promote and uphold privacy rights

We:

- negotiated and accepted enforceable undertakings from the Commonwealth Bank of Australia Ltd and Wilson Asset Management (International) Pty Ltd
- conducted targeted privacy assessments in areas such as finance, telecommunications, government, data matching and digital health
- finalised 2,919 privacy complaints, a 5.5% increase on the number of privacy complaints we closed last financial year, while managing a 12.1% increase in privacy complaints received
- published quarterly reports on the operation of the Notifiable Data Breach (NDB) scheme and the *Notifiable Data Breaches Scheme 12-Month Insights Report*
- finalised 79% of notifications received for 950 notifiable data breaches (under the NDB scheme) within 60 days, finalised 66.1% of voluntary notifications for 175 data breaches within 60 days and finalised 90% of notifications received for My Health Record data breaches within 60 days
- made two public interest determinations on the disclosure of homicide data for the Australian Federal Police and the Australian honours system for the Department of Home Affairs
- released a new training resource about the *Privacy (Australian Government Agencies — Governance) APP Code 2017* (Privacy Code) and the Notifiable Data Breaches (NDB) scheme
- launched new resources for My Health Record consumers
- launched our new website for public feedback.

Promote and uphold information access rights

We:

- finalised 659 Information Commissioner (IC) reviews, an 8% increase on the number of IC reviews we closed last financial year, while managing a 15.9% increase in IC review applications
- published the Information Publication Scheme (IPS) Survey 2018
- published a revised guide for Access to Government Information — Administrative Access
- launched a digital campaign for Right to Know Day 2018.

Results

Our performance is measured against the activities in the *OAIC Corporate Plan 2018–19*. Where a performance measure covers a target in the Portfolio Budget Statement, an asterisk (*) is shown against the performance measure.

Privacy performance measures

Corporate Plan activity 1.1

Develop the privacy management capabilities of businesses and Australian Government agencies and promote privacy best practice.

Performance measure 1.1.1 The OAIC applies a risk-based, proportionate approach to facilitate privacy compliance and promote privacy best practice.

✓ Achieved

During this reporting period, we engaged with entities reporting under the NDB scheme on requirements of the NDB scheme, causes of the data breach and measures to prevent reoccurrence. We used intelligence from privacy enquiries, privacy complaints and NDB reports, privacy assessments, media reports and tip-offs, to decide on appropriate regulatory action. We conducted preliminary inquiries or opened investigations on the Commissioner's own initiative for 15 matters.

We regularly engaged with business and Australian Government agencies, including providing advice and guidance on how to comply with the *Privacy Act 1988* (Privacy Act) and deliver privacy best practice.

We released a new training resource about the Privacy Code and NDB scheme during Privacy Awareness Week (12 to 18 May 2019) to educate Australian Government agencies about privacy best practice.

We published the *Notifiable Data Breaches Scheme 12-Month Insights Report*, which is available on our website, to help businesses and agencies understand the common causes of data breaches and how they can implement proactive strategies to prevent data breaches.

We launched new resources for My Health Record consumers.

Performance measure 1.1.2 Guidance and educational materials are updated to include learnings from regulatory activities such as assessments and investigations.

Achieved

We regularly updated our guidance and educational materials to make sure they are current and relevant.

For example, we released a new website for public review in June 2019 (see performance measure 1.7.4). During Privacy Awareness Week (PAW) we provided guidance to organisations and Australian Government agencies about their obligations under the Privacy Code.

Performance measure 1.1.3 Regular engagement and consultation with businesses and Australian Government agencies is undertaken.

Achieved

We engaged regularly with businesses and Australian Government agencies, including providing advice on a wide range of matters such as the Australian Competition and Consumer Competition's (ACCC) Digital Platforms Inquiry, the Consumer Data Right scheme, changes to the My Health Record system and the *Privacy (Credit Reporting) Code 2014*.

We drafted submissions on nine different issues, such as cooperative intelligent transport systems, automated vehicle data, Australian Government data sharing and telecommunications.

Performance measure 1.1.4 Privacy Professionals' Network (PPN) members are provided with information that is relevant and engaging, a minimum of 10 times per year.

Achieved

We continued to offer PPN members regular information and updates. In 2018–19, PPN members received 10 e-newsletters. We also invited them to events which included discussion panels and OAIC privacy training.

Performance measure 1.1.5 Levels of engagement with PPN members are recorded.

Achieved

We had our highest number of organisations supporting our PAW campaign with 507 becoming PAW partners, up from 360 in 2017–18.

During this reporting period, the PPN membership continued to grow from 3,442 members to 3,623. More than half PPN members (51%) opened our e-newsletter and 39% clicked on a specific link in the e-newsletter.

Corporate Plan activity 1.2

Manage data breach notifications.

Performance measure 1.2.1* 80% of data breach notifications are finalised within 60 days.

Not achieved

We:

- finalised 79% of notifications received under the NDB scheme within 60 days
- finalised notifications received under the NDB scheme in an average of 45.3 days
- finalised 66.1% of voluntary data breach notifications received within 60 days
- finalised voluntary data breach notifications in an average of 60.4 days.

Performance measure 1.2.2* 80% of My Health Records data breach notifications are finalised within 60 days.

Achieved

We finalised 90% of My Health Record data breach notifications received within 60 days.

Performance measure 1.2.3 Guidance and support tools are promoted for the data breach notification schemes the OAIC oversees.

Achieved

We published a resource for regulated entities on tips to prevent and mitigate data breaches with the Australian Cyber Security Centre.

We recorded and published:

- an interactive webinar with the Royal Australian College of General Practitioners (RACGP) on the requirements of the NDB scheme for health service providers, with case studies and frequently asked questions
- resources and information for RACGP members including updated flowcharts on the NDB scheme and My Health Record data breaches
- an interactive webinar on the requirements of the NDB scheme, and the lessons from the first 12 months of the NDB scheme's operation, with case studies on best practice and approaches to multi-party data breaches.

Performance measure 1.2.4 Statistics on data breach notifications are published.

Achieved

We published four quarterly reports on the operation of the NDB scheme. These reports included key statistics on the number of notifications received, the number of individuals whose personal information was involved in the data breach, detailed breakdowns on the reported sources of data breaches, comparisons of data breaches reported by the top five sectors and the kinds of personal information affected. They also provided detailed breakdowns of the types of data breaches notified by the top two reporting sectors.

In May 2019, we published the *Notifiable Data Breaches Scheme 12-Month Insights Report*, which is available on our website. The report provided lessons learned from the first year of the NDB scheme's operation, as well as information about the changing international landscape with regards to privacy and mandatory data breach reporting schemes. The report also highlighted best practice tips and case studies from organisations that had notified under the NDB scheme, and strategies for mitigating the risk of cyber incidents.

Corporate Plan activity 1.3

Conduct Commissioner initiated investigations (CIIs).

Performance measure 1.3.1* 80% of CIIs are finalised within eight months.

Achieved

Of the privacy CIIs finalised during this reporting period, 86% were finalised within eight months.

This reflected our commitment to working with respondents to resolve issues of non-compliance and improve privacy practices, as well as our efforts to reduce the time taken to progress a privacy CII.

For more information about CIIs, see page 65.

Performance measure 1.3.2 CIIs result in improvements in the privacy practices of investigated organisations.

Achieved

We made inquiries of, or investigated, organisations to ensure compliance with the Privacy Act. We accepted enforceable undertakings from two respondents in 2018–19: the Commonwealth Bank of Australia Ltd and Wilson Asset Management (International) Pty Ltd.

Each enforceable undertaking included steps the respondent agreed to take to address concerns we raised in the CII. By implementing these steps, the respondents will improve their privacy policies and procedures.

Performance measure 1.3.3 CII outcomes and lessons learnt are publicly communicated.

Achieved

We:

- published the enforceable undertakings accepted from the Commonwealth Bank of Australia Ltd and Wilson Asset Management (International) Pty Ltd on our website
- published statements and media releases on our website about the conclusion of these matters and the lessons learnt
- publicly communicated the lessons learnt from CIIs in external speeches and presentations given by OAIC staff.

Performance measure 1.3.4 The OAIC applies a risk-based and proportionate approach to commencing and conducting CIIs.

Achieved

We applied the framework set out in the Guide to Privacy Regulatory Action (which is available on our website) when deciding whether to commence an investigation. As a result we commenced investigations into 15 matters.

Corporate Plan activity 1.4

Resolve privacy complaints.

Performance measure 1.4.1* 80% of privacy complaints are finalised within 12 months.

Achieved

We:

- finalised 95.1% of all privacy complaints within 12 months of receipt — 4.4 months was the average time taken to close a privacy complaint
- closed 5.5% more privacy complaints than in 2017–18
- responded to an 11% increase in privacy complaints in the number of privacy complaints received (2017–18: 18% increase)
- increased staffing levels in our Early Resolution team to continue the efficient processing of privacy complaints.

We ensured the quality of our privacy complaint process by:

- handling privacy complaints in line with our privacy regulatory action policy and privacy regulatory action guide
- undertaking regular staff training, including conciliation and investigations training, administrative law training and mental health training
- enabling staff to participate in complaint handling networks and events, including the Commonwealth Ombudsman's Complaint Handling Forum and PAW activities
- holding regular staff meetings to discuss matters of significance across the teams and to ensure consistency in decision-making — for example, all the Dispute Resolution branch staff regularly met to discuss privacy cases

For more information on resolving privacy complaints, see page 57.

Performance measure 1.4.2 The complaint handling service is promoted to the community.

✓ Achieved

We promoted our complaints handling service to the community through media releases, speaking engagements, event campaigns and social media.

We promoted the OAIC's regulatory function and complaint handling service as part of our My Health Record privacy controls campaign on Facebook and Twitter.

We also promoted our complaint handling service through our campaigns for Privacy Awareness Week and Right to Know Day.

Performance measure 1.4.3 Complaint handling processes are reviewed to ensure they align with current best practice and relevant legislative developments.

✓ Achieved

We reviewed our internal processes and developed a policy for responding to unreasonable client conduct. When finalised, this policy will always ensure best practice when handling unreasonable clients and support staff to manage challenging interactions.

We hired an external consultant to help us improve the timeliness of our privacy complaint process. We are currently developing strategies to reduce a backlog of privacy complaints.

Corporate Plan activity 1.5

Conduct privacy assessments.

Performance measure 1.5.1 Complete assessments in accordance with the schedule developed in consultation with the business or agency being assessed.

✗ Not achieved

We generally completed the information review and fieldwork stages of privacy assessments in line with a schedule we developed with the business or agency being assessed; however, the assessment report was not finalised on schedule in all cases. We will continue to improve our assessment reporting process in the next financial year and work with the business or agency being assessed to finalise draft assessment reports promptly.

Performance measure 1.5.2 Monitoring and compliance approaches are coordinated with the business and operational needs of the business or agency being assessed.

✓ Achieved

We undertook professional, independent and systematic assessments in line with our privacy regulatory action policy and our guide to privacy regulatory action.

We engaged with and provided preliminary briefings to the business or agency being assessed prior to starting the formal assessment. This clarified our expectations and allowed us to develop a schedule that recognised the operational needs of the business or agency being assessed.

We engaged ICT security consultants to assist with the technical aspects of some of our Australian Privacy Principle 11 (security of personal information) assessments. For example, we engaged these consultants to support a series of assessments that considered how particular telecommunications service providers were protecting personal information.

Performance measure 1.5.3 A high proportion of recommendations are accepted by the business or agency being assessed.

✓ Achieved

All businesses or agencies assessed accepted all our recommendations.

During an assessment, we proactively and openly raised privacy risks we identified and our recommendations to the business or agency being assessed. This promoted discussions with the business or agency about strategies to mitigate the privacy risks.

Performance measure 1.5.4 Key assessment outcomes and lessons learnt are publicly communicated where appropriate.

✓ Achieved

We undertook assessments in the form of surveys with a number of businesses or agencies in a particular sector. We provided those businesses or agencies with individual reports and intend to publish a summary report on our website in 2019–20. This will provide general guidance to APP entities, while also providing tailored advice to the entities assessed.

Corporate Plan activity 1.6

Provide a privacy public information service.

Performance measure 1.6.1* 90% of written enquiries are responded to within 10 working days.

✓ Achieved

We finalised 92% of written privacy enquiries within 10 working days. This is a significant improvement on our 2017–18 response rate of 74%. This improvement reflects a reallocation of resources and changes to the management of the OAIC's enquiries service, which were put in place in 2017–18, and our ongoing commitment to provide a timely public information service to the Australian public. For more information, see Privacy Enquiries on page 50.

Performance measure 1.6.2 Community, legal and other networks are identified for targeted promotion of the public information service.

✓ Achieved

We partnered with Legal Aid NSW during PAW (12 to 18 May 2019) to produce a podcast interview about credit reporting. By discussing a series of examples, we helped community workers and the public understand the circumstances in which they can gain access to their credit reports for free, how they may correct the information on their credit reports, and their rights to pursue complaints about their credit reports with recognised external dispute resolution schemes and the OAIC.

The Commissioner presented information about the OAIC and our functions to the Communications and Media Law Association and the annual conference of communications consumer representatives.

We also worked closely with the RACGP to increase member awareness of our regulatory role, including providing information about our public information service.

Performance measure 1.6.3 Website content is reviewed and updated as required to support our public information service.

✓ Achieved

We released a new website for public feedback in June 2019 (see performance measure 1.7.4).

Corporate Plan activity 1.7

Promote awareness and understanding of privacy rights in the community.

Performance measure 1.7.1 Media and social media mentions about privacy rights increase.

✓ Achieved

There were 2,805 online media mentions and 6,770 social media mentions of privacy rights and the OAIC during this reporting period (2017–18: 2,851 online media mentions and 4,400 social media mentions).

We responded to 238 media enquiries during the year, including 194 about privacy and 25 about My Health Record.

Performance measure 1.7.2 Awareness and understanding about privacy rights and the role of the OAIC improves.

✓ Achieved

The consistent number of online media mentions and increasing number of social media mentions demonstrate continued and growing awareness of our privacy role. Our social media following has also increased.

The increase in privacy complaints also demonstrates increased awareness of the OAIC's complaint handling service.

Performance measure 1.7.3 Attendance numbers and positive feedback from public facing events increases.

✓ Achieved

We successfully hosted a breakfast event for PAW, attended by 160 privacy professionals and other stakeholders. The event sold out, and 95% of attendees surveyed indicated they would attend the PAW business breakfast again next year.

A joint webinar with Wolters Kluwer on the NDB scheme had more than 200 participants and 95% rated the webinar as 'excellent' or 'very good'.

The OAIC also ran a number of privacy training sessions for Australian Government privacy officers, with each session booked to capacity.

Performance measure 1.7.4 The OAIC's website is accessible to the community and content about privacy rights is regularly reviewed and updated.

✓ Achieved

We released our new website for public feedback in June 2019. The website features improvements such as:

- better search functionality, design and navigation in response to user feedback
- information in one location — information that was once repeated or found over several pages is now on a single page
- removing non-current information so the search function works more effectively
- removing the print-based concept of 'fact sheets' and 'resources' and consolidating content into topics
- content for individuals rewritten in plain English.

Corporate Plan activity 1.8

Develop legislative instruments.

Performance measure 1.8.1 Applications for public interest determinations and Australian Privacy Principles (APP) codes are considered and responded to in a timely manner.

✓ Achieved

We did not receive any APP code applications during 2018–19.

We received three applications for a public interest determination:

- Privacy (Disclosure of Homicide Data) Public Interest Determination 2019 — commenced 20 March 2019 — permits the Australian Federal Police to disclose certain personal information to the Australian Institute of Criminology for the purpose of the Australian Institute of Criminology's research under the National Homicide Monitoring Program and the publication of aggregate findings.
- Privacy (Australian Honours System) Public Interest Determination 2018 — commenced 12 October 2018 — permits the Department of Home Affairs to disclose personal information to the Office of the Official Secretary to the Governor-General and the Department of the Prime Minister and Cabinet for verifying the Australian citizenship and/or permanent residency status of individuals who are the subject of nominations for membership or honorary membership of the Order of Australia, or for other awards in the Australian honours system.

- Australian Financial Complaints Authority (AFCA) — received 17 June 2019 — requested a public interest determination to be made by the Commissioner deeming AFCA an 'agency' for the sole purpose of interpreting APP 12. APP 12 provides that if an entity is an agency, the entity is not required to give access to personal information if the entity is required or authorised to refuse an individual access to personal information under the *Freedom of Information Act 1982* (FOI Act) or any other federal Act. We are currently considering this application.

Performance measure 1.8.2 Legislative instruments are reviewed when necessary.

✓ Achieved

The acting Australian Information Commissioner and acting Privacy Commissioner approved a variation of the *Privacy (Credit Reporting) Code 2014* (v2) (CR Code) on 29 May 2018, following an application by the code developer, the Australian Retail Credit Association. The variation addressed some of the recommendations and feedback in the independent review of the CR Code undertaken in 2017. The varied CR Code commenced on 1 July 2018.

On 18 April 2019, the Australian Retail Credit Association made a second application to vary the CR Code under section 26T of the Privacy Act. This variation addresses the remainder of the recommendations and feedback in the independent review of the CR Code undertaken in 2017. This application is currently under consideration.

Corporate Plan activity 1.9

Conduct regulatory activities and help businesses understand their rights and responsibilities under the Consumer Data Right (CDR).

Performance measure 1.9.1 Regular dialogue with the ACCC and other relevant stakeholders is conducted to ensure the effective operation of the CDR scheme.

✓ Achieved

We engaged regularly with the ACCC and the Treasury, including through the provision of advice on draft legislative instruments and draft CDR rules, as well as guidance on general privacy matters affecting the CDR scheme.

We also engaged regularly with the Data Standards Body (CSIRO's Data61), including through the provision of advice on development work for the technical standards relating to consumer experience and attended as observers Data Standards Advisory Committee meetings.

Performance measure 1.9.2 Guidance and education materials are developed to support a clear understanding of rights and obligations under the CDR scheme.

Achieved

Since the publication of the *OAIC Corporate Plan 2018–19* the commencement date of the CDR scheme in the banking sector has moved from July 2019 to 1 February 2020.

Development of guidance and education materials is underway, including guidelines for the avoidance of acts or practices that may breach the privacy safeguards.

Performance measure 1.9.3 Internal processes and protocols are developed to support the implementation of the CDR.

Achieved

We created internal governance mechanisms to support the implementation of the CDR including developing project plans and reporting tools and establishing a CDR Project Governance Board.

We have reviewed existing processes and have begun developing new processes to support an efficient and effective CDR complaint handling process.

We have also started preparing internal training and other resources to ensure our Enquiries team are well equipped to answer questions from the public regarding the CDR.

Freedom of information performance measures

Corporate Plan activity 2.1

Develop the freedom of information (FOI) capabilities of Australian Government agencies and ministers, and promote FOI best practice.

Performance measure 2.1.1 Tools and guidance are updated to assist Australian Government agencies to comply with the Information Publication Scheme (IPS).

✗ Not achieved

In June 2019 we published the *Information Publication Scheme Survey 2018*, a survey of all Australian Government agencies subject to the FOI Act. The survey reviewed the operation of the IPS and gave agencies an opportunity to comply with the requirement to conduct a review under s 9 of the FOI Act.

In 2019–20, we will develop tools and guidance, including updating the Part 13 of the FOI Guidelines, to address issues identified in the IPS survey to help agencies better comply with their IPS obligations.

Performance measure 2.1.2 Guidance and resources are reviewed and updated to assist Australian Government agencies and ministers to apply the FOI Act.

✓ Achieved

We consulted Australian Government agencies on a revised Part 4 (Charges) of the FOI Guidelines. We will issue the final version in 2019–20.

In September 2018, we published the revised 'Agency Resource 14 — Access to Government Information — Administrative Access'.

In preparation for the release of our new website, all FOI resources were reviewed, and updated, where necessary, for migration to the new website.

Performance measure 2.1.3 Information is provided to stakeholders that is relevant in both content and delivery.

✓ Achieved

In 2018–19, we met with many Australian Government agencies to discuss issues affecting FOI.

Our Information Contact Officers Network (ICON) comprising 527 at 30 June 2019, received 13 newsletters and updates updates with information about FOI. The average click-through rate for the ICON newsletter was 28%.

We also emailed a monthly newsletter to subscribers of OAICnet (known as Information Matters since May 2019). This newsletter contained news and updates about the OAIC, FOI and privacy matters and information on upcoming events.

In September 2018 and April 2019 we held ICON information sessions in Canberra to update members on recent FOI activity, trends and the OAIC's priorities. Agencies who attended the information sessions gave positive feedback on the delivery of the session and the content.

The Information Commissioner addressed access to information issues in several speeches and presentations throughout the year, including the International Conference of Information Commissioners in South Africa in March and the Australian Government Solicitor FOI and Privacy Forum in May 2019.

Corporate Plan activity 2.2

Conduct Information Commissioner reviews.

Performance measure 2.2.1* 80% of Information Commissioner (IC) reviews are completed within 12 months.

⊗ Not achieved

We completed 73.1% of IC reviews within 12 months.

The significant increase in IC review applications we received and our focus on reducing the number of cases over 12 months old prevented us from reaching our target of completing 80% within 12 months.

We used alternative dispute resolution methods and early appraisal to clarify at an early stage the issues to be resolved or the information to be provided by either party in support of their claims or submissions. This includes reviewing the material submitted by both parties and providing a preliminary view on the merits of the case to the relevant party. The party may then make further submissions or take other action as appropriate (an applicant withdrawing application or the agency revising the decision).

We facilitated the early resolution of IC reviews by helping the parties to reach an agreement about the outcome of the review in line with s 55F of the FOI Act, including by arranging teleconferences between parties where appropriate.

We used our regulatory powers under the FOI Act to ensure efficient and timely processes, including by issuing notices to agencies under ss 55E (to provide an adequate statement of reasons) and 55R (notice to produce information or documents).

The Information Commissioner made 60 IC review decisions under s 55K of the FOI Act (which are published on AustLII). These decisions help agencies interpret the FOI Act and provide guidance on the exercise of their powers and functions, by addressing novel issues and building on existing jurisprudence.

We developed the capacity of our staff to identify matters that can be resolved quickly and informally through early resolution processes, whether it be through agreement or negotiation, case appraisals or preliminary views, as well as identifying significant matters which should proceed to a s 55K decision by the Commissioner.

Corporate Plan activity 2.3

Investigate FOI complaints and conduct Commissioner initiated investigations (CIIs).

Performance measure 2.3.1* 80% of FOI complaints finalised within 12 months.

✓ Achieved

We finalised 82% of FOI complaints within 12 months of receipt during this reporting period.

We identified at an early stage whether a complaint or an IC review is the appropriate mechanism. We also used early appraisal to clarify the issues to be resolved or the information to be provided by either party in support of their claims or submissions in relation to the complaint.

Performance measure 2.3.2* 80% of FOI-related CIIs finalised within eight months.

— Not applicable

Only one FOI-related CII was opened in 2018–19 and the eight-month period had not elapsed by 30 June 2019.

Corporate Plan activity 2.4

Provide an FOI public information service.

Performance measure 2.4.1* 90% of FOI written enquiries are finalised within 10 working days.

✓ Achieved

We finalised 94% of all FOI written enquiries within 10 working days in 2018–19.

This is an improvement in response times from 2016–17 and 2017–18, when 88% of all written enquiries were finalised within 10 working days. During this reporting period, the FOI team focused on improving the processes for responding to FOI enquiries. As a result, the timeliness of the FOI team's response to FOI enquiries has improved.

Performance measure 2.4.2 New community, legal and other networks are identified for targeted promotion of the public information service.

✓ Achieved

Some of our staff attended the National Association of Community Legal Centres conference in Sydney in August 2018 and promoted information access rights to staff from community legal centres from across Australia.

We held two ICON information sessions in Canberra — one in September 2018 and the other in April 2019.

Information access issues, recent decisions and resource updates were highlighted for agency staff and members of the public throughout the year in regular OAICnet (from May 2019 called 'Information Matters') and ICON email newsletters.

The Information Commissioner made the keynote address at the Australian Government Solicitor's FOI and Privacy Forum in Canberra on 17 May 2019. During this reporting period, members of the FOI team also participated in FOI practitioner forums that the Australian Government Solicitor hosted.

To celebrate Right to Know Day on 28 September 2018, we launched our first Right to Know Day digital campaign, which included three short videos.

Staff also celebrated Right to Know Day with an information booth during the morning transport peak period in Wynyard Park, Sydney, a major public transport hub area.

Performance measure 2.4.3 Website content is regularly reviewed and updated to support our public information service.

Achieved

We released a new website for public review in June 2019 (see performance measure 1.7.4).

Corporate Plan activity 2.5

Promote awareness and understanding of information access rights in the community.

Performance measure 2.5.1 Media and social media mentions about information access rights increase.

Achieved

During this reporting period there were 334 online media mentions (2017–18; 345) and 556 social media mentions of information access rights and the OAIC (2017–18; 428), resulting in a total of 890 mentions (2017–18: 773).

The work that we did to achieve these mentions included:

- conducting a campaign for Right to Know Day 2018, which included relaunching the Right to Know website
- creating three videos for Right to Know Day, two for the public and one for Australian Government FOI contact officers
- using Twitter to highlight Information Awareness Month (May 2019)
- responding to 13 media inquiries about FOI issues
- increasing our international engagement
- participating in the Association of Information Access Commissioners (AIAC).

Performance measure 2.5.2 The OAIC's website is accessible to the community and content about information access rights is regularly reviewed and updated.

Achieved

We released a new website for public review in June 2019 (see performance measure 1.7.4).

Privacy

The Privacy Act requires Australian Government agencies and private sector organisations covered by the Privacy Act to follow a set of rules when collecting, using and storing an individual's personal information. 'Personal information' is any information that is about an individual. The most obvious example is an individual's name — other examples include their address, their date of birth, a photo of their face, or a record of their opinion and views. Any information that is about an identifiable individual is personal information.

Australian Privacy Principles

The Privacy Act includes 13 Australian Privacy Principles (APPs), which set out standards for business and government agencies managing personal information.

APP 1 — Open and Transparent Management of Personal Information

APP 2 — Anonymity and Pseudonymity

APP 3 — Collection of Solicited Personal Information

APP 4 — Dealing with Unsolicited Personal Information

APP 5 — Notification of the Collection of Personal Information

APP 6 — Use or Disclosure of Personal Information

APP 7 — Direct Marketing

APP 8 — Cross-Border Disclosure of Personal Information

APP 9 — Adoption, Use or Disclosure of Government Related Identifiers

APP 10 — Quality of Personal Information

APP 11 — Security of Personal Information

APP 12 — Access to Personal Information

APP 13 — Correction of Personal Information

Privacy enquiries

The OAIC offers a free public information service on privacy-related matters. Our service is mainly delivered through handling phone and written enquiries.

During this reporting period, we experienced a 10% decrease in privacy enquiries from 2017–18, consistent across both phone and written enquiries. We answered 13,457 phone enquiries about privacy matters and responded to 3,966 written privacy enquiries. We also helped with 22 in-person privacy enquiries.

We significantly improved our response time for written privacy enquiries. During this reporting period, we responded to 92% of written privacy enquiries within 10 working days, up from 74% in 2017–18.

We continued to receive a broad range of enquiries from the community. More than 60% of all phone enquiries about privacy matters concerned the operation of the APPs. We also continued to receive a significant proportion of enquiries about credit reporting and the new NDB scheme.

As a part of our Memorandum of Understanding (MOU) with the Australian Capital Territory (ACT) Government we continued to provide privacy services to ACT public sector agencies, including responding to enquiries from the public about the *Information Privacy Act 2014* (ACT) (Information Privacy Act) and its Territory Privacy Principles (TPPs).

Examples of privacy enquiries handled during this reporting period are described in Case Studies 2.1 and 2.2.

Case Study 2.1: A business owner responds to a data breach

A business owner contacted the OAIC after discovering a staff member had stolen the credit card details of some clients and used this information to run up a bill of more than $10,000. The business owner had reported the matter to the police but was seeking advice about their obligations under the Privacy Act.

One of our enquiries officers discussed with the business owner the nature of their business and discovered that the business was a private health service provider. As a private health service provider, the business, even though a small business, must follow the APPs.

The enquiries officer gave the business owner information on APP 11 Security of Personal Information and advised that the data breach may be notifiable under the NDB scheme. They also referred the business owner to our website for guidance on the NDB scheme, which may help the business to assess the data breach and mitigate the risk to the individuals whose personal information was involved.

Case Study 2.2: An individual seeks access to his personal information

An individual involved with an organisation became aware a complaint had been made about him to the organisation. The individual contacted us to ask if he could put in a FOI request to the organisation to find out who had submitted the complaint and what it was about.

One of our enquiries officers explained to the individual that the Commonwealth FOI legislation applied to Australian Government agencies not private organisations; however, under APP 12 — Access to Personal Information, he had the right to access the personal information that the organisation held about him.

The enquiries officer also advised the individual that while he could put in a request to the organisation for access to his personal information under APP 12 the organisation would need to consider whether giving access may have an unreasonable impact on the privacy of the individual who made the complaint and so he may not be entitled to any information about that individual, such as their name.

Issues raised in privacy enquiries

During this reporting period the most common privacy enquiries we received were about the use and disclosure of personal information (APP 6), followed by access to an individual's own personal information (APP 12) and then various exceptions to the APPs (see Table 2.1).

Table 2.1: Phone enquiries related to the APPs*

Issue raised in phone enquiry	Number
APP 1 — Open and Transparent Management of Personal Information	84
APP 2 — Anonymity and Pseudonymity	9
APP 3 — Collection of Solicited Personal Information	938
APP 4 — Unsolicited Personal Information	16
APP 5 — Notification of the Collection of Personal Information	593
APP 6 — Use or Disclosure of Personal Information	1,461
APP 7 — Direct Marketing	154
APP 8 — Cross-Border Disclosure of Personal Information	70
APP 9 — Adoption, Use or Disclosure of Government Related Identifiers	8
APP 10 — Quality of Personal Information	85
APP 11 — Security of Personal Information	1,077
APP 12 — Access to Personal Information	1,390
APP 13 — Correction of Personal Information	110
Exceptions	1,176
General enquiries	1,284

* There may be more than one issue handled in an enquiry.

We also handled questions about other privacy issues, reflecting the broad range of matters the OAIC regulates. Table 2.2 categorises these enquiries.

Table 2.2: Phone enquiries on other privacy matters*

Issue raised in phone enquiry	Number
Credit reporting	688
Notifiable Data Breaches scheme	640
Spent convictions	105
My Health Record	103
Data breach notification (voluntary)	70
Tax file numbers	39
Territory Privacy Principles (ACT)	31
Privacy codes	9
Healthcare identifier	9
Data matching	6
National Privacy Principles	3
Consumer Data Right or open banking	2
Student identifiers	1

* There may be more than one issue handled in an enquiry.

Privacy complaints

During this reporting period we continued to provide an effective complaints service — conciliating, investigating and resolving complaints individuals made to the OAIC about the possible mishandling of their personal information.

We can consider complaints by individuals about alleged interference with their privacy under the APPs, any registered APP code and consumer credit reporting. We can also consider complaints about the handling of other information such as: tax file numbers; spent convictions; data matching; healthcare identification information, including My Health Record.

In 2018–19, we received 3,306 privacy complaints (see Figure 2.1). This is a 12.1% increase on the number of privacy complaints we received in 2017–18 and follows the recent trend (2017–18: 18% increase; 2016–17: 17% increase). Consumers are increasingly aware of their privacy rights, including their right to make a complaint to the OAIC, which has contributed to the overall significant upward trend in number of complaints we have received since 2015–16.

The start of the NDB scheme and the European Union's General Data Protection Regulation in 2018 helped to focus attention on privacy. This focus was maintained during this reporting period with the transition of the My Health Record system to an opt-out system, the ACCC's inquiry into digital platforms, and several high-profile data breaches. The national and international focus on privacy has contributed to improved awareness about obligations to protect personal information under the Privacy Act and added to the substance and complexity of many matters brought to us to investigate.

While managing this significant increase in privacy complaint numbers, we finalised 2,920 complaints in 2018–19 (see Figure 2.2). This is a 5.6% increase on the number of complaints we closed last financial year and follows substantial increases in the previous two financial years as a result of making our processes more efficient and applying our resources more effectively (2017–18: 11% increase; 2016–17: 22% increase).

Figure 2.1: Privacy complaints received each month during the last three financial years

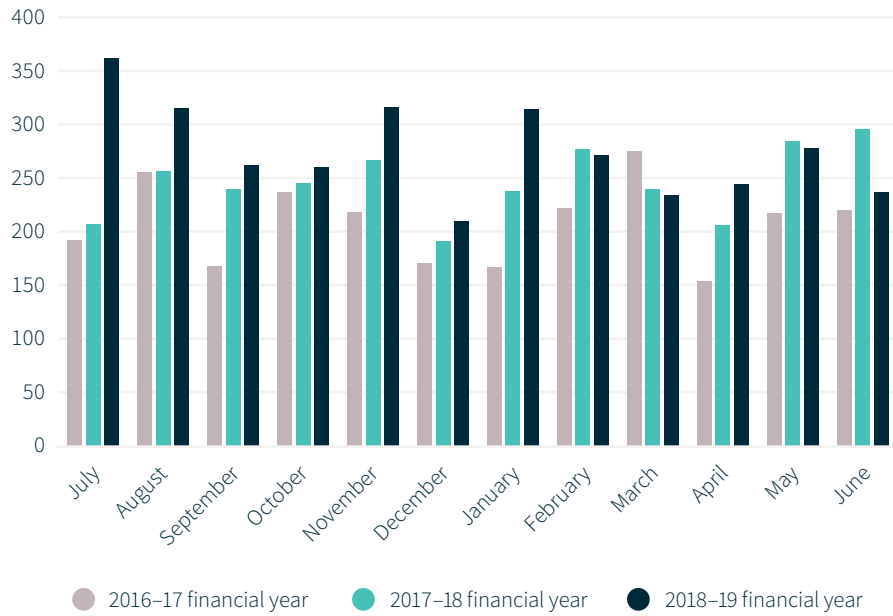
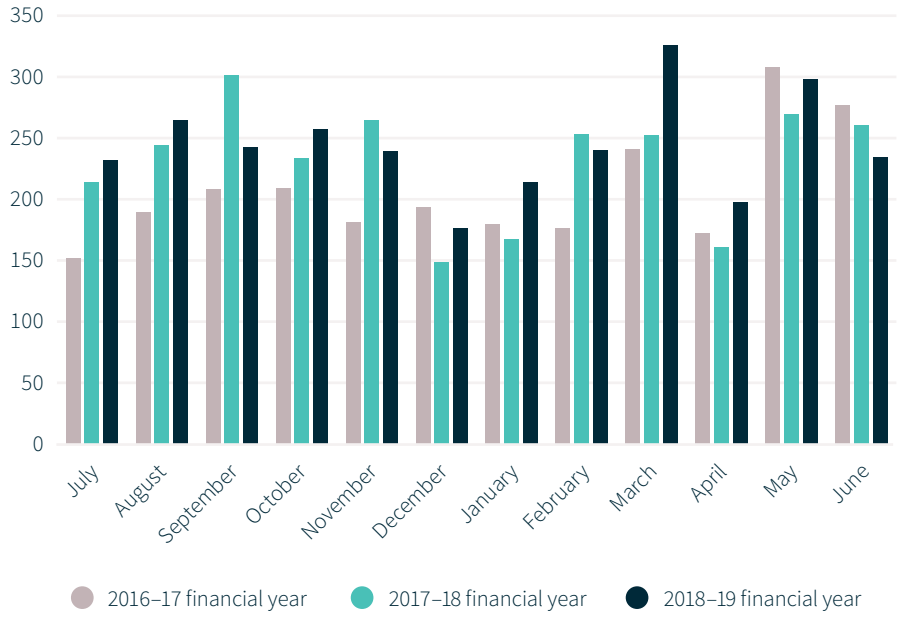


Figure 2.2: Privacy complaints closed each month during the last three financial years



As part of our MOU with the ACT Government, we continued to provide privacy services to ACT public sector agencies including handling privacy complaints under the Information Privacy Act.

Issues raised in privacy complaints

The majority (71.1%) of privacy complaints we received were about the handling of personal information under the APPs. The most common issues raised in these complaints were:

1. Use or disclosure of personal information (APP 6)
2. Security of personal information (APP 11)
3. Access to personal information (APP 12)
4. Collection of solicited personal information (APP 3)
5. Quality of personal information (APP 10).

During this reporting period, only 10.4% of the privacy complaints we received were about credit reporting — a decrease from the last two financial years (2017–18: 14%; 2016–17: 16%). This decrease reflected the continuing role of external dispute resolution schemes in resolving complaints about credit reporting matters.

More information is available in Appendix D.

Sectors

Privacy complaints can occur in a broad range of sectors. The top six sectors complained about are consistent with those in 2017–18 and 2016–17, except for complaints about credit reporting bodies, which was overtaken by online services (see Table 2.3 and Case Study 2.3).

Table 2.3: Top 10 sectors by privacy complaints received

Sector	Number
Finance (including superannuation)	418
Australian Government	389
Health service providers	327
Telecommunications	240
Retail	176
Online services	172
Credit reporting bodies	156
Personal services (includes employment, childcare and vets)	135
Real estate agents	131
Debt collectors	92

Case Study 2.3: Disclosure of personal information by telecommunication providers

The complainant became aware that her personal information had been inappropriately disclosed by a telecommunications provider to a public directory. The complainant was unclear which party was at fault: the telecommunications provider or the publisher of the public directory. The complainant had been the victim of domestic violence and the disclosure of her information in the public directory had adverse consequences and put her safety at risk.

We investigated and conciliated the matter. Both respondents acknowledged they had interfered with the complainant's privacy and each gave the complainant $20,000 in compensation.

Resolving privacy complaints

In 2018–19, the average time we took to close a privacy complaint was 4.4 months. This compares to 3.7 months in 2017–18 and 4.7 months in 2016–17.

Our early resolution process, which we introduced in 2017–18, aims to see if a resolution can be achieved between the parties soon after the complaint is lodged. Our Early Resolution team finalised 64.5% of all privacy complaints in 2018–19, an improvement on 2017–18 when that team closed 53% of all privacy complaints.

When we cannot resolve a privacy complaint using the early resolution process, we make further inquiries and conciliate and/or investigate the matter.

Where we resolved complaints through conciliation, we achieved positive outcomes: either through the shuttle conciliation our Early Resolution team conducted or the formal conciliation conferences our Investigations team undertake. In many cases, parties advised the case officer of a high level of satisfaction with the outcome they had achieved together.

We support our staff to resolve complaints through providing conciliation training. We have a number of staff involved in conciliation, including senior staff, accredited under the National Mediator Accreditation Standards.

During this reporting period we closed 95.1% of all complaints within 12 months (2017–18: 97%).

In 2018–19, the main remedies we achieved in resolving privacy complaints were:

1. Record amended
2. Access provided
3. Other or confidential
4. Apology
5. Compensation.

See Case Studies 2.4 to 2.7. More information is available in Appendix D.

Case Study 2.4: Complaint about a false profile on a dating platform

The complainant became aware that a false profile, including their photos and personal details, had been created on the respondent's dating platform.

We made inquiries with the respondent. The respondent conducted several searches to attempt to locate the profile in question and determined that it had been deleted, possibly by the individual who created the account. The respondent advised that when they receive a complaint of this nature their practice is to locate and delete any accounts that appear to be fraudulent. The respondent also told the complainant what steps can be taken if a similar issue arises in the future. For example, the complainant could contact the respondent's privacy team directly or use their app's reporting tools.

Case Study 2.5: Disclosure of sensitive information by a medical centre

The complainant became aware that the respondent, a medical centre, had disclosed their sensitive medical information to their spouse without their consent.

We successfully conciliated the matter. The respondent gave the complainant a formal apology prepared by the doctor who was responsible for the disclosure. The doctor also got advice and privacy education material from their insurer, and in turn, carried out a training seminar for other practitioners working at the medical centre.

Case Study 2.6: Disclosure of personal information by a retail store

The complainant discovered that the respondent, a retail store, disclosed their personal information to a third party who fraudulently impersonated the complainant.

We resolved the matter by conciliation. The respondent apologised to the complainant, strengthened their identity verification processes and paid:

- for the complainant's subscription to a credit and identity protection service and mail re-direction
- for counselling sessions for the complainant
- $5,000 compensation to the complainant.

Case Study 2.7: Failure to ensure the security of personal information by a superannuation fund

The complainant alleged that the respondent, a superannuation fund provider, inadvertently included his welcome letter in correspondence they sent to another customer. The letter included the complainant's name, age, account number, address, account balance and investments.

We resolved the matter by conciliation. The respondent apologised to the complainant, implemented additional security measures and paid $1,500 compensation.

Community and sector engagement

An important part of our role is interacting with key industry and community stakeholders, including government bodies and external dispute resolution schemes, about recurring or significant issues arising in complaints.

External dispute resolution schemes

The Information Commissioner can recognise an external dispute resolution scheme to handle particular privacy-related complaints (s 35A of the Privacy Act). The external dispute resolution schemes that are recognised are:

- Australian Financial Complaints Authority
- Energy & Water Ombudsman NSW
- Energy & Water Ombudsman SA
- Energy and Water Ombudsman (Victoria) Limited
- Energy & Water Ombudsman Queensland
- Energy and Water Ombudsman Western Australia
- Public Transport Ombudsman Limited (Victoria)
- Telecommunications Industry Ombudsman Limited
- Tolling Customer Ombudsman.

Community engagement

For PAW (12 to 18 May 2019), the OAIC produced a podcast with Legal Aid NSW in which our staff were interviewed about credit reporting.

During this reporting period, we continued to use social media to promote privacy awareness. For example, we used Twitter and Facebook to raise awareness about the privacy controls available in My Health Record and to encourage Australians to use them.

Determinations

Under s 52 of the Privacy Act, the Commissioner may make determinations in relation to privacy complaints. The Commissioner may also make determinations in relation to privacy CIIs. The Commissioner must make these determinations personally, that is, the decision cannot be delegated.

In 2018–19, the Commissioner made three privacy determinations. One of these determinations included findings that the respondent had not interfered with the individual's privacy. This complaint was dismissed under s 51(1)(a) of the Privacy Act. See Determinations 2.1 to 2.3.

Determination 2.1: 'QP' and Commonwealth Bank of Australia Ltd (Privacy) AICmr 48 (28 June 2019)

The Commissioner found that the Commonwealth Bank of Australia Limited (CBA) interfered with the complainant's privacy by using and disclosing personal information about the complainant which was inaccurate, out-of-date or incomplete and in breach of APP 10.2.

In this instance, the Commissioner declared under s 52(2)(b)(ii) that CBA issue a written apology to the complainant acknowledging their interference with the complainant's privacy and declared under s 52(1)(b)(iii) that CBA pay the complainant $15,000 for non-economic loss suffered.

Determination 2.2: 'QF' and Others and Spotless Group Limited (Privacy) [2019] AICmr 20 (28 May 2019)

The Commissioner found that Spotless Group Limited (Spotless) interfered with the complainants' privacy by improperly disclosing, through their related entity Cleanevent, the complainants' personal information to the Australian Workers' Union, in breach of National Privacy Principle (NPP) 2. The Commissioner also found Spotless failed to take reasonable steps to protect the complainants' personal information from misuse and unauthorised disclosure, in breach of NPP 4.

In this instance, the Commissioner declared under s 52(2)(b)(ii) that Spotless give each complainant a written apology acknowledging their interference with the complainants' privacy and the distress it caused, and that Spotless engage an independent reviewer with privacy expertise to undertake a review of Spotless's current privacy compliance procedures, policies and processes, as well as those of Spotless's subsidiaries, and give the Commissioner a copy of the reports from the independent review.

The Commissioner also declared under s 52(1)(b)(iii) that Spotless pay each complainant compensation between $3,000 and $6,000 for non-economic loss suffered.

Determination 2.3: 'QD' and Dr 'QE' and Idameneo (No.123) Pty Limited (Privacy) [2019] AICmr 17 (3 May 2019)

The complainant alleged that Idameneo (No. 123) Pty Limited (Idameneo) and Dr QE had interfered with their privacy by failing to give access to personal information on request, in breach of APP 12.1. The complainant also alleged the respondents had failed to take reasonable steps to give access to the information in a way that met the party's needs, and failed to give reasons for their refusal in breach of APP 12.5 and APP 12.9.

The Commissioner found that Idamenao and Dr QE could rely on the exception at APP 12.3(a) to refuse access. APP 12.3(a) provides that an entity is not required to give access where the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual.

The Commissioner determined that the respondents gave sufficient consideration to alternative means of access and that the steps taken by the respondents were reasonable in the particular circumstances, finding no breach of APP 12.5.

The Commissioner also considered that although the respondents had not yet given the complainant a written notice of refusal of access, the 'reasonable time' limit had not yet expired, finding no breach of APP 12.9.

Data breach notifications

NDB scheme

The NDB scheme commenced on 22 February 2018. Under the NDB scheme, Australian Government agencies and private sector organisations with existing personal information security obligations under the Privacy Act must notify individuals who are likely to be at risk of serious harm as a result of a data breach. The OAIC must also be notified (see Table 2.4).

Our responsibilities under the NDB scheme include:

- receiving notifications of eligible data breaches
- encouraging compliance with the NDB scheme, including handling complaints and taking regulatory action in response to instances of non-compliance
- offering advice and guidance to regulated organisations and informing the community about how the NDB scheme operates.

We reviewed each notice received under the NDB scheme to consider whether the data breach had been contained, that the organisation or agency had taken reasonable steps to mitigate the impact of the data breach on the individuals at risk of serious harm, and that the organisation or agency was taking reasonable steps to minimise the likelihood of a similar data breach occurring again. The Commissioner's new powers under the NDB scheme include the discretion to direct an entity to notify individuals of eligible data breaches or declare that notification does not need to occur or can be delayed.

The first 12 months of the NDB scheme saw a 733% increase in the number of data breach notifications, compared to those received under the previous voluntary scheme. This is consistent with international trends in jurisdictions with comparable mandatory data breach notification schemes and shows that organisations and agencies were aware of their obligations and engaging with the requirements of the NDB scheme.

As well as quarterly statistics reports, in May 2019 we published the *Notifiable Data Breaches Scheme 12-Month Insights Report*, which gives a detailed overview of the first year of the NDB scheme's operation. We have also jointly published with the Australian Cyber Security Centre a resource for organisations and agencies on tips to mitigate the risk of data breaches.

Case Studies 2.8 and 2.9 describe some data breaches we have handled during this reporting period.

Case Study 2.8: Human error

In preparation for a product launch, an employee made an unintended change to an organisation's system configuration. This resulted in customers being able to view details for other customers when activating their account online. The data breach mainly affected contact information, but in some instances also included passport or driver licence information.

The organisation notified affected individuals by text message and offered to pay the cost of their passport being reissued or setting up a credit-monitoring service.

To prevent reoccurrence of a similar data breach, the organisation took a range of steps, including introducing additional reviews for its content delivery network and implementing system configuration changes via an application programming interface.

Case Study 2.9: Cyber-related incident

An organisation detected suspicious activity on several customer accounts. They investigated and found that some accounts had been accessed without authorisation using correct credentials. The investigation concluded that the incident was not a result of a vulnerability in the organisation's systems but occurred due to 'credential stuffing', where previously compromised credentials are used to gain unauthorised access to systems via large-scale automated log-in requests.

The organisation informed affected individuals that their personal information including contact details, date of birth and membership number had been compromised and offered identity and cyber support services at no cost.

In response to the incident, the organisation reset passwords on all affected accounts, implemented additional security measures to detect and mitigate malicious traffic and undertook continuous system monitoring.

Voluntary data breaches

Prior to the introduction of the NDB scheme, we administered a voluntary data breach notification scheme. This scheme allowed organisations and agencies to self-report possible data breaches to us. We continued to register voluntary data breach notifications for incidents that do not fall within the scope of the NDB scheme (see Table 2.4). These included data breaches that occurred prior to 22 February 2018, incidents that did not meet the threshold of the NDB scheme, and data breaches that did not involve organisations or agencies the NDB scheme regulates.

Table 2.4: NDB, voluntary and mandatory My Health Record notifications

Year	2016–17	2017–18	2018–19
Notifiable data breaches	–	305	950*
Voluntary notifications	114	174	175
Mandatory notifications (*My Health Records Act 2012*)	35	28	35
Total	**149**	**507**	**1,160**

* Where data breaches affect multiple entities, we may receive multiple notifications relating to the same data breach. Notifications to us about the same data breach incident are counted as a single notification in this number. End-of-year statistics may differ from quarterly publication statistics.

In 2018–19, the number of voluntarily reported data breaches remained consistent with the previous financial year and represented a 53.5% increase on voluntary data breaches reported in 2016–17, prior to the introduction of the NDB scheme.

The consistent number of voluntary notifications can be explained, in part, by our activities in engaging with stakeholders about the requirements of the NDB scheme, along with global regulatory developments which focused on the importance of understanding and responding to data breaches, and the domestic focus on transparency and good governance arising from the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry.

Given this significant increase in mandatory and voluntary notifications, we did not meet our overall target for finalising data breach notifications, with 79% of notifications under the NDB scheme finalised within 60 days and 66.1% of voluntary data breach notifications finalised within 60 days.

We also administered a mandatory scheme for digital health data breaches. See Table 4 and the *Annual Report of the Australian Information Commissioner's Activities in Relation to Digital Health 2018–19*, which will be available on our website no later than 28 November 2019.

Privacy Commissioner initiated investigations

Section 40(2) of the Privacy Act allows the Commissioner to investigate an act or practice that may be an interference with privacy on the Commissioner's own initiative. This power is used to investigate possible interferences with privacy that are of concern but are not in direct response to an individual privacy complaint.

A Privacy Commissioner initiated preliminary inquiry or investigation (CII) is conducted in response to an incident of significant community concern or discussion or notification from a third party about potentially serious privacy issues, or result from a notification about a data breach. Our key objective in undertaking Commissioner initiated preliminary inquiries or an investigation is improving the privacy practices of the organisation or agency involved.

During this reporting period, we opened preliminary inquiries or and/or an investigation in relation to 15 matters (see Table 2.5). At 30 June 2019, 10 of these matters and 12 matters from 2017–18 were ongoing.

Table 2.5: Privacy Commissioner initiated investigations

Year	Number of CIIs
2016–17	29
2017–18	21
2018–19	15

Privacy assessments

During this reporting period, we assessed privacy practices in the finance, telecommunications and government sectors, as well as the digital health sector.

We used a range of methods to conduct our assessments, such as comprehensive and in-depth review of policy documents, interviews with staff and site inspections. Consistent with last financial year, the businesses or government agencies we assessed accepted all our recommendations or planned to act on them.

Loyalty programs

During this reporting period we followed up on recommendations and suggestions we made in our 2016 loyalty program assessments of Woolworths Limited (Woolworths) and Coles Supermarkets Australia (Coles) with the following results:

- Woolworths provided evidence to show that they had adopted all our suggestions.
- Coles provided evidence to show that they had implemented our recommendation.
- Coles adopted several of our suggestions and gave adequate reasons where they did not adopt one of our suggestions.

Finance

In 2018–19 we assessed the privacy policies of 20 organisations in the finance sector that use the Document Verification Service (DVS) for identity verification. We considered whether the privacy policy of each organisation was clearly expressed, available, up-to-date and contained the content required for the purposes of APP 1.3 to 1.5. We finalised these assessments during this reporting period and made a total of 40 recommendations.

Telecommunications

We began a series of assessments in 2017–18 to see if certain telecommunications service providers are meeting their information security obligations under APP 11 — Security of Personal Information, for the personal information they are required to retain under the data retention scheme that came into full effect on 13 April 2017. In 2017–18 we conducted the fieldwork for two assessments. We conducted the fieldwork for two more assessments in this series in 2018–19. We will finalise this series of assessments in 2019–20.

Government

Unique student identifier

In 2018–19, under our MOU with the Department of Education and Training acting through the Student Identifiers Registrar (the Registrar), we assessed how the Unique Student Identifiers (USI) Office, acting on behalf of the Registrar, managed privacy controls for the USI Transcript Service. Our assessment considered the USI Office's practices, procedures and systems to make sure they complied with APP 1.2. This was the first assessment to consider the application of the Privacy Code. We did not identify any privacy risks that resulted in recommendations in this assessment.

We also followed up on the implementation of recommendations made in our 2016 assessment of how the USI Office handled personal information. We were satisfied that the USI Office had implemented the recommendations.

ACT Government

Under our MOU with the ACT Government, in 2017–18 we conducted an assessment of Housing and Community Services ACT. The assessment is examining whether Housing ACT is:

- using and disclosing personal information in line with their TPP 6 obligations
- taking reasonable steps to secure their personal information holdings as required by TPP 11

We will complete this assessment in 2019–20.

In 2018–19 we conducted an assessment involving 10 ACT Government agencies. This assessment is outlined in the *Memorandum of Understanding with the Australian Capital Territory for the Provision of Privacy Services 2018–19 Annual Report*, which is available on our website no later than 22 October 2019.

More information is available in Appendix C.

Data matching

We perform several functions to help government agencies to understand their privacy requirements and adopt best privacy practice when undertaking data-matching activities.

Data matching is the process of bringing together data sets that come from different sources and comparing those data sets with the intention of producing a match. Several government agencies use data matching to detect non-compliance, identify instances of fraud and recover debts owed to the Australian Government. For example, to identify individuals or businesses that may be under-reporting income or turnover, the Australian Taxation Office (ATO) may match tax return data with the data provided by banks.

Government agencies that carry out data-matching activities must comply with the Privacy Act. Data matching raises privacy risks because it involves analysing personal information about large numbers of people, the majority of whom are not under suspicion of non-compliance.

Statutory data matching

The Information Commissioner has statutory responsibilities under the *Data-matching Program (Assistance and Tax) Act 1990* (Data-matching Act). The Data-matching Act authorises the use of tax file numbers in data-matching activities by the Department of Human Services (DHS), the Department of Veterans' Affairs and the ATO. In previous financial years, we have inspected DHS's data-matching records to make sure they comply with the requirements of the Data-matching Act. Agencies continue to rely less on data matching using tax file numbers, so this financial year we again focused on providing advice and oversight of data-matching activities outside the Data-matching Act.

Enhanced Welfare Payment Integrity

The Enhanced Welfare Payment Integrity — non-employment income data-matching measure was announced in the 2015–16 Mid-Year Economic and Fiscal Outlook (MYEFO). It increases DHS's capability to conduct data matching to identify non-compliance by welfare recipients. In 2017–18, we conducted two privacy assessments of DHS's handling of personal information. The first assessment looked at the Non-Employment Income Data Matching (NEIDM) program. The second assessment examined the Pay-As-You-Go (PAYG) program. During this reporting period, we finalised the NEIDM program assessment. We will finalise the PAYG program assessment in 2019–20.

During this reporting period we also conducted two privacy assessments which looked at how DHS secures the personal information used in the NEIDM and PAYG programs and at the role of the ATO as a source of data for DHS's data-matching activities. We will finalise both assessments in 2019–20.

Data-matching under the voluntary guidelines

We administer the Guidelines on Data-matching in Australian Government Administration, which are voluntary guidelines to help government agencies adopt appropriate privacy practices when undertaking data-matching activities not covered by the Data-matching Act. This financial year we reviewed 13 data-matching program protocols submitted by matching agencies including the ATO, the Department of Home Affairs and the DHS.

Digital health assessments

Health information is considered particularly sensitive. This sensitivity has been recognised in the *My Health Records Act 2012* (My Health Records Act) and *Healthcare Identifiers Act 2010*, which regulate the collection, use and disclosure of personal information, and give the Information Commissioner a range of enforcement powers. This sensitivity is also recognised in the Privacy Act which treats health information as 'sensitive information'.

We initiated three assessments relating to the My Health Record system in 2018–19 and continue to progress two assessments that began in the previous financial year. See the *Annual Report of the Australian Information Commissioner's Activities in Relation to Digital Health 2018–19*, which is available on our website no later than 28 November 2019.

Advice for businesses and agencies

Our teams provided advice for businesses and Australian Government agencies on their obligations under the Privacy Act. We also helped businesses and agencies achieve best practice in their approach to privacy management.

During this reporting period we issued advice on a variety of matters, including:

- adoption, use and disclosure of government related identifiers
- Australian Government Privacy Code
- credit reporting
- data breach notification requirements, including the NDB scheme
- de-identification and re-identification

- digital identity systems
- direct marketing
- draft CDR legislation, rules and technical standards
- government data matching
- higher education proposals affecting the handling of information about students
- law enforcement and national security
- the My Health Record system
- new and emerging technologies
- online communications and privacy
- privacy and international agreements
- privacy and security, as part of the Attorney-General's Department's reforms to the Protective Security Policy Framework
- telecommunications.

We also drafted submissions on issues such as:

- artificial intelligence
- Australian Government data sharing
- CDR draft legislation (see Case Study 2.10)
- cooperative intelligent transport systems and automated vehicle data
- digital platforms
- human rights and technology
- identity information
- the My Health Record system
- telecommunications.

Case Study 2.10: Consumer Data Right regulatory framework

The CDR is a right for consumers to access particular data in a readily usable form and to direct a business to transfer that data securely to a data recipient. It aims to give consumers greater control over how their data is used and disclosed in order to create more choice and competition in sectors of the economy the Treasurer designates.

In 2018–19, we gave privacy advice to the Treasury, the ACCC and CSIRO's Data61 in the course of their respective development of the CDR legislation, rules and technical standards.

In August 2018, the Treasury released the exposure draft of the Treasury Laws Amendment (Consumer Data Right) Bill. We provided a submission on the exposure draft, acknowledging the potential of the CDR to give consumers greater choice and control over how their data is used, while highlighting important areas where further clarification or consideration of privacy issues was required. Many of our recommendations were reflected in the legislation introduced to Parliament in February 2019. We continued to engage with the Treasury throughout the development of the legislation.

We provided advice to the ACCC on their development of the CDR rules. These rules complement the legislation by defining the elements for consent, outlining the accreditation framework for data recipients and elaborating on the privacy safeguards.

We also provided advice to Data61 regarding development work for technical standards relating to consumer experience. The consumer experience standards will focus on the steps data recipients must take when seeking consent, and data holders must take when seeking authorisation, from consumers.

Resources

We released our new website for public feedback in June 2019 (see performance measure 1.7.4).

We published a new training resource about the Privacy Code to educate Australian Government agencies about privacy best practice. We also published the *Notifiable Data Breaches Scheme: 12-Month Insights Report*, to help businesses and agencies understand the common causes of data breaches and how they can implement proactive strategies to prevent data breaches.

Privacy legislative instruments

Under the Privacy Act, the Information Commissioner has powers to make certain legislative instruments. These legislative instruments must comply with the requirements of the *Legislation Act 2003*. They are publicly available on the Federal Register of Legislative Instruments.

Privacy (Australian Honours System) Public Interest Determination 2018

On 5 October 2018, the Information Commissioner made Privacy (Australian Honours System) Public Interest Determination 2018. This followed an application for a public interest determination (PID) on 6 March 2018 from the Department of Home Affairs and replaced Privacy (Australian Honours System) Temporary Public Interest Determination 2018.

The PID allows the Department of Home Affairs to disclose Australian citizenship and permanent residency status information without breaching APP 6 — Use or Disclosure of Personal Information, for a period of 10 years. The disclosures can be made to the Department of the Prime Minister and Cabinet and to the Office of the Official Secretary to the Governor-General for the purposes of their consideration of nominees for awards (such as those in the Australian honours system).

Privacy (Disclosure of Homicide Data) Public Interest Determination 2019

On 18 March 2019, the Information Commissioner made Privacy (Disclosure of Homicide Data) Public Interest Determination 2019. This followed an application for a PID on 1 November 2018 from the Australian Federal Police (AFP).

The PID allows the AFP to disclose personal information to the Australian Institute of Criminology (AIC) without breaching APP 6 — Use or Disclosure of Personal Information, for a period of seven years. The information which can be disclosed under the PID is personal information requested by the AIC about offenders and suspects in relation to homicides in the ACT, for the purposes of the AIC's research under the National Homicide Monitoring Program and the publication of aggregate findings.

This PID replaced PID No. 5 which expired on 1 October 2018.

National Health (Privacy) Rules 2018

On 11 October 2018, the Information Commissioner issued the *National Health (Privacy) Rules 2018* (National Health (Privacy) Rules). These rules are required under s 135AA of the *National Health Act 1953* (National Health Act). The National Health (Privacy) Rules commenced on 1 April 2019 and repealed the previous s 135AA instrument — the *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs* — on the same date.

The National Health (Privacy) Rules regulate the way that Australian Government agencies link and store claims information obtained under the Medicare Benefits Program and the Pharmaceutical Benefits Program.

Among other things, s 135AA(5) of the National Health Act requires that these rules prohibit agencies from storing claims information obtained under the Medicare Benefits Program and the Pharmaceutical Benefits Program on the same database.

Privacy awareness

During this reporting period we continued to promote awareness and understanding of privacy rights in the community, with a focus on data breaches, online security, credit reporting, health information and personal data.

Over the past year, in Australia and around the world, privacy has come into sharper focus as one of the top priorities for organisations and the public alike.

Our personal information is a critical input to the economy and government agencies, and we are seeing heightened awareness of privacy issues as organisations and agencies face increasingly complex data protection challenges.

Privacy Awareness Week is an annual event that highlights the importance of protecting personal information, and helps organisations, agencies and the public navigate the privacy landscape.

For organisations and agencies, it's a reminder to review privacy practices and policies and educate their staff about information handling obligations.

For the public, it's an opportunity to share information and practical tips that empower people to take control of their personal information.

Our central message is 'Don't be in the Dark on Privacy', and over the course of the week we will explore a series of privacy priorities including data breaches, online security, your credit, health information and your data.

We hope that you will all join the conversation, at our events and on social media, to shine a light on these important issues.

Angelene Falk, Australian Information Commissioner and Privacy Commissioner, in 'Welcome to Privacy Awareness Week', September 2019.

Reaching our audiences

We offered training and guidance on the Australian Government Agencies Privacy Code (which commenced in July 2018) to Australian Government privacy officers, including face-to-face training sessions (118 attendees).

In early 2019, we ran a social media campaign to promote the My Health Record system's privacy controls.

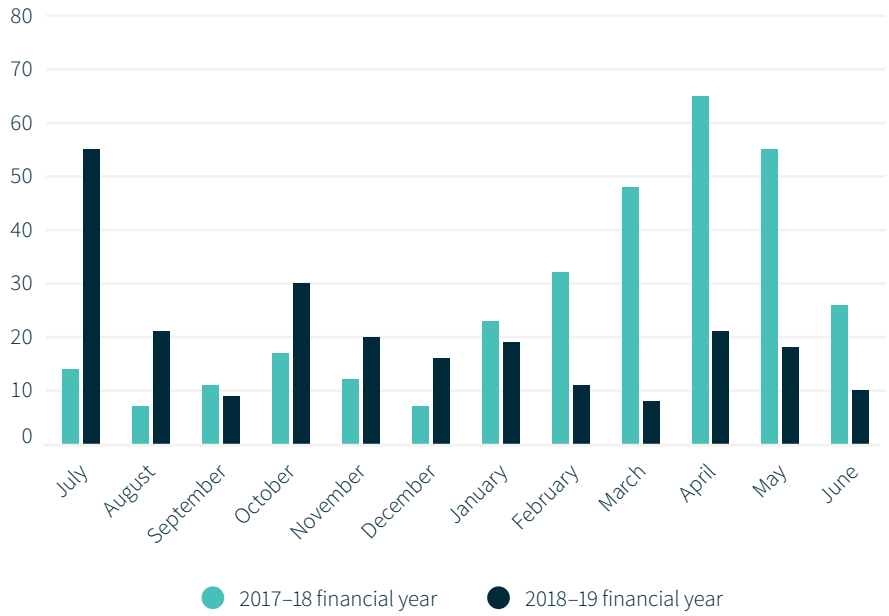
Speaking engagements

This year we participated in 34 speaking engagements aimed at privacy professionals.

Media

In 2018–19 we received 238 media enquiries: 219 were about privacy and 25 of those about My Health Record; the other 19 enquiries were about the OAIC and FOI.

Figure 2.3: Media enquiries received during 2018–19



Freedom of information (FOI)

FOI provides a legally enforceable right of access to government documents. It applies to Australian Government ministers and most agencies, although the obligations of agencies and ministers are different.

Individuals have rights under the FOI Act to request access to government documents. The FOI Act also requires government agencies to publish specified categories of information. It also encourages them to release other information proactively.

FOI enquiries

The OAIC handles enquiries from the public on FOI issues, including the IC review function.

During this reporting period, we experienced a 49.2% increase in FOI enquiries from 2017–18. Our Enquiries Line answered 2,051 telephone calls about FOI and responded to 824 written enquiries about FOI. We also helped with six in-person enquiries about FOI. Most enquiries were about the OAIC's jurisdiction (47%) and general processes for FOI applicants (39%), including how to make an FOI request or complaint, or seek review of an FOI decision. See Table 2.6.

Table 2.6: FOI enquiries by issue

Issue	Number*
OAIC's jurisdiction	1,343
General processes	1,130
Processing by agency	263
Agency statistics	236
Access to personal information	34
Access to general information	20
Vexatious application	10
Amendment and annotation	5
Information Publication Scheme	4

* There may be more than one issue handled in an enquiry.

IC reviews

An IC review is a review of decision made by an Australian Government agency or minister subject to the FOI Act, including a decision:

- refusing to grant access to a document wholly or in part
- where a requested a document does not exist or cannot be found
- granting access to a document where a third party has a right to object (for example, if a document contains their personal information)
- to impose charges for access to a document, including a decision to refuse to waive or reduce charges, or
- refusing to amend or annotate a record of personal information.

During this reporting period we experienced another significant increase in IC review applications, receiving 928 applications — a 15.9% increase over 2017–18. The overall increase in IC review applications since 2015–16, when we received 510, was 82%.

Despite this continuing significant increase in IC review applications, we finalised 659 IC reviews in 2018–19 (an 8% increase over 2017–18, when we finalised 610 IC reviews). We finalised 73.1% within 12 months. The increase in IC review applications and our focus on reducing the number of cases over 12 months old prevented us from reaching our target of finalising 80% of IC reviews within 12 months.

Informal resolution

We pursued informal resolution of IC reviews where possible. We used various approaches to help resolve an IC review such as narrowing the scope of a review, providing an appraisal or preliminary view, and trying to reach agreement between the parties. In 2018–19, we finalised 599 IC reviews without a formal decision being made (90.9%).

We finalised 76 IC reviews (12.7%) after the applicant withdrew their application following:

- action the agency took to resolve the issues in the IC review (such as issuing a decision and statement of reasons in a deemed access refusal case, or making a revised decision under s 55G of the FOI Act to give the applicant access to further documents or material), or
- our appraisal of their case's merits.

We also finalised 25 IC reviews by written agreement between the parties under s 55F of the FOI Act.

IC review decisions under s 55 K of the FOI Act

The Information Commissioner made 60 decisions under s 55K of the FOI Act in 2018–19. Of these:

- 37 decisions (61.7%) set aside and substituted the decision under review
- 4 decisions (6.7%) varied the decision under review
- 19 decisions (31.7%) affirmed the decision under review.

Of the decisions the Information Commissioner affirmed, two were revised during the IC review to give greater access to the documents sought under s 55G of the FOI Act.

Two were access grant decisions, where the Information Commissioner agreed with the agency that the documents were not exempt under the FOI Act and must be released.

The decisions we published under s 55K of the FOI Act continued to be an important part of our work. They addressed novel issues and built on existing FOI laws and judgments. They helped agencies interpret the FOI Act and guide them in exercising their powers and functions.

All IC review decisions are published on the AustLII website as part of the Australian Information Commissioner (AICmr) series.

Case Studies 2.11 and 2.15 describe IC review decisions made during this reporting period.

For more information about IC review decisions under s 55K of the FOI Act, see Appendix D, Review of FOI Decisions.

Case Study 2.11: Jack Waterford and Department of Human Services (Freedom of information) [2019] AICmr 21 (5 June 2019)

The applicant sought access to documents the DHS generated in response to a media request he made to them and a media article he wrote in the week before making the request.

On completing the request consultation process (s 24AB of the FOI Act), the DHS refused the applicant's request on the basis that a practical refusal reason existed. They believed the request did not meet the identification requirements of s 15(2)(b) of the FOI Act (these require a request to supply enough information to enable the DHS to identify the document sought) and processing the request would substantially and unreasonably divert the DHS's resources from their other operations (ss 24AA(1)(a)(i) and 24AA(1)(b) of the FOI Act).

The Information Commissioner was not satisfied that the request consultation notice fulfilled the requirements of s 24AB of the FOI Act, because it did not give the name of a contact person and how the applicant could contact this person, as s 24AB(2)(c) requires. Also, the Information Commissioner was not satisfied the DHS had taken reasonable steps to help the applicant to revise his request and remove the practical refusal reason (s 24AB(3) of the FOI Act). The DHS's notice gave the applicant limited information to help him revise his request and from the applicant's response it was apparent that he had concerns about the steps the DHS took to help him to revise the request.

The DHS also estimated it would take 238 hours to process the request. The Information Commissioner was not satisfied that the DHS discharged its onus to justify the estimated processing time. Also, the Information Commissioner was not satisfied that the DHS had proved that processing the request would substantially and unreasonably divert the DHS's resources from its other operations.

Case Study 2.12: Justin Warren and Department of Human Services (Freedom of information) [2019] AICmr 22 (5 June 2019)

The applicant sought access to meeting agendas, minutes and other notes for meetings held between the DHS and the Minister for Human Services or Minister for Social Services between 1 January 2016 and 31 December 2016.

On completing the request consultation process (s 24AB of the FOI Act), the DHS refused the applicant's request on the basis a practical refusal reason existed. The DHS asserted that processing the request would substantially and unreasonably divert the DHS's resources from its other operations (s 24AA(1)(a)(i)).

The Information Commissioner was not satisfied the DHS took reasonable steps to help the applicant revise the scope of his request to remove the practical refusal reason (s 24AB(3)). The applicant had tried to revise the request but was unsuccessful because he did not understand the terms the DHS used. The Information Commissioner said that where it is apparent that an applicant's attempt to revise the scope of their request doesn't remove the practical refusal reason, the contact person should consider whether they could take additional steps to help the applicant revise their request.

The DHS estimated it would take more than 130 hours to process the request because every branch of the DHS would need to conduct searches for the requested documents. During the IC review, the applicant indicated he would be willing to reduce the scope of his request in light of information the DHS supplied. The DHS then conducted searches within the revised scope and advised that they could not locate any documents. The Information Commissioner considered that when an applicant proposes a revised scope based on advice from the agency that results in no documents being found, unless there are compelling reasons not to, the agency should generally consult with the applicant about why no documents exist and help them to revise the scope of their request before making a decision about the request.

Case Study 2.13: 'QG' and Department of Human Services (Freedom of information) [2019] AICmr 23 (5 June 2019)

The applicant sought access to: 'A copy of all communication, including emails, correspondence, phone calls, internal memos, sms and faxes between Child Support and Complex Assessment departments relating to me.'

On completing the request consultation process (s 24AB of the FOI Act), the DHS refused the applicant's request on the basis a practical refusal reason existed. The DHS asserted the request didn't meet the identification requirements of s 15(2)(b) of the FOI Act (s 24AA(1)(b) of the FOI Act).

The Information Commissioner considered whether the agency had followed the request consultation process under s 24AB of the FOI Act. The Information Commissioner was not satisfied that the DHS had taken reasonable steps to help the applicant revise the scope of the request to remove the practical refusal reason (s 24AB(3). The applicant tried to revise the scope of the request based on the information the DHS supplied. The DHS had a very particular approach to interpreting terms the applicant used in the revised request such as 'relating to' and 'including'. The Information Commissioner said that where an agency or minister takes a very particular approach to interpreting terms an applicant uses, it may be difficult for an applicant to revise the scope of a request to remove the practical refusal reason without the agency or minister suggesting what would be a reasonable request in the circumstances. The Information Commissioner noted that the DHS proposed a revised scope of the request at the start of the IC review and it appeared that this scope could have been proposed during the request consultation process.

The Information Commissioner noted that the FOI Guidelines explain that an agency or minister must read a document request fairly, being mindful not to take a narrow or pedantic approach to its construction. The Information Commissioner was satisfied that the applicant had supplied sufficient information for the DHS to identify the documents sought (s 15(2)(b) of the FOI Act).

Case Study 2.14: Seven Network (Operations) Limited and Australian Federal Police (Freedom of information) [2019] AICmr 32 (6 June 2019)

This is the first IC review decision to consider the application of s 46 of the FOI Act (where the disclosure of the requested documents would be a contempt of Parliament or a Court).

The applicant sought access to documents, including CCTV footage, related to an incident in the Parliament House precinct. The exemption under s46(c) of the FOI Act was applied on a basis that disclosure would infringe parliamentary privilege.

The FOI Guidelines explain that the term 'parliamentary privilege' refers to the privileges or immunities of the Houses of the Parliament, and the powers of the Houses to protect the integrity of their processes. The use of CCTV footage captured by the Parliament House CCTV system is subject to a code which restricts viewing, storing, accessing, releasing and disposing of CCTV footage without the approval of the President of the Senate and the Speaker of the House of Representatives (Presiding Officers).

The Information Commissioner also considered s 6 of the *Parliamentary Precincts Act 1988*, which states that the parliamentary precincts are under the control and management of the Presiding Officers. Given the authority of the Presiding Officers under the Parliamentary Precincts Act 1988 and their endorsement of the code, the Information Commissioner considered the code amounts to a rule of the Houses of Parliament that restricts the use and disclosure of CCTV footage captured in the parliamentary precincts and the act of disclosing CCTV footage contrary to the code would infringe parliamentary privilege.

The Information Commissioner was satisfied that conduct which improperly interfered with the free exercise by the House of Parliament of its authority or functions, such as the contravention of a rule or order of a House of Parliament, may constitute contempt of the parliament and infringe the privileges of the parliament.

The Information Commissioner affirmed the decision refusing access to the CCTV footage.

We have updated paragraphs 5.188 to 5.195 of the FOI Guidelines to refer to this decision.

Case Study 2.15: Rex Patrick and Minister for Resources and Northern Australia (Freedom of information) [2019] AICmr 13 (25 March 2019)

The applicant applied to the Minister for Resources and Northern Australia for access to diary entries relating to the National Radioactive Waste Management Facility at Kimba and Hawker. The Minister refused the request under s 24A of the FOI Act because no 'diary entries' exist.

During the IC review, the Minister's office accepted that the term 'diary' included electronic calendars and other email calendars and schedules. The Minister's office subsequently indicated the Minister was willing to process the request because the scope of the applicant's request included the Minister's electronic email calendars and schedules.

The Information Commissioner was satisfied that documents within the scope of the applicant's request did exist.

FOI complaints

Under s 69 of the FOI Act, the Information Commissioner has power to investigate agency actions about the handling of FOI matters.

Part 11 of the FOI Guidelines explains that making a complaint is not an appropriate mechanism where IC review is available, unless there is a special reason to undertake an investigation and the matter can be dealt with more appropriately and effectively in that way. Generally, an IC review is the more appropriate way for a person to seek review of the merits of an FOI decision, particularly an access refusal or access grant decision. This approach accounts for the relatively small number of FOI complaints received compared with IC review applications.

In 2018–19, we received 61 FOI complaints and closed 22. This represents a slight decrease (1.6%) in lodgements compared with 2017–18 (when 62 FOI complaints were received) and a 24% decrease in finalisations compared with 2017–18 (when 29 FOI complaints were finalised). The decrease in the number of FOI complaints finalised is primarily the result of us receiving a sustained increase in the number of IC review applications and our focus on finalising IC reviews, in particular those over 12 months old.

Of the FOI complaints finalised during this reporting period, 81.8% were closed within 12 months of receipt — meeting the OAIC's target of closing 80% of all FOI complaints within 12 months.

As in previous years, the most common complaints about the handling of FOI matters by agencies were:

- agencies not meeting statutory timeframes
- problems with consultation under practical refusal provisions
- the imposition or amount of a charge
- poor customer service (most commonly a failure to reply to correspondence).

In 2018–19, there was an increase in the number of complaints about decision-makers not stating their name and designation in the notice of decision as s 26 of the FOI Act requires and agency administration of the IPS.

FOI extensions of time

The FOI Act sets out timeframes within which agencies and ministers must process FOI requests.

Where an agency or minister is unable to process an FOI request within the processing period, they may request an extension of time from the FOI applicant or the Information Commissioner.

Where the applicant agrees to an extension of time in writing, the agency or minister must advise the Information Commissioner of the agreement to extend the statutory processing time as soon as practicable.

An agency or minister can apply to the Information Commissioner for an extension of time to the processing period where an agency or minister is able to demonstrate that the processing of the FOI request has been delayed because the FOI request is voluminous or complex in nature (s 15AB of the FOI Act) or where the agency or minister has been unable to process the request within the statutory timeframe and the agency or minister is deemed to have made a decision refusing the FOI request (s 15AC of the FOI Act). See Tables 2.7 and 2.8.

Table 2.7: FOI extension of time (EOT) notifications and requests received and closed

Year	2016–17	2017–18	2018–19
Received	4,412	3,367	3,785
Closed	4,420	3,333	3,779

During this reporting period, we finalised 84% of extension of time applications within five working days.

Table 2.8: FOI extensions of time (EOT) notifications and requests closed, by type

Request type	2016–17	2017–18	2018–19
Section 15AA (notification of EOT agreements between agency and applicant)	3,808	2,762	2,959
Section 15AB (request to OAIC by agency where voluminous or complex)	453	370	562
Section 15AC (request to OAIC by agency where deemed refusal decision)	112	122	178
Section 51DA (request to OAIC by agency for EOT for dealing with amendment/annotation request)	–	1	1
Section 54B (extension of the period to make an internal review request made by agency)	–	–	1
Section 54D (request to OAIC by agency for EOT where deemed affirmation on internal review)	29	38	37
Section 54T (request to OAIC for EOT for person to apply for IC review)	18	40	41
Total	**4,420**	**3,333**	**3,779**

FOI vexatious applicant declarations

The Information Commissioner has the power to declare a person to be a vexatious applicant if she is satisfied that the grounds set out in s 89L of the FOI Act exist.

During 2018–19, the Information Commissioner received nine applications from agencies under s 89K seeking to have a person declared a vexatious applicant. Eight applications were finalised in 2018–19, with three declarations being made, three refused and two withdrawn.

Declarations are published on the AustLII website as part of the AICmr series.

Case Study 2.16 describes an FOI vexatious applicant declaration made during this reporting period.

Case Study 2.16: Office of the Registrar of Indigenous Corporations and 'PW' (Freedom of information) [2019] AICmr 6 (13 February 2019)

'PW' was the subject of a vexatious applicant declaration made by a former Information Commissioner which expired on 3 June 2017. Between 26 July 2017 and 5 July 2018, PW engaged in a further 28 access actions.

In deciding whether to make the declaration, the Information Commissioner considered whether the agency had used other provisions in the FOI Act to lessen the impact of PW's access actions on its operations and whether deficiencies in the agency's FOI administration had contributed to the respondent's access actions. This included: the impact of PW's access actions on the agency's other work, the size of the agency, the resources the agency could reasonably allocate to FOI processing, the impact PW's access actions had on FOI administration in the agency and whether PW had cooperated reasonably with the agency to enable efficient FOI processing.

The Information Commissioner had regard to the parties' submissions and was satisfied the agency had established that PW had repeatedly engaged in access actions that involved an abuse of process by unreasonably interfering with the agency's operations.

The Information Commissioner decided that a declaration for three years was appropriate in circumstances where the respondent had previously been declared vexatious.

FOI agency resources

We produced guidelines and other resources during this reporting period to promote FOI best practice and help Australian Government agencies understand their FOI obligations.

FOI Guidelines

In June 2019, we amended Part 5 of the FOI Guidelines about the exemption in s 46 of the FOI Act (where the disclosure of the requested documents would be a contempt of Parliament or a Court) to reflect the IC review decision: *Seven Network (Operations) Limited and Australian Federal Police (Freedom of information)* [2019] AICmr 32 (6 June 2019). This was the first IC review decision to consider the exemption.

Administrative access resource

In September 2018, we re-issued FOI Agency Resource 14: Access to Government Information — Administrative Access. We sought comments from interested stakeholders about the readability and accessibility of the revised resource.

The resource helps agencies and ministers understand administrative access and emphasises the importance of considering administrative access as an alternative to formal FOI processes. This approach is consistent with the object of the FOI Act to facilitate and promote public access to information promptly and at the lowest reasonable cost.

The resource is available on our website under FOI Guidelines, Administrative Access.

Disclosure log determination

Section 11C of the FOI Act includes some circumstances in which an agency or minister is not required to publish information released in response to FOI requests on their website. Section 11(1)(c) of the FOI Act provides that if the Information Commissioner has made a determination under s 11C(2) of the FOI Act, an agency is not required to publish information specified in the determination.

On 28 November 2018, the Information Commissioner made a determination under s 11C(2) of the FOI Act: *Freedom of Information (Disclosure Log — Exempt Documents) Determination 2018*.

This determination establishes two circumstances in which an agency or minister is not required to publish information, in addition to those already found in s 11C of the FOI Act. The additional circumstances are:

- Information was exempt from disclosure when the agency or minister gave access to the applicant.
- Information in the document that the agency or minister would have decided was exempt at the time access was given to the applicant, if the request had been made by someone other than the applicant.

The determination is otherwise substantially the same as the previous determination and will be in effect for five years.

Newsletters

We sent 13 newsletters and updates to FOI contact officers who signed up to our ICON members. These newsletters included news and information about FOI, information management and general OAIC updates. ICON members also received alerts including reminders for upcoming ICON events, reporting and policy updates, and summaries of recent IC review decisions.

Events

We participated in a range of activities throughout the year to raise awareness about accessing government-held information, the role of the OAIC and our processes.

ICON information sessions

We re-established six-monthly information sessions for information contact officers. These ICON sessions were held in Canberra in September 2018 and April 2019. Both sessions were attended by more than 70 information contact officers.

The ICON sessions provided an opportunity to network with FOI colleagues and to discuss information access issues. Examples of topics covered at ICON meetings include:

- policy and operational updates from the Information Commissioner and other key OAIC staff, including the Deputy and Assistant Commissioners
- the role of the FOI practitioner in promoting accountability and transparency

- the OpenAustralia Foundation introducing its Right to Know website
- the National Archives of Australia published a new records authority for ministerial records.

National Association of Community Legal Centres Conference

In August 2018, staff from the OAIC attended the National Association of Community Legal Centres Conference in Sydney, where they explained the right to access government-held information to staff from community legal centres across Australia.

Australian Government Solicitor forums

The Information Commissioner gave the keynote address at the Australian Government Solicitor's FOI and Privacy Forum in Canberra on 17 May 2019.

In her address, 'From personal information to information access rights: building a strong foundation for our democracy and digital economy', the Information Commissioner spoke about how important it is for practitioners to handle personal information in an honest and ethical way. She also canvassed the international access to information landscape, sharing insights from the International Conference of Information Commissioners in South Africa in March.

Right to Know Day 2018

International Right to Know Day is held on 28 September each year. In 2018, we promoted the event and general awareness of information access rights with a digital campaign.

The campaign included three short videos highlighting information access themes: 'It's your right to know', 'How to make an FOI request' and '12 tips for FOI decision-makers'. These videos are available as an ongoing resource on our website and YouTube channel.

Staff also set up an information booth at Wynyard in Sydney to promote Right to Know Day on 28 September. They talked to more than 500 commuters and provided printed material about open government and the right to access government-held information.

Media

The AIAC issued a joint media statement for Right to know Day following a meeting hosted by the OAIC in Sydney on 20 to 21 September 2018.

The statement encouraged all government agencies across Australia and New Zealand to take a proactive approach towards releasing information and documents.

> *The community's right to know is the foundation of open and accountable government. Access to the information and data held by government strengthens our democracy by promoting greater public participation and scrutiny and supporting better decision-making.*
>
> *International Right to Know Day, held on 28 September, recognises citizens' right to access this information and reinforces the importance of transparency in building trust in government. As Information Commissioners we strive to promote and uphold the fundamental right of citizens to access government information.*
>
> *We are also supporting information access officers in carrying out their very important role as part of the effective management of government-held information.*
>
> Statement of Australian and New Zealand information access commissioners for International Right to Know Day 2018

Website

We released a new website for public feedback in June 2019 (see performance measure 1.7.4).

IPS

Between May and August 2018, we undertook an IPS survey of all Australian Government agencies subject to the FOI Act. ORIMA Research conducted the survey on behalf of the OAIC.

The survey reviewed the operation of the IPS in each agency and gave agencies an opportunity to comply with the requirement to conduct a review under s 9 of the FOI Act. This section requires an agency to complete a review of the operation of the IPS within their agency as appropriate from time to time and within five years of the commencement of the IPS.

The final report was published in June 2019. The survey had a response rate of 82% (compared to 78% in 2012) with 190 agencies participating.

The results show the IPS continued to be an important element in ensuring information Australian Government agencies hold is managed for public purposes and is treated as a national resource.

Agency responses confirmed a continued commitment to IPS requirements and principles, although a decline was observed in the four key areas of compliance measured in both the 2012 and 2018 survey. Larger agencies generally reported higher levels of compliance with IPS requirements and better practice principles, compared with micro to small agencies.

Compliance with the IPS is an ongoing statutory responsibility for agencies subject to the FOI Act. The survey's results have helped us to identify areas where improvements can be made to further promote the proactive publication of Australian Government information.

FOI processing statistics received from Australian Government agencies and ministers

Below is a selection of the FOI request processing statistics provided by Australian Government agencies and ministers to the OAIC. The figures have been rounded to the nearest whole number. For detailed figures, see Appendix D.

The number of FOI requests received across Australian Government agencies increased by 13% from 34,438 in 2017–18 to 38,879 in 2018–19. This increase was experienced in both requests for personal information and other (non-personal) information;

however, the increase in personal requests was more pronounced (15% higher than 2017–18) than non-personal requests (3% higher than 2017–18). The increase in requests for personal information is in large part due to the Department of Home Affairs (DHA) receiving 24% more personal requests in 2018–19 than in the previous financial year.

In 2018–19, 32,440 or 83% of all FOI requests were for documents containing personal information. This is marginally higher than in 2017–18 and 2016–17 when 82% of all requests were for personal information.

In 2018–19, the DHA, the DHS and the Department of Veterans' Affairs together continued to receive the majority of FOI requests (69% of the total). Of these, 96% were for personal information.

The percentage of FOI requests processed within the applicable statutory time period decreased from 85% in 2017–18, to 83% in 2018–19.

The percentage of FOI requests granted in full increased from 50% of all requests in 2017–18 to 52% in 2018–19 and the number of requests refused decreased from 16% of all FOI requests in 2017–18 to 13% in 2018–19.

The personal privacy exemption in s 47F of the FOI Act remains the most claimed exemption (38% of all exemptions claimed).

The total reported costs attributable to processing FOI requests in 2018–19 was $59.85 million, a 15% increase on 2017–18 ($52.19 million).

Australian Government agencies and ministers issued 2,225 notices advising of an intention to refuse a request for a practical refusal reason in 2018–19. This is a 47% decrease on the number issued in 2017–18. Of these requests, 77% were subsequently refused or withdrawn; that proportion was 84% in 2017–18.

There was a 7% decrease in the total charges notified in 2018–19 but a 6% increase in the total charges collected by Australian Government agencies ($122,774).

The total number of entries added to agency website disclosure logs in 2018–19 (1,200) is 9% higher than 2017–18, when 1,104 new entries were added. However, the proportion of entries from which members of the public can directly access disclosure log documents from agency websites remains low at 59%.

There was a 12% increase in internal review applications in 2018–19. Of the 829 decisions on internal review, 429 (52%) affirmed the original decision, 91 (11%) set aside the original decision and granted access in full and 232 (28%) granted access in part.

For more information, see Appendix E.

Part 3
Management and accountability

Corporate governance

Setting strategic direction, implementing effective policies and processes, and monitoring progress are key elements of our corporate governance framework.

Enabling legislation

The Office of the Australian Information Commissioner (OAIC) was established in November 2010 as an independent statutory agency under the *Australian Information Commissioner Act 2010* (AIC Act). We are responsible for privacy functions conferred by the *Privacy Act 1988* (Privacy Act) and other laws.

We have freedom of information (FOI) functions, including the oversight of the operation of the *Freedom of Information Act 1982* (FOI Act) and review of decisions made by agencies and ministers under that Act.

We are accountable as a non-corporate Commonwealth entity under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). Our annual reporting responsibilities are under s 46 of the PGPA Act and s30 of the AIC Act. We also have a range of reporting and other responsibilities under legislation generally applicable to Australian Government authorities.

Portfolio structure and responsible minister

The OAIC is a statutory authority within the Attorney-General's portfolio. The minister responsible is the Hon Christian Porter MP.

Executive

During this reporting period, our Executive team, comprising the Commissioner, Deputy and Assistant Commissioners, met weekly and oversaw all aspects of our business covering corporate management and performance, finance, human resources, governance, risk management, external engagement and business planning.

Risk management

Our risk management framework helped staff to assess risks, make informed decisions and confidently engage with risk.

Our Executive team regularly considered and reviewed the risks the agency faced and the reports on risk received from the Audit Committee.

Fraud

Our fraud control plan, fraud control policy and guidelines were made available to all staff through internal communications channels.

Audit Committee

Our Audit Committee assisted the Commissioner to discharge her responsibilities on the OAIC's finances and performance, risk oversight and management, and system of internal control. The Audit Committee oversaw the work of our internal auditors, ensured the annual work program was adhered to and ensured appropriate coverage of our strategic and operational risks.

The Audit Committee was chaired by a member of our Executive team and had two independent members. The independent members are employees of the National Disability Insurance Scheme Agency and the Australian Human Rights Commission (AHRC). Representatives from the Australian National Audit Office (ANAO) attend meetings of the Audit Committee as observers.

Corporate services

We have a memorandum of understanding (MOU) with the AHRC that covers the provision of corporate services. This includes financial, administrative, information and communications technology and human resources services. We also sublease our premises in Sydney from the AHRC under this arrangement.

See Appendix C for more information on the MOU with the AHRC.

External scrutiny

During this reporting period, there were no judicial decisions or decisions of administrative tribunals that had a significant impact on our operations.

There were no reports on our operations by the Auditor-General, a parliamentary committee or the Commonwealth Ombudsman.

Human resources

We strove to provide a workplace that offered fulfilling and challenging work, and promoted the professional and personal development of our staff. As the national expert in both privacy and FOI regulation, we relied on a team of highly skilled and competent staff.

In 2018–19, we continued to build the capacity of existing staff, to develop the necessary skill sets to meet the heightened demands for privacy and information management for the Australian public, government agencies and wider industry.

Our people

As a small agency in a competitive market, we continued to face challenges in recruiting and retaining skilled people. We used a number of strategies to attract talent including online and social media advertising.

During this reporting period, we had an average staffing level of 85.3. Our staff turnover was approximately 24% for ongoing staff. This involved 19 ongoing staff resigning, retiring or transferring to other Australian Government agencies. We had 20 ongoing staff join us during 2018–19. As of 30 June 2019, we had 89.7 full-time equivalent (FTE) staff, including ongoing and non-ongoing employees.

Table 3.1: Staffing profile as at 30 June 2019

Classifications	Male	Female	Full-time	Part-time	Total ongoing	Total non-ongoing	Total
Statutory office holder	–	1	1	–	–	1	1
SES Band 2	–	1	1	–	1	–	1
SES Band 1	1	1	1	1	2	–	2
Executive Level 2 ($120,356–$137,355)	3	11	7	7	12	2	14
Executive Level 1 ($103,618–$110,840)	5	22	20	7	25	2	27
APS 6 ($82,219–$90,539)	5	24	24	5	26	3	29
APS 5 ($74,563–$78,827)	4	9	10	3	7	6	13
APS 4 ($66,881–$71,064)	5	5	9	1	5	5	10
Total	**23**	**74**	**73**	**24**	**78**	**19**	**97**

Employment statistics

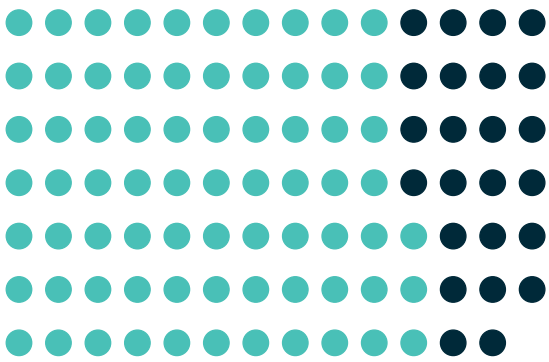
Our staff

97
Total staff

Employment type

73
Full-time

24
Part-time



Gender

74
Female

23
Male

Diversity

31%
Non-English speaking background

1%
Indigenous

Learning and development

We are committed to ongoing learning and development of our staff, recognising the importance of building and developing capabilities to meet current and future needs.

Our work is increasingly becoming more technical as the digital environment becomes more complex, and we are also seeing more complex and substantive complaints and investigations compared to previous financial years.

Staff can access a range of learning and development opportunities in line with the Australian Public Service Commission's 70:20:10 model of learning.

We provided the following components of our learning and development program for staff.

Talking about performance

Our Performance Management and Development scheme 'Talking about performance' provided regular and formal assessment of staff members' work performance and identified learning and development needs.

Professional skills development

Staff undertake specialised training to ensure they are continuously building on their subject-matter expertise and able to access the latest information from industry and government.

During this reporting period, relevant staff attended specialist training in decision writing, administrative law, conciliation and investigations, auditing skills, leadership and management, plain English, mental health and managing unreasonable complainant conduct.

Study and professional membership assistance

We encouraged staff to undertake study to develop their knowledge and skills in relevant areas. Study assistance provided skilled and knowledgeable staff for our current and future requirements and supports staff in meeting their learning and development needs.

Benefits

We offer our people the following non-salary related benefits:

- flexible working arrangements including home-based work where appropriate
- employee assistance program
- extended purchased leave
- maternity and adoption leave
- parental leave
- leave for personal compelling reasons and exceptional circumstances
- access to paid leave at half pay
- Flextime (APS staff)
- study assistance
- support for professional and personal development
- healthy lifestyle reimbursement
- screen-based eyesight testing and screen-based prescription glasses reimbursements
- influenza vaccinations.

Workplace relations

The Fair Work Commission approved our Enterprise Agreement 2016–19 on 5 May 2016. On 7 March 2019, the Commissioner issued the Public Service (Office of the Australian Information Commissioner Non-SES Employees) Determination 2019 made under s 24(1) of the *Public Service Act 1999*. The determination commenced on 13 May 2019 and staff covered by the enterprise agreement received an increase to their existing salary and specified allowances, and will receive further increases in 2020 and 2021.

In 2018–19, no staff received performance pay. Six staff had an individual flexibility arrangement.

OAIC Consultation Forum

The OAIC Consultation Forum provides an opportunity for our staff and their representatives to meet and consider issues relating to working at the OAIC.

Statutory office holder and SES remuneration

The Remuneration Tribunal determined the terms and conditions of our statutory office holder. Remuneration for the Senior Executive Service (SES) officers is governed by determinations made by the Commissioner under s 24(1) of the *Public Service Act 1999*.

For information on executive remuneration, see Appendix B.

Workplace diversity

In 2018–19, 31% of staff had a non-English speaking background and 1% identified as Indigenous.

Our Diversity Committee, during this reporting period, was led by an Assistant Commissioner and included representatives from the Regulation and Strategy Branch, Enquiries Line and Dispute Resolution Branch. The Diversity Committee was responsible for driving our wider diversity strategy and coordinating our obligations under Multicultural Access and Equity Reporting.

Work health and safety

We shared expertise and resources on work health and safety (WHS) issues with the AHRC. Our WHS representatives were members of the joint agencies' WHS Committee. We conducted regular site inspections as a preventative measure and there were no significant incidents reported by staff during this reporting period. All new staff are provided with WHS information upon commencement and ongoing support and assistance is offered to our people.

Procurement

During this reporting period, we complied with the Australian Government's procurement policy framework. We encouraged competition, value for money, transparency and accountability.

All procurement was conducted in line with the Commonwealth Procurement Rules to ensure the efficient, effective, economical and ethical use of Australian Government resources.

During this reporting period, no contracts were exempt from reporting on AusTender on the basis that publishing contract details would disclose exempt matters under the FOI Act. All awarded contracts valued at $100,000 (GST inclusive) or greater contained standard clauses granting the Auditor-General access to contractors' premises.

Consultants

We engaged consultants where we lacked specialist expertise or when independent research, review or assessment was required.

Typically, we engaged consultants to:

- investigate or diagnose a defined issue or problem
- carry out defined reviews or evaluations
- provide independent advice, information or creative solutions to assist with our decision-making.

During this reporting period, three new consultancy contracts were entered into involving total actual expenditure of $185,543 (excluding GST). In addition, one ongoing consultancy contract was active during the period, involving total actual expenditure of $50,000 (excluding GST).

Before we engaged consultants, we took into account the skills and resources required for the task, the skills available internally and the cost-effectiveness of engaging external expertise. All the decisions that we made relating to consultancy contracts were made in line with the PGPA Act and related regulations, including the Commonwealth Procurement Rules.

This report contains information about actual expenditure on contracts for consultancies. Information on the value of contracts and consultancies is available on the AusTender website.

Small business

We supported small business participation in the Commonwealth Government procurement market and engaged with small businesses wherever appropriate during our work. Small and medium enterprises (SME) and small enterprise participation statistics are available on the Department of Finance's website. We also recognised the importance of ensuring that small businesses were paid on time. Our statistics are available in the Survey of Australian Government Payments to Small Business, which is available on the Department of Employment, Skills, Small and Family Business's website.

Other requirements

Advertising and market research

During this reporting period, the OAIC conducted the following advertising campaign: Paid Facebook promotion of consumer resources explaining the privacy controls available at oaic.gov.au.

Grant programs

No grant programs took place in 2018–19.

Fraud

We have a fraud control plan, fraud control policy and guidelines which are made available to staff through internal communication channels.

Memoranda of understanding

We received funding for specific services under a range of memoranda of understanding, see Appendix C.

Disability reporting

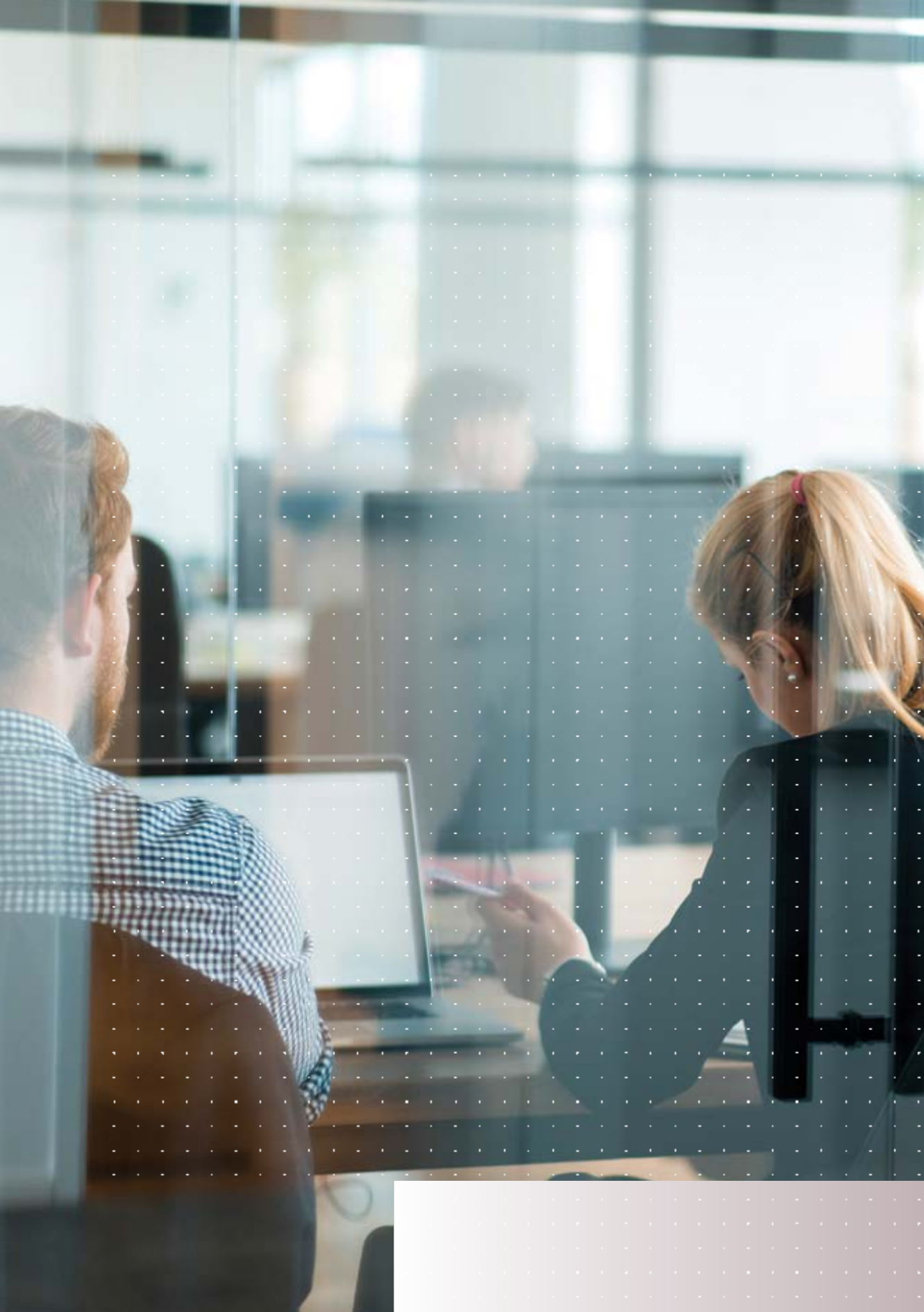
The Commonwealth Disability Strategy has been overtaken by the National Disability Strategy 2010–20, which set out a 10-year national policy framework to improve the lives of people with disability, promote participation and create a more inclusive society. A high-level two-yearly report tracks progress against each of the six outcome areas of the strategy and presents a picture of how people with disability are faring. The first of these reports can be found at dss.gov.au

Ecologically sustainable development and environment performance

Section 516A of the *Environment Protection and Biodiversity Conservation Act 1999* requires us to report on how our activities accord with the principles of ecologically sustainable development. Our role and activities do not directly link with the principles of ecologically sustainable development or impact on the environment, other than through our business operations regarding the consumption of resources required to sustain our operations. We use energy saving methods in the OAIC's operation and endeavour to make the best use of resources.

Information Publication Scheme

As required by the FOI Act, we have an Information Publication Scheme entry on our website that provides information on our structure, functions, appointments, annual reports, consultation arrangements, FOI officer, information we routinely release following FOI requests and information we routinely provide to the Australian Parliament.



Part 4
Financial Statements

Australian National Audit Office

INDEPENDENT AUDITOR'S REPORT

To the Attorney-General

Opinion

In my opinion, the financial statements of the Office of the Australian Information Commissioner ('the Entity') for the year ended 30 June 2019:

(a) comply with Australian Accounting Standards – Reduced Disclosure Requirements and the *Public Governance, Performance and Accountability (Financial Reporting) Rule 2015*; and

(b) present fairly the financial position of the Entity as at 30 June 2019 and its financial performance and cash flows for the year then ended.

The financial statements of the Entity, which I have audited, comprise the following statements as at 30 June 2019 and for the year then ended:

- Statement by the Accountable Authority and Chief Financial Officer;
- Statement of Comprehensive Income;
- Statement of Financial Position;
- Statement of Changes in Equity;
- Cash Flow Statement; and
- Notes to the financial statements, comprising a Summary of Significant Accounting Policies and other explanatory information.

Basis for opinion

I conducted my audit in accordance with the Australian National Audit Office Auditing Standards, which incorporate the Australian Auditing Standards. My responsibilities under those standards are further described in the *Auditor's Responsibilities for the Audit of the Financial Statements* section of my report. I am independent of the Entity in accordance with the relevant ethical requirements for financial statement audits conducted by the Auditor-General and his delegates. These include the relevant independence requirements of the Accounting Professional and Ethical Standards Board's APES 110 *Code of Ethics for Professional Accountants* (the Code) to the extent that they are not in conflict with the *Auditor-General Act 1997*. I have also fulfilled my other responsibilities in accordance with the Code. I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my opinion.

Accountable Authority's responsibility for the financial statements

As the Accountable Authority of the Entity, the Australian Information Commissioner is responsible under the *Public Governance, Performance and Accountability Act 2013* (the Act) for the preparation and fair presentation of annual financial statements that comply with Australian Accounting Standards – Reduced Disclosure Requirements and the rules made under the Act. The Australian Information Commissioner is also responsible for such internal control as the Australian Information Commissioner determines is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, the Australian Information Commissioner is responsible for assessing the ability of the Entity to continue as a going concern, taking into account whether the Entity's operations will cease as a result of an administrative restructure or for any other reason. The Australian Information Commissioner is also responsible for disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless the assessment indicates that it is not appropriate.

GPO Box 707 CANBERRA ACT 2601
19 National Circuit BARTON ACT
Phone (02) 6203 7300 Fax (02) 6203 7777

Auditor's responsibilities for the audit of the financial statements

My objective is to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes my opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with the Australian National Audit Office Auditing Standards will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements.

As part of an audit in accordance with the Australian National Audit Office Auditing Standards, I exercise professional judgement and maintain professional scepticism throughout the audit. I also:

- identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for my opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control;
- obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Entity's internal control;
- evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by the Accountable Authority;
- conclude on the appropriateness of the Accountable Authority's use of the going concern basis of accounting and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the Entity's ability to continue as a going concern. If I conclude that a material uncertainty exists, I am required to draw attention in my auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify my opinion. My conclusions are based on the audit evidence obtained up to the date of my auditor's report. However, future events or conditions may cause the Entity to cease to continue as a going concern; and
- evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

I communicate with the Accountable Authority regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that I identify during my audit.

Australian National Audit Office

Jodi George

Executive Director

Delegate of the Auditor-General

Canberra

11 September 2019

Office of the Australian Information Commissioner

STATEMENT BY THE ACCOUNTABLE AUTHORITY AND CHIEF FINANCIAL OFFICER

In our opinion, the attached financial statements for the year ended 30 June 2019 comply with subsection 42(2) of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), and are based on properly maintained financial records as per subsection 41(2) of the PGPA Act.

In our opinion, at the date of this statement, there are reasonable grounds to believe that the Office of the Australian Information Commissioner (OAIC) will be able to pay its debts as and when they fall due.

Angelene Falk
Australian Information Commissioner

10 September 2019

Brenton Attard
Chief Financial Officer

10 September 2019

Statement of comprehensive income

for the period ended 30 June 2019

	Notes	2019 $'000	2018 $'000	Original budget $'000
NET COST OF SERVICES				
Expenses				
Employee benefits	1.1A	**12,003**	9,481	10,572
Suppliers	1.1B	**4,618**	4,271	5,127
Depreciation and amortisation	2.2A	**464**	530	399
Total expenses		**17,085**	14,282	16,098
Own-source income				
Own-source revenue				
Rendering of services	1.2A	**2,029**	2,590	2,170
Other revenue	1.2B	**36**	36	–
Total own-source revenue		**2,065**	2,626	2,170
Gains				
Other gains	1.2C	**–**	1	33
Total gains		**–**	1	33
Total own-source income		**2,065**	2,627	2,203
Net cost of services		**(15,020)**	(11,655)	(13,895)
Revenue from Government	1.2D	**13,825**	10,711	13,496
Deficit attributable to the Australian Government		**(1,195)**	(944)	(399)
OTHER COMPREHENSIVE INCOME				
Items not subject to subsequent reclassification to net cost of services				
Changes in asset revaluation surplus		**–**	19	–
Total other comprehensive income		**–**	19	–

The above statement should be read in conjunction with the accompanying notes.

Budget variances commentary

The major variances on the Statement of Comprehensive Income are employee benefits, depreciation and amortisation, rendering of services revenue, revenue from Government and the operating deficit.

During the reporting period the OAIC incurred higher than anticipated employee benefits costs. The increased costs relate to: recruitment activities to support workload requirements, including by way of short-term contractors and an additional and unforeseeable lump sum superannuation contribution as required by the Department of Finance.

Rendering of services revenue reflects variations to memorandums of understanding with other government entities during the financial year, which resulted in a reduction of revenue.

Depreciation and amortisation variation relates new intangibles such as the new oaic.gov.au website which was established during the reporting period.

As part of the 2019–20 Budget the OAIC received an additional $329,000 as appropriated funding.

The operating deficit relates to the above variances that were not known at the time of original the budget preparation.

Statement of financial position

as at 30 June 2019

	Notes	2019 $'000	2018 $'000	Original budget $'000
ASSETS				
Financial assets				
Cash	2.1A	**601**	589	661
Trade and other receivables	2.1B	**4,527**	5,072	1,656
Total financial assets		**5,128**	5,661	2,317
Non-financial assets				
Infrastructure, plant and equipment	2.2A	**643**	977	1,967
Intangibles	2.2A	**684**	610	554
Other non-financial assets	2.2B	**483**	79	80
Total non-financial assets		**1,810**	1,666	2,601
Total assets		**6,937**	7,327	4,918
LIABILITIES				
Payables				
Suppliers	2.3A	**1,131**	1,174	899
Other payables	2.3B	**1,371**	1,698	–
Total payables		**2,503**	2,872	899
Non-interest bearing liabilities				
Lease incentives	2.4A	**488**	729	253
Total interest bearing liabilities		**488**	729	253
Provisions				
Employee provisions	4.1A	**2,303**	1,745	1,771
Total provisions		**2,303**	1,745	1,771
Total liabilities		**5,293**	5,346	2,923
Net assets		**1,644**	1,981	1,995
EQUITY				
Contributed equity		**2,873**	2,013	2,873
Reserves		**172**	172	154
Accumulated results		**(1,400)**	(205)	(1,032)
Total equity		**1,645**	1,981	1,995

The above statement should be read in conjunction with the accompanying notes.

Budget variances commentary

The major variances on the Statement of Financial Position are financial assets, non-financial assets, payables, non-interest bearing liabilities and equity. As noted on the Statement of Comprehensive Income, a contributing factor to these variations were a number of activities that could not be readily budgeted for.

The cash balance and other receivables reflect a timing difference between funds held in the OAIC's operating bank account and appropriations receivable in the Official Public Account (OPA). The OAIC generally maintains a working bank account balance by transferring funds from the OPA when required. Note 2.1B provides details of the receivables.

Prepayments are the only other non-financial asset held by the OAIC and includes insurance premium, annual subscription costs and lease security deposits. The variation largely relates to security deposits for new short-term leases and a Memorandum of Understanding prepayment to the Australian Human Rights Commission.

The payables variance arose due to the timing difference for supplier payables at year-end.

The variance in liabilities arising from lease commitments results from increased lease space due to the increase in staffing numbers.

The variation in Infrastructure, Plant and Equipment relates to the decision to defer capital works activities.

The employee provision variance represents the increase in staffing numbers not known at the time of budget preparation.

Commentary on equity variance is included on the Statement of Changes in Equity.

Statement of changes in equity

for the period ended 30 June 2019

	Notes	2019 $'000	2018 $'000	Original budget $'000
CONTRIBUTED EQUITY				
Opening balance				
Balance carried forward from previous period		**2,013**	2,013	2,013
Contributions by owners				
Equity injection — appropriations		**860**	–	860
Total transactions with owners		**860**	–	860
Closing balance as at 30 June		**2,873**	2,013	2,873
RETAINED EARNINGS				
Opening balance				
Balance carried forward from previous period		**(205)**	739	(620)
Adjustment for changes in accounting policies		**–**	–	(13)
Adjusted opening balance		**(205)**	739	(633)
Comprehensive income				
Deficit for the period		**(1,195)**	(944)	(399)
Total comprehensive income		**(1,195)**	(944)	(399)
Closing balance as at 30 June		**(1,400)**	(205)	(1,032)
ASSET REVALUATION RESERVE				
Opening balance				
Balance carried forward from previous period		**173**	154	154
Comprehensive income				
Other comprehensive income		**–**	19	–
Total comprehensive income		**–**	19	–
Closing balance as at 30 June		**173**	173	154
TOTAL EQUITY				
Opening balance				
Balance carried forward from previous period		**1,981**	2,906	1,547
Comprehensive income				
Deficit for the period		**(1,195)**	(944)	(399)
Other comprehensive income		**–**	19	–
Total comprehensive income		**(1,195)**	(925)	(399)

Statement of changes in equity (continued)

for the period ended 30 June 2019

	Notes	2019 $'000	2018 $'000	Original budget $'000
Transactions with owners				
Contributions by owners				
Equity injection — appropriations		**860**	–	860
Total transactions with owners		**860**	–	860
Closing balance as at 30 June		**1,645**	1,981	1,995

The above statement should be read in conjunction with the accompanying notes.

Accounting policy

Equity injections

Amounts appropriated which are designated as 'equity injections' for a year (less any formal reductions) and Departmental Capital Budgets are recognised directly in contributed equity in that year.

Budget variances commentary

The major variance on the Statement of Changes in Equity relates to retained earnings and comprehensive income.

As a non-corporate Commonwealth entity and in accordance with net cash appropriation arrangements the OAIC budgets for a break-even operating result, adjusted for depreciation and amortisation expense. During the reporting period a combination of factors as outlined in the commentary on the Statement of Comprehensive Income resulted in an operating deficit.

Cash flow statement

for the period ended 30 June2019

	Notes	2019 $'000	2018 $'000	Original budget $'000
OPERATING ACTIVITIES				
Cash received				
Appropriations		**13,496**	10,711	13,496
Cash transferred from the Public Account		**4,325**	1,500	–
Sale of goods and rendering of services		**1,484**	3,395	2,170
GST received		**537**	411	250
Total cash received		**19,842**	16,017	15,916
Cash used				
Employees		**(11,459)**	(9,879)	(10,572)
Suppliers		**(5,853)**	(4,769)	(5,692)
Section 74 receipts transferred to OPA		**(2,473)**	(3,328)	–
Total cash used		**(19,785)**	(17,976)	(16,264)
Net cash from/(used by) operating activities		**57**	(1,959)	(348)
INVESTING ACTIVITIES				
Cash used				
Purchase of infrastucture, plant and equipment		**–**	–	(879)
Purchase of intangibles		**(205)**	(163)	–
Total cash used		**(205)**	(163)	(879)
Net cash from/(used by) investing activities		**(205)**	(163)	(879)
FINANCING ACTIVITIES				
Cash received				
Contributed equity		**160**	–	860
Total cash received		**160**	–	860
Net cash from/(used by) financing activities		**160**	–	860
Net increase/(decrease) in cash held		**12**	(2,122)	(367)
Cash and cash equivalents at the beginning of the reporting period		**589**	2,711	661
Cash and cash equivalents at the end of the reporting period	2.1A	**601**	589	294

The above statement should be read in conjunction with the accompanying notes.

Budget variances commentary

The major variances on the Cash Flow Statement includes cash received, cash used and purchase of intangibles.

As noted in the commentary on the Statement of Comprehensive Income and Statement of Financial Position, the OAIC ensured delivery of its program outcomes during the reporting period which impacted on cash received and cash used activities as well as the purchase of intangibles.

Overview

Objectives of the OAIC

The OAIC is an Australian Government controlled entity established under the *Australian Information Commissioner Act 2010*.

The OAIC budgeted for a breakeven result, adjusted for depreciation and amortisation of $464,000. During the reporting period there were a number of factors which were not anticipated that resulted in an operating deficit. A significant factor included an additional and unforeseeable lump sum superannuation contribution of $531,000 that the OAIC became aware of in May 2019.

The OAIC is structured to meet the following outcome:

> Provision of public access to Commonwealth Government information, protection of individuals' personal information, and performance of Information Commissioner, freedom of information and privacy functions.
>
> The OAIC activities contributing toward this outcome are classified as departmental. Departmental activities involve the use of assets, liabilities, income and expenses controlled or incurred by the OAIC in its own right.

The basis of preparation

The financial statements are general purpose financial statements and are required by s 42 of the *Public Governance, Performance and Accountability Act 2013*.

The financial statements have been prepared in accordance with:

a) *Public Governance, Performance and Accountability (Financial Reporting) Rule 2015* (FRR) for reporting periods ending on or after 1 July 2015; and

b) Australian Accounting Standards and Interpretations — Reduced Disclosure Requirements issued by the Australian Accounting Standards Board (AASB) that apply for the reporting period.

The financial statements have been prepared on an accrual basis and in accordance with the historical cost convention, except for certain assets and liabilities at fair value. Except where stated, no allowance is made for the effect of changing prices on the results or the financial position. The financial statements are presented in Australian dollars.

New accounting standards

Adoption of new accounting standard requirements

No accounting standard has been adopted earlier than the application date as stated in the standard. No new, revised, amending standards and interpretations that were issued prior to the sign-off date and are applicable to the current reporting period have a material effect, or expected to have a future material effect, on the OAIC's financial statements.

Future Australian accounting standard requirements

The following new standards and interpretations were issued by the Australian Accounting Standards Board prior to the signing of the statement by the accountable authority and chief financial officer, which are expected to have a material impact on the OAIC's financial statements for future reporting period(s):

Standard/interpretation	Application date for the OAIC[1]	Nature of impending change/s in accounting policy and likely impact on initial application
AASB 15 Revenue from Contracts with Customers AASB 2014-5 Amendments to Australian Accounting Standards arising from AASB 15 AASB 2015-8 Amendments to Australian Accounting Standards – Effective Date of AASB 15	1 July 2019	AASB 15 contains a single model that applies to contracts with customers and two approaches to recognising revenue: at a point in time or over time. The model features a contract-based five-step analysis of transactions to determine whether, how much and when revenue is recognised. Depending on the nature of the transaction and the OAIC's current policy, the new standard may have a minimal impact on the timing of the recognition of revenue. Final outcome will need to be considered once the related Income for Not-for-Profit project is completed.
AASB 16 Leases	1 July 2019	AASB 16 removes the classification of leases as either operating leases or finance leases – for the lessee – effectively treating all leases as finance leases. AASB 16 requires a lessee to recognise assets and liabilities for all leases with a term of more than 12 months, unless the underlying asset is of low value. A lessee is required to recognise a right-of-use asset representing its right to use the underlying leased asset and a lease liability representing its obligations to make lease payments. AASB 16 requires enhanced disclosures for both lessees and lessors to improve information disclosed about an entity's exposure to leases. The property lease will create a right of use asset and lease liability for the OAIC. This will impact the value of assets and liabilities, and potentially increase expenses and the value of the depreciation.

1 All other new, revised, amending standards and interpretations that were issued prior to the sign-off date and are applicable to future reporting period(s) are not expected to have a future material impact on the OAIC's financial statements.

Taxation

The OAIC is exempt from all forms of taxation except Fringe Benefits Tax and the Goods and Services Tax (GST).

Events after the reporting period

There are no known events after the reporting period that could have a material impact on the financial statements.

Financial performance

This section analyses the financial performance of the OAIC for the year ended 2019.

1.1 Expenses

	2019 $'000	2018 $'000
1.1A: Employee benefits		
Wages and salaries	**8,856**	7,387
Superannuation		
Defined contribution plans	**1,060**	861
Defined benefit plans	**918**	381
Leave and other entitlements	**1,123**	735
Separation and redundancies	**–**	2
Other employee expenses	**45**	115
Total employee benefits	**12,003**	9,481

Accounting policy

Accounting policies for employee related expenses is contained in the People and Relationships section.

1.1B: Suppliers		
Goods and services supplied or rendered		
Insurance	**23**	22
Office consumables	**47**	23
Official travel	**288**	240
Printing and publications	**22**	44
Professional services and fees	**2,858**	2,646
Property outgoing	**292**	317
Reference materials, subscriptions and licenses	**147**	82
Staff training	**107**	239
Telecommunications	**31**	20
Other	**175**	89
Total goods and services supplied or rendered	**3,990**	3,722
Goods supplied	**215**	149
Services rendered	**3,774**	3,573
Total goods and services supplied or rendered	**3,990**	3,722

1.1 Expenses (continued)

	2019 $'000	2018 $'000
Other suppliers		
Operating lease rentals in connection with		
Related parties		
Subleases	**603**	531
Workers compensation expenses	**25**	18
Total other suppliers	**628**	549
Total suppliers	**4,618**	4,271

Leasing commitments

The OAIC in its capacity as sub-lessee, leases office accommodation that is subject to the provisions of the headlease. The initial periods of accommodation are still current and there are two options in the headlease agreement to renew.

Commitments for minimum lease payments in relation to non-cancellable operating leases are payable as follows:		
Within 1 year	**2,214**	1,266
Between 1 to 5 years	**2,143**	2,553
Total operating lease commitments	**4,357**	3,819

Accounting policy

Operating lease payments are expensed on a straight-line basis which is representative of the pattern of benefits derived from the leased assets.

The discount rate used is the interest rate implicit in the lease. Leased assets are amortised over the period of the lease.

1.2 Own-source revenue and gains

	2019 $'000	2018 $'000
OWN-SOURCE REVENUE		
1.2A: Rendering of services		
Rendering of services	**2,029**	2,590
Total sale of goods and rendering of services	**2,029**	2,590

Accounting policy

Revenue from rendering of services is recognised by reference to the stage of completion of contracts at the reporting date.

The stage of completion of contracts at the reporting date is determined by reference to the proportion that costs incurred to date bear to the estimated total costs of the transaction.

Receivables for goods and services, which have 30-day terms, are recognised at the nominal amounts due less any impairment allowance account. Collectability of debts is reviewed at end of the reporting period. Allowances are made when collectability of the debt is no longer probable.

1.2B: Other revenue		
Resources received free of charge		
Remuneration of auditors	**36**	36
Total other revenue	**36**	36

Accounting policy

Resources received free of charge

Resources received free of charge are recognised as revenue when, and only when, a fair value can be reliably determined and the services would have been purchased if they had not been donated. Use of those resources is recognised as an expense. Resources received free of charge are recorded as either revenue or gains depending on their nature.

GAINS		
1.2C: Other gains		
Sale of assets	–	1
Total other gains	–	1

Accounting policy

Sale of assets

Gains from disposal of assets are recognised when control of the asset has passed to the buyer.

1.2 Own-source revenue and gains (continued)

	2019 $'000	2018 $'000
1.2D: Revenue from Government		
Appropriations		
Departmental appropriation	**13,825**	10,711
Total revenue from Government	**13,825**	10,711

Accounting policy

Revenue from Government

Amounts appropriated for departmental appropriations for the year (adjusted for any formal additions and reductions) are recognised as Revenue from Government when the OAIC gains control of the appropriation, except for certain amounts that relate to activities that are reciprocal in nature, in which case revenue is recognised only when it has been earned. Appropriations receivable are recognised at their nominal amounts.

Financial position

This section analyses the OAIC's assets used to conduct its operations and the operating liabilities incurred as a result. Employee related information is disclosed in the People and Relationships section.

2.1 Financial assets

	2019 $'000	2018 $'000
2.1A: Cash		
Cash on hand and at bank	**601**	589
Total cash and cash equivalents	**601**	589

Accounting policy

Cash is recognised at its nominal amount. Cash and cash equivalents include cash on hand.

2.1B: Trade and other receivables		
Goods and services receivables		
Goods and services	**698**	652
Total goods and services receivables	**698**	652
Appropriations receivables		
Appropriation receivable	**3,736**	4,325
Total appropriations receivables	**3,736**	4,325
Other receivables		
GST Receivable from the Australian Taxation Office	**92**	95
Total other receivables	**92**	95
Total trade and other receivables (gross)	**4,527**	5,072
Total trade and other receivables (net)	**4,527**	5,072
Trade and other receivables (net) expected to be recovered		
No more than 12 months	**4,527**	5,072
Total trade and other receivables (net)	**4,527**	5,072

Accounting policy

Receivables

Receivables are measured at amortised cost using the effective interest method less impairment.

2.2 Non-financial assets

2.2A: Reconciliation of the opening and closing balances of infrastructure, plant and equipment

Reconciliation of the opening and closing balances of infrastructure, plant and equipment for 2019

	Leasehold improvements $'000	Computer, plant and equipment $'000	Total $'000
As at 1 July 2018			
Gross book value	**953**	**24**	**977**
Accumulated depreciation, amortisation and impairment	**–**	**–**	**–**
Total as at 1 July 2018	**953**	**24**	**977**
Depreciation and amortisation	**(318)**	**(15)**	**(333)**
Disposals	**–**	**(1)**	**(1)**
Total as at 30 June 2019	**635**	**8**	**643**
Total as at 30 June 2019 represented by			
Gross book value	**953**	**23**	**976**
Accumulated depreciation, amortisation and impairment	**(318)**	**(15)**	**(333)**
Total as at 30 June 2019	**635**	**8**	**643**

No indicators of impairment were found for infrastructure, plant and equipment.

No infrastructure, plant and equipment are expected to be sold or disposed of within the next 12 months.

Revaluations of non-financial assets

As at 30 June 2019 no independent revaluation had been conducted. The OAIC extended the useful life of a small number of assets there was no material impact on asset balances. The last valuation occurred on 30 June 2018.

2.2 Non-financial assets (continued)

Reconciliation of the opening and closing balances of infrastructure, plant and equipment for 2018

	Leasehold improvements $'000	Computer, plant and equipment $'000	Total $'000
As at 1 July 2017			
Gross book value	1,248	39	1,287
Accumulated depreciation, amortisation and impairment	–	–	–
Total as at 1 July 2017	1,248	39	1,287
Additions			
Purchase	–	–	–
Work-in-progress transfer	–	–	–
Revaluations and impairments recognised in other comprehensive income	17	2	19
Depreciation and amortisation	(312)	(17)	(329)
Total as at 30 June 2018	953	24	977
Total as at 30 June 2018 represented by			
Gross book value	953	24	977
Accumulated depreciation, amortisation and impairment	–	–	–
Total as at 30 June 2018	953	24	977

2.2 Non-financial assets (continued)

Reconciliation of the opening and closing balances of intangibles for 2019

	Intangibles	Total
As at 1 July 2018		
Gross book value	**2,782**	**2,782**
Accumulated depreciation, amortisation and impairment	**(2,172)**	**(2,172)**
Total as at 1 July 2018	**610**	**610**
Additions	**205**	**205**
Depreciation and amortisation	**(131)**	**(131)**
Total as at 30 June 2019	**684**	**684**
Total as at 30 June 2019 represented by		
Gross book value	**2,987**	**2,987**
Accumulated depreciation, amortisation and impairment	**(2,303)**	**(2,303)**
Total as at 30 June 2019 represented by	**684**	**684**

No indicators of impairment were found for intangibles.

No intangibles are expected to be sold or disposed of within the next 12 months.

2.2 Non-financial assets (continued)

Reconciliation of the opening and closing balances of intangibles for 2018

	Intangibles	Total
As at 1 July 2017		
Gross book value	2,619	2,619
Accumulated depreciation, amortisation and impairment	(1,971)	(1,971)
Total as at 1 July 2017	648	648
Additions		
Purchase	43	43
Work-in-progress transfer	120	120
Depreciation and amortisation	(201)	(201)
Total as at 30 June 2018	610	610
Total as at 30 June 2018 represented by		
Gross book value	2,782	2,782
Accumulated depreciation, amortisation and impairment	(2,172)	(2,172)
Total as at 30 June 2018 represented by	610	610

Accounting policy

Assets are recorded at cost on acquisition except as stated below. The cost of acquisition includes the fair value of assets transferred in exchange and liabilities undertaken.

Assets acquired at no cost, or for nominal consideration, are initially recognised as assets and income at their fair value at the date of acquisition, unless acquired as a consequence of restructuring of administrative arrangements. In the latter case, assets are initially recognised as contributions by owners at the amounts at which they were recognised in the transferor's accounts immediately prior to the restructuring.

Asset recognition threshold

Purchases of infrastructure, plant and equipment are recognised initially at cost in the Statement of Financial Position, except for purchases costing less than $5,000, which are expensed in the year of acquisition (other than where they form part of a group of similar items which are significant in total).

Revaluations

Following initial recognition at cost, plant and equipment are carried at fair value. Valuations are conducted with sufficient frequency to ensure that the carrying amounts of assets did not differ materially from the assets' fair values as at the reporting date. The regularity of independent valuations depended upon the volatility of movements in market values for the relevant assets.

Revaluation adjustments are made on a class basis. Any revaluation increment is credited to equity under the heading of asset revaluation reserve except to the extent that it reversed a previous revaluation decrement of the same asset class that was previously recognised in the surplus/deficit. Revaluation decrements for a class of assets are recognised directly in the surplus/deficit except to the extent that they reversed a previous revaluation increment for that class.

Any accumulated depreciation as at the revaluation date was eliminated against the gross carrying amount of the asset and the asset restated to the revalued amount.

Depreciation

Depreciable infrastructure, plant and equipment assets are written-off to their estimated residual values over their estimated useful lives to the OAIC using, in all cases, the straight-line method of depreciation.

Depreciation rates (useful lives), residual values and methods are reviewed at each reporting date and necessary adjustments are recognised in the current, or current and future reporting periods, as appropriate.

Depreciation rates applying to each class of depreciable asset are based on the following useful lives:

	2019	2018
Leasehold improvements	Lease term	Lease term
Computer, plant and equipment	4 to 10 years	4 to 10 years

Impairment

All assets were assessed for impairment at 30 June 2019. Where indications of impairment exist, the asset's recoverable amount is estimated and an impairment adjustment made if the asset's recoverable amount is less than its carrying amount.

The recoverable amount of an asset is the higher of its fair value less costs of disposal and its value in use. Value in use is the present value of the future cash flows expected to be derived from the asset. Where the future economic benefit of an asset is not primarily dependent on the asset's ability to generate future cash flows, and the asset would be replaced if the OAIC were deprived of the asset, its value in use is taken to be its depreciated replacement cost.

Derecognition

An item of plant and equipment is derecognised upon disposal or when no further future economic benefits are expected from its use or disposal.

Intangibles

The OAIC's intangibles comprise software developed for internal use. These assets are carried at cost less accumulated amortisation and accumulated impairment losses.

Software is amortised on a straight-line basis over its anticipated useful life. The useful lives of the OAIC's software are 2 to 5 years (2018: 2 to 5 years).

All software assets were assessed for indications of impairment as at 30 June 2019.

Accounting judgements and estimates

The fair value of infrastructure, plant and equipment has been taken to be the market value of similar assets as determined by an independent valuer.

2.2 Non-financial assets (continued)

	2019 $'000	2018 $'000
2.2B: Other non-financial assets		
Prepayments	**483**	79
Total other non-financial assets	**483**	79
Other non-financial assets expected to be recovered		
No more than 12 months	**483**	79
Total other non-financial assets	**483**	79

No indicators of impairment were found for other non-financial assets.

2.3 Payables

	2019 $'000	2018 $'000
2.3A: Suppliers		
Trade creditors and accruals	**880**	848
Rent payable	**251**	326
Total suppliers	**1,131**	1,174
Suppliers expected to be settled		
No more than 12 months	**943**	901
More than 12 months	**188**	273
Total suppliers	**1,131**	1,174

Settlement is generally made in accordance with the terms of the supplier invoice.

2.3B: Other payables		
Salaries and wages	**61**	71
Superannuation	**12**	11
Other employee expenses	**–**	5
Revenue received in advance	**1,298**	1,611
Total other payables	**1,371**	1,698
Other payables to be settled		
No more than 12 months	**1,371**	1,698
Total other payables	**1,371**	1,698

2.4 Non-interest bearing liabilities

	2019 $'000	2018 $'000
2.4A: Lease incentives		
Lease incentives	**488**	729
Total lease incentives	**488**	729
Minimum lease payments expected to be settled		
Within 1 year	**242**	242
Between 1 to 5 years	**246**	487
Total lease incentives	**488**	729

Accounting policy

Refer to Note 1.1.B.

Funding

This section identifies the OAIC's funding structure.

3.1 Appropriations

3.1A: Annual appropriations ('recoverable GST exclusive')

Annual appropriations for 2019

	Annual appropriation $'000	Adjustments to appropriation[1] $'000	Total appropriation $'000	Appropriation applied in 2019 (current and prior years) $'000	Variance[2] $'000
Departmental					
Ordinary annual services	**13,496**	**552**	**14,048**	**(16,931)**	**(2,883)**
Other services					
Equity injections	**860**	**–**	**860**	**(160)**	**700**
Total departmental	**14,356**	**552**	**14,908**	**(17,091)**	**(2,183)**

1 Adjustments including for PGPA Act s 74 receipts.

2 Variance represents the application of current and previous years appropriation and own-source revenue.

3.1 Appropriations

Annual appropriations for 2018

	Annual appropriation[1] $'000	Adjustments to appropriation[2] $'000	Total appropriation $'000	Appropriation applied in 2018 $'000	Variance[3] $'000
Departmental					
Ordinary annual services	10,711	566	11,277	(14,377)	(3,100)
Total departmental	10,711	566	11,277	(14,377)	(3,100)

1 In 2017–18, there was an amount of $29,000 withheld (s 51 of the PGPA Act) appropriation relating to Attorney-General's portfolio efficiencies.

2 Adjustments including for PGPA Act s 74 receipts.

3 Variance represents the application of current and previous years appropriation and own-source revenue.

3.1B: Unspent annual appropriations ('recoverable GST exclusive')

	2019 $'000	2018 $'000
Departmental		
Appropriation Act (No. 1) 2018–19	**2,473**	–
Appropriation Act (No. 2) 2018–19	**700**	–
Appropriation Act (No. 1) 2017–18	**–**	3,328
Appropriation Act (No. 1) 2016–17	**–**	997
Cash held by OAIC	**601**	589
Total departmental	**3,774**	4,914

3.2 Net cash appropriation arrangements

	2019 $'000	2018 $'000
Total comprehensive income/(loss) less depreciation/amortisation expenses previously funded through revenue appropriations	**(731)**	(414)
Plus: depreciation/amortisation expenses previously funded through revenue appropriation	**(464)**	(530)
Total comprehensive income/(loss) — as per the Statement of Comprehensive Income	(1,195)	(944)
Total comprehensive income — as per the Statement of Comprehensive Income	(1,195)	(944)

People and relationships

This section describes a range of employment and post-employment benefits provided to our people and our relationships with other key people.

4.1 Employee provisions

	2019 $'000	2018 $'000
4.1A: Employee provisions		
Leave	**2,303**	1,745
Total employee provisions	**2,303**	1,745
Employee provisions expected to be settled		
No more than 12 months	**1,765**	1,339
More than 12 months	**538**	406
Total employee provisions	**2,303**	1,745

Accounting policy

Liabilities for short-term employee benefits and termination benefits expected within 12 months of the end of reporting period are measured at their nominal amounts.

Leave

The liability for employee benefits includes provision for annual leave and long service leave.

The leave liabilities are calculated on the basis of employees' remuneration at the estimated salary rates that will be applied at the time the leave is taken, including the OAIC's employer superannuation contribution rates to the extent that the leave is likely to be taken during service rather than paid out on termination.

The liability for long service leave has been determined by reference to the work of an actuary performed for the Department of Finance (DoF) and summarised in the Standard Parameters for use in 2018–19 Financial Statements published on the DoF website. The estimate of the present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

Separation and redundancy

Provision is made for separation and redundancy benefit payments. The OAIC recognises a provision for termination when it has developed a detailed formal plan for the terminations and has informed those employees affected that it will carry out the terminations.

Accounting policy (continued)

Superannuation

The OAIC's staff are members of the Commonwealth Superannuation Scheme (CSS), the Public Sector Superannuation Scheme (PSS), or the PSS accumulation plan (PSSap), or other superannuation funds held outside the Australian Government.

The CSS and PSS are defined benefit schemes for the Australian Government. The PSSap is a defined contribution scheme.

The liability for defined benefits is recognised in the financial statements of the Australian Government and is settled by the Australian Government in due course. This liability is reported in DoF's schedules and notes.

The OAIC makes employer contributions to the employees' defined benefit superannuation scheme at rates determined by an actuary to be sufficient to meet the current cost to the Government. The OAIC accounts for the contributions as if they were contributions to defined contribution plans.

The liability for superannuation recognised as at 30 June represents outstanding contributions for the final fortnight of the financial year.

Accounting judgements and estimates

The long service leave has been estimated in accordance with the FRR taking into account expected salary growth, attrition and future discounting using the government bond rate.

4.2 Key management personnel remuneration

Key management personnel are those persons having authority and responsibility for planning, directing and controlling the activities of the OAIC, directly or indirectly, including any director (whether executive or otherwise) of the OAIC. The OAIC has determined the key management personnel to be the Australian Information Commissioner and Deputy Commissioner. Key management personnel remuneration is reported in the table below:

	2019 $'000	2018 $'000
Short-term employee benefits	**879**	1,184
Post-employment benefits	**101**	169
Other long-term employee benefits	**25**	23
Termination benefits	**–**	393
Total key management personnel remuneration expenses[1]	**1,005**	1,769

The total number of key management personnel that are included in the above table is 4 (2018: 4).

1 The above key management personnel remuneration excludes the remuneration and other benefits of the Portfolio Minister. The Portfolio Minister's remuneration and other benefits are set by the Remuneration Tribunal and are not paid by the entity.

4.3 Related party disclosures

Related party relationships

The OAIC is an Australian Government controlled entity. Related parties to this entity are key management personnel including the Portfolio Minister and Cabinet and Executive, and other Australian Government entities.

Transactions with related parties

Given the breadth of Government activities, related parties may transact with the government sector in the same capacity as ordinary citizens. Such transactions include the payment or refund of taxes, receipt of a Medicare rebate or higher education loans. These transactions have not been separately disclosed in this note.

The following transactions with related parties occurred during the financial year.

Significant transactions with related parties can include:

- the payments of grants or loans
- purchases of goods and services
- asset purchases, sales transfers or leases
- debts forgiven; and
- guarantees.

Giving consideration to relationships with related entities, and transactions entered into during the reporting period by the entity, it has been determined that there are no related party transactions to be separately disclosed.

Managing uncertainties

This section analyses how the OAIC manages financial risks within its operating environment.

5.1 Contingent assets and liabilities

Quantifiable contingencies

As at 30 June 2018 the OAIC had no quantifiable contingent liabilities.

Unquantifiable contingencies

As at 30 June 2019 the Australian Information Commissioner (AIC) was a respondent to three (3) matters in the Federal Court of Australia and a respondent in one matter in the Federal Circuit Court.

The four (4) matters before the federal courts in which the AIC was a respondent are *Administrative Decisions (Judicial Review) Act 1977* reviews of decisions to finalise privacy complaints and Information Commissioner reviews on FOI requests.

Although the federal courts may award costs, the AIC's exposure to a costs order is highly unlikely in all matters, based on current legal advice. It is not possible to estimate the amounts of payment(s) that may be required in relation to the matters where a costs order may materialise at the conclusion of the matter.

The AIC is also a respondent to four matters in the Administrative Appeals Tribunal, one (1) of which is in relation to a determination made by the AIC under s 52 of the *Privacy Act 1988*, one (1) of which is in relation to a direction given by the AIC under s 26WR of the *Privacy Act 1988*, one (1) of which was relation to a declaration made by the AIC under s 89K of the *Freedom of Information Act 1982*, and one (1) other in relation to an FOI request decision made by the OAIC. However, as the Tribunal is a 'no costs' jurisdiction consideration of contingent liabilities is not necessary in these matters.

Accounting policy

Contingent liabilities and contingent assets are not recognised in the statement of financial position but are reported in the notes. They may arise from uncertainty as to the existence of a liability or asset or represent an asset or liability in respect of which the amount cannot be reliably measured. Contingent assets are disclosed when settlement is probable but not virtually certain and contingent liabilities are disclosed when settlement is greater than remote.

5.2 Financial instruments

	2019 $'000	2018 $'000
5.2A: Categories of financial instruments		
Financial assets under AASB 139		
Receivables		
Cash on hand and at bank		589
Trade and other receivables		651
Total receivables		589
Total financial assets		589
Financial assets under AASB 9		
Financial assets at amortised cost		
Cash on hand and at bank	**601**	
Trade and other receivables	**698**	
Total financial assets at amortised cost	**1,299**	
Total financial assets	**1,299**	
Financial liabilities		
Financial liabilities measured at amortised cost		
Trade creditors and accruals	**1,131**	1,174
Total financial liabilities measured at amortised cost	**1,131**	1,174
Total financial liabilities	**1,131**	1,174

5.2 Financial instruments (continued)

Classification of financial assets on the date of initial application of AASB 9

Financial assets class	Note	AASB 139 original classification	AASB 9 new classification	AASB 139 carrying amount at 1 July 2018 $'000	AASB 9 carrying amount at 1 July 2018 $'000
Cash and cash equivalents	3.1A	Held-to-maturity	Amortised cost	**589**	589
Trade and other receivables	3.1B	Held-to-maturity	Amortised cost	**651**	651
Total financial assets				**1,240**	1,240

Reconciliation of carrying amounts of financial assets on the date of initial application of AASB 9

	AASB 139 carrying amount at 30 June 2018 $'000	Reclassification $'000	Remeasurement $'000	AASB 9 carrying amount at 1 July 2018 $'000
Financial assets at amortised cost				
Held to maturity				
Cash and cash equivalents	**589**	–	–	**589**
Loans and receivables				
Trade and other receivables	**651**	–	–	**651**
Total amortised cost	**1,240**	–	–	**1,240**

1 There is no change in the carrying amounts based on measurements under AASB 139 and transition to AASB 9.

Accounting policy

Financial assets

With the implementation of AASB 9 Financial Instruments for the first time in 2019, the entity classifies its financial assets in the following categories:

a) financial assets at fair value through profit or loss

b) financial assets at fair value through other comprehensive income

c) financial assets measured at amortised cost.

The classification depends on both the entity's business model for managing the financial assets and contractual cash flow characteristics at the time of initial recognition. Financial assets are recognised when the entity becomes a party to the contract and, as a consequence, has a legal right to receive or a legal obligation to pay cash and derecognised when the contractual rights to the cash flows from the financial asset expire or are transferred upon trade date.

Comparatives have not been restated on initial application.

Financial assets at amortised cost

Financial assets included in this category need to meet two criteria:

1. The financial asset is held in order to collect the contractual cash flows; and
2. The cash flows are solely payments of principal and interest (SPPI) on the principal outstanding amount.

Amortised cost is determined using the effective interest method.

Effective interest method

Income is recognised on an effective interest rate basis for financial assets that are recognised at amortised cost.

Financial assets at fair value through other comprehensive income (FVOCI)

Financial assets measured at fair value through other comprehensive income are held with the objective of both collecting contractual cash flows and selling the financial assets and the cash flows meet the SPPI test.

Any gains or losses as a result of fair value measurement or the recognition of an impairment loss allowance is recognised in other comprehensive income.

Financial assets at fair value through profit or loss (FVTPL)

Financial assets are classified as financial assets at fair value through profit or loss where the financial assets either doesn't meet the criteria of financial assets held at amortised cost or at FVOCI (i.e. mandatorily held at FVTPL) or may be designated.

Financial assets at FVTPL are stated at fair value, with any resultant gain or loss recognised in profit or loss. The net gain or loss recognised in profit or loss incorporates any interest earned on the financial asset.

Accounting policy (continued)

Impairment of financial assets

Financial assets are assessed for impairment at the end of each reporting period based on expected credit losses, using the general approach which measures the loss allowance based on an amount equal to *lifetime expected credit losses* where risk has significantly increased, or an amount equal to *12-month expected credit losses* if risk has not increased.

The simplified approach for trade, contract and lease receivables is used. This approach always measures the loss allowance as the amount equal to the lifetime expected credit losses.

A write-off constitutes a derecognition event where the write-off directly reduces the gross carrying amount of the financial asset.

Financial liabilities

Financial liabilities are classified as either financial liabilities 'at fair value through profit or loss' or other financial liabilities. Financial liabilities are recognised and derecognised upon 'trade date'.

Financial liabilities at fair value through profit or loss

Financial liabilities at fair value through profit or loss are initially measured at fair value. Subsequent fair value adjustments are recognised in profit or loss. The net gain or loss recognised in profit or loss incorporates any interest paid on the financial liability.

Financial liabilities at amortised cost

Financial liabilities, including borrowings, are initially measured at fair value, net of transaction costs. These liabilities are subsequently measured at amortised cost using the effective interest method, with interest expense recognised on an effective interest basis.

Supplier and other payables are recognised at amortised cost. Liabilities are recognised to the extent that the goods or services have been received (and irrespective of having been invoiced).

5.3 Fair value measurement

The following tables provide an analysis of assets and liabilities that are measured at fair value.

The different levels of the fair value hierarchy are defined below.

Level 1: Quoted prices (unadjusted) in active markets for identical assets or liabilities that the entity can access at measurement date.

Level 2: Inputs other than quoted prices included within Level 1 that are observable for the asset or liability, either directly or indirectly.

Level 3: Unobservable inputs for the asset or liability.

Accounting policy

The OAIC considers the fair value hierarchy levels at the end of the reporting period. There were no transfers in or out of any levels during the reporting period.

5.3: Fair value measurement (continued)

	Fair value measurements at the end of the reporting period			
	2019 $'000	2018 $'000	Category (Level 1, 2 or 3)	Valuation technique(s) and inputs used
Non-financial assets[1]				
Infrastructure, plant and equipment	**643**	977	2	Market approach. Market replacement cost less estimate of written down value of asset used.

1. There was non non-financial assets where the highest and best use differed from its current use during the reporting period.

Other information

6.1 Aggregate assets and liabilities

6.1A: Aggregate assets and liabilities

	2019 $'000	2018 $'000
Assets expected to be recovered in:		
No more than 12 months	**5,010**	5,151
Total assets	**5,010**	5,151
Liabilities expected to be settled in:		
No more than 12 months	**3,378**	3,279
More than 12 months	**784**	893
Total liabilities	**4,162**	4,172

Part 5
Appendices

Appendix A: Agency resource statement and resources for outcomes

Table A.1: OAIC resource statement 2018–19*

		Actual available appropriation for 2018–19 ($'000)	Payments made 2018–19 ($'000)	Balance remaining for 2018–19 ($'000)
		(a)	(b)	(a) – (b)
Ordinary annual services†				
Departmental appropriation		19,624	16,550	3,074
Total		**19,624**	**16,550**	**3,074**
Administered expenses				
Total ordinary annual services	**A**	**19,624**	**16,550**	
Other services				
Administered expenses		–	–	
Departmental non-operating		–	–	–
Equity injections‡		860	160	700
Administered non-operating				
Total other services	**B**	**860**	**160**	**700**
Total available annual appropriations and payments		**20,484**	**16,710**	**3,774**
Special appropriations		–	–	
Total special appropriations	**C**			
Special accounts		–	–	
Total special accounts	**D**	**–**	–	
Total resourcing and payments A + B + C + D		**20,484**	**16,710**	

	Actual available appropriation for 2018–19 ($'000)	Payments made 2018–19 ($'000)	Balance remaining for 2018–19 ($'000)
	(a)	(b)	(a) – (b)
Less appropriations drawn from annual or special appropriations above and credited to special accounts	–	–	
And/or payments to corporate entities through annual appropriations	–	–	
Total net resourcing and payments for the OAIC	**20,484**	**16,710**	

* All figures are GST exclusive.

† *Appropriation Act (No.1) 2018–2019*. Includes prior year departmental appropriation and *Public Governance, Performance and Accountability Act 2013* (PGPA Act 2013), s 74 retained revenue receipts.

‡ *Appropriation Act (No.2) 2018–2019*.

Table A.2: OAIC resource statement 2018–19

	Budget 2018–19 ($'000)	Actual expenses 2018–19 ($'000)	Variation 2018–19 ($'000)
	(a)	(b)	(a) – (b)
Outcome 1 Provision of public access to Commonwealth Government information, protection of individuals' personal information, and performance of Information Commissioner, freedom of information and privacy functions			
Program 1.1 Complaint handling, compliance and monitoring, and education and promotion			
Administered expenses	–	–	–
Departmental expenses			
Departmental appropriation*	16,162	16,621	(459)
Special appropriations	–	–	–
Special accounts	–	–	–
Expenses not requiring appropriation in the Budget year	432	464	(32)
Total for program 1.1	**16,594**	**17,085**	**(491)**
Outcome 1 totals by appropriation type			
Administered expenses	–	–	–
Departmental expenses			
Departmental appropriation*	16,162	16,621	(459)
Special appropriations	–	–	–
Special accounts	–	–	–
Expenses not requiring appropriation in the Budget year	432	464	(32)
Total expenses for outcome 1	**16,594**	**17,085**	**(491)**
	2018–19	**2018–19**	
Average staffing level (number)	93	85.3	7.7

* Departmental appropriation combines ordinary annual services (Appropriation Act No. 1) and PGPA Act 2013, s 74 retained revenue receipts.

Appendix B: Executive remuneration

This appendix contains information about the remuneration of the Office Australian Information Commissioner's (OAIC) key management personnel and Senior Executive Service.

Key management personnel

The OAIC has determined that our key management personnel (KMP) are the Australian Information Commissioner and the Deputy Commissioner. Ms Angelene Falk held the position of Australian Information Commissioner for the duration of the reporting period. Ms Falk initially acted in the position until her formal appointment on 16 August 2019.

Mr Andrew Solomon and Ms Melanie Drayton were acting in the Deputy Commissioner's role from the commencement of the reporting period to 6 February 2019. On 14 January 2019 Ms Elizabeth Hampton was appointed to the substantive position.

Details of KMP remuneration are in Note 4.2 of the financial statements. Disaggregated information is shown in Table B.1 and is prepared in accordance with the *Public Governance, Performance and Accountability Rule 2014* (PGPA Rule) and *Commonwealth Entities Executive Remuneration Reporting Guide for Annual Reports, Resource Management Guide No. 13*8 (RMG 138).

Senior Executive Service

The OAIC has three substantive Senior Executive Service (SES) positions including the Deputy Commissioner; the Assistant Commissioner, Dispute Resolution; and the Assistant Commissioner, Regulation and Strategy.

Table B.2 is prepared in accordance with the PGPA Rule and RMG 138 and provides the average annual reportable remuneration for substantive SES.

Remuneration policies and practices

In accordance with s 17 of the *Australian Information Commissioner Act 2010*, the Australian Information Commissioner's remuneration is set by the Remuneration Tribunal. The Remuneration Tribunal also determine increases to remuneration or allowances.

The OAIC's SES remuneration is determined by the Australian Information Commissioner under s 24(1) of the *Public Service Act 1999*. When determining SES remuneration, the Australian Information Commissioner has regard to the Australian Public Service Commission's Australian Public Service Remuneration Report and comparable agencies.

SES determinations set out the salary on commencement and provide for increments in salary, in line with any percentage up to 5% set by the Remuneration Tribunal for the Australian Information Commissioner.

To be eligible for an increase in salary an SES officer must obtain an annual performance rating of effective or above. The OAIC's performance management framework, Talking About Performance, enables SES officers performance agreements. The agreement objectives are directly linked to the SES officer's business line responsibilities of the OAIC's Corporate Plan.

The Australian Information Commissioner sets and reviews the Deputy Commissioner's performance agreement. The Deputy Commissioner sets and reviews Assistant Commissioners' performance agreements.

Remuneration governance arrangements

As a small agency, the Australian Information Commissioner is responsible for setting and monitoring remuneration for the OAIC's SES officers.

Table B.1: KMP remuneration

		Short-term benefits			Post-employment benefits	Other long-term benefits			
Name	**Position title**	**Base salary ($)**	**Bonuses ($)**	**Other benefits and allowances ($)**	**Superannuation contributions ($)**	**Long service leave ($)**	**Other long-term benefits ($)**	**Termination benefits ($)**	**Total remuneration ($)**
Angelene Falk	Australian Information Commissioner	449,986	–	Nil	34,292	10,599	–	–	494,877
Elizabeth Hampton	Deputy Commissioner	130,723	–	4,524*	22,436	3,004	–	–	160,687
Andrew Solomon	Acting Deputy Commissioner	162,093	–	397†	24,877	6,397	–	–	193,764
Melanie Drayton	Acting Deputy Commissioner	131,124	–	Nil	19,661	5,118	–	–	155,903
Total		**873,927**	**–**	**4,921**	**101,266**	**25,118**	**–**	**–**	**1,005,232**

* $4,524 for travel allowance.

† $397 for motor vehicle allowance.

Table B.2: Average SES remuneration

		Short-term benefits			Post-employment benefits	Other long-term benefits		Termination benefits	Total remuneration
Remuneration band	Number of senior executives	Average base salary ($)	Average bonuses ($)	Average other benefits and allowances ($)	Average superannuation contributions ($)	Average long service leave ($)	Average other long-term benefits ($)	Average termination benefits ($)	Average total remuneration ($)
$0 – $220,000	2*	76,300	–	–	13,961	4,763	–	–	95,024†

* Represents total number of substantive SES positions and excludes individuals partially assigned to SES responsibilities.

† Excludes KMP remuneration, which is shown in Table B.1.

Appendix C: Memoranda of understanding

Australian Digital Health Agency

Under our Memorandum of Understanding (MOU) with the Australian Digital Health Agency we continued to provide support and assistance on privacy matters relating to both the Healthcare Identifiers Service and My Health Record system. These services included:

- responding to enquiries and complaints relating to the privacy aspects of the My Health Record system
- investigating acts and practices that may have been a misuse of healthcare identifiers or a contravention of the My Health Record system, if required
- receiving data breach notifications and providing advice
- conducting privacy assessments
- providing guidance material for individuals and participants in the My Health Record system
- liaising and coordinating on privacy-related matters and activities with key stakeholders
- preparing relevant communication materials
- providing policy and legislation advice relating to the privacy aspects of the Health Identifiers Service and My Health Record System
- monitoring and participating in digital health developments.

During this reporting period, the Office of the Australian Information Commissioner received $1,626,023.40 (GST exclusive).

For further information on our activities under this MOU, see the *Annual Report of the Australian Information Commissioner's Activities in Relation to Digital Health 2018–19* (available on our website no later than 28 November 2019).

Australian Human Rights Commission

The Australian Human Rights Commission (AHRC) continued to provide a number of corporate services to our office this year, including financial, administrative, information technology and human resource related tasks. We also sublet premises in Sydney from the AHRC.

For the corporate services we paid $916,956.72 (GST exclusive) and for the premises (including outgoings) we paid $1,083,040.92 (GST exclusive) to the AHRC.

Australian Capital Territory Government

In 2018 we entered into a new MOU with the Australian Capital Territory (ACT) Government to continue to provide privacy services to ACT public sector agencies. These services included:

- responding to privacy complaints and enquiries about ACT public sector agencies in relation to the *Information Privacy Act 2014* (ACT) and its Territory Privacy Principles
- providing policy and legislation advice
- providing advice on data breach notifications, where applicable
- carrying out a privacy assessment
- providing access to our Privacy Professional Network meetings.

For these services, we received $177,500 (GST exclusive) from the ACT Government.

For further information on our activities under this MOU, see the *Memorandum of Understanding with the Australian Capital Territory for the Provision of Privacy Services 2018–19 Annual Report* (available on our website no later than 22 October 2019).

Department of Education and Training

In July 2018 we entered into a new MOU to continue to support the Department of Education and Training (now the Department of Education) with their student identifier initiative, providing expert and timely advice on privacy matters. Our services to the department included:

- developing the content for four editions of the TRANSPARENT privacy newsletter for publication on the Unique Student Identifier website
- responding to any enquiries and complaints relating to the privacy aspects of the Student Identifier initiative
- conducting a webinar on privacy matters for registered training organisations
- giving a presentation on privacy matters at a vocational education conference
- conducting a privacy assessment of the Unique Student Identifier Transcript Service.

For these services, we received $100,000 (GST exclusive).

Department of Home Affairs

In November 2017, the Attorney-General's Department and the OAIC signed an MOU for the provision of privacy assessments in relation to the National Facial Biometric Matching Capability (NFBMC).

On 20 December 2017, the Department of Home Affairs assumed responsibility for the NFBMC as part of Machinery of Government changes and subsequently assumed responsibility for the roles and responsibilities under the MOU.

In February 2018, the Identity-matching Services Bill 2018 was introduced into Parliament but was not passed, so our privacy assessments have been deferred to later financial years. In May 2019 we signed a variation to the MOU to defer commencing privacy assessments and associated payments for two years.

Appendix D: Privacy statistics

Privacy complaints

Table D.1: Australian Privacy Principles (APP) issues in privacy complaints in 2018–19

AAP issue*	Number of complaints	% of total
Use or disclosure of personal information (APP 6)	973	29.46
Security of personal information (APP 11)	780	23.61
Access to personal information (APP 12)	480	14.53
Collection of solicited personal information (APP 3)	426	12.90
Quality of personal information (APP 10)	321	9.72
Direct marketing (APP 7)	160	4.84
Notification of the collection of personal information (APP 5)	93	2.82
Correction of personal information (APP 13)	46	1.39
Open and transparent management of personal information (APP 1)	23	0.70
Dealing with unsolicited personal information (APP 4)	9	0.27
Anonymity and pseudonymity (APP 2)	6	0.18
Cross-border disclosure of personal information (APP 8)	6	0.18
Adoption, use or disclosure of government related identifiers (APP 9)	2	0.06

* A complaint may cover more than one issue.

Table D.2: The main remedies agreed in conciliated privacy complaints in 2018–19

	Jurisdiction				
Remedy*	**Privacy principles†**	**Credit reporting**	**Spent convictions and tax file number**	**My Health Records**	**Total**
Record amended	267	82	1	13	363
Access provided	196	9	–	–	205
Other or confidential	169	8	–	18	195
Apology	181	3	5	3	192
Compensation	111	6	1	–	118
Changed procedures	100	1	2	1	104
Staff training or counselling	93	–	4	–	97

* A resolved complaint may involve more than one type of remedy.

† Includes APPs, National Privacy Principles and the Australian Capital Territory's Territory Privacy Principles.

Table D.3: Compensation amounts in closed privacy complaints in 2018–19

	Jurisdiction			
Compensation amount	**Privacy principles***	**Credit reporting**	**Tax file number**	**Total**
Up to $1,000	31	3	–	34
$1,001 to $5,000	56	3	1	60
$5,001 to $10,000	15	–	–	15
Over $10,001	9	–	–	9

* Only includes APP complaints.

Privacy assessments and digital health assessments

Table D.4: Privacy assessments in 2018–19

	Privacy assessment subject	Number of entities assessed	Year opened	Date closed
1	Department of Home Affairs (previously the Department of Immigration and Border Protection (DIBP)) — third-party provider for advance passenger processing	1	2016–17	November 2018
2	Loyalty program	2	2016–17	June 2019
3	Department of Home Affairs (previously DIBP) — passenger name record	1	2016–17	Ongoing
4	Data retention scheme — telecommunications service provider 1	1	2017–18	November 2018
5	Data retention scheme — telecommunications service provider 2	1	2017–18	Ongoing
6	Department of Home Affairs (previously DIBP) — connected information environment	1	2017–18	Ongoing
7	ACT Government — ACT Housing	1	2017–18	Ongoing
8	Privacy policy assessment of finance sector organisations	20	2018–19	January 2019
9	Follow up of loyalty programs	2	2018–19	June 2019
10	Data retention scheme — telecommunications service provider 3	1	2018–19	Ongoing
11	Data retention scheme — telecommunications service provider 4	1	2018–19	Ongoing
12	Unique Student Identifier Transcript Service	1	2018–19	Ongoing
13	ACT Government	10	2018–19	Ongoing

Table D.5: Digital health assessments in 2018–19

Privacy assessment subject	Number of entities assessed	Year opened	Date closed
Handling of individual healthcare identifiers by a private healthcare operator	1	2017–18	Ongoing
Australian Digital Health Agency — handling of personal information	1	2017–18	Ongoing
Access security governance for the My Health Record system — pharmacies	14	2018–19	Ongoing
Access security governance for the My Health Record system — pathology and diagnostic imaging services	8	2018–19	Ongoing
Access security governance for the My Health Record system — private hospitals	2	2018–19	Ongoing

Table D.6: Enhanced welfare payment integrity (data matching) assessments

Privacy assessment subject	Number of entities assessed	Year opened	Date closed
Department of Human Services non-employment income data matching (NEIDM) program	1	2017–18	June 2019
Department of Human Services Pay-As-You-Go (PAYG) data-matching program	1	2017–18	Ongoing
Department of Human Services — information security for the NEIDM and PAYG programs	1	2017–18	Ongoing
Australian Taxation Office — information security as a data source for the Department of Human Services	1	2018–19	Ongoing

Appendix E: FOI statistics

This appendix contains information regarding:

- requests for access to documents
- applications for amendment of personal records
- charges
- disclosure logs
- review of freedom of information (FOI) decisions
- complaints about agency FOI actions
- the impact of FOI on agency resources
- the impact of Information Publication Scheme (IPS) on agency resources.

It has been prepared using data collected from Australian Government agencies and ministers subject to the *Freedom of Information Act 1982* (FOI Act), and separately from the Administrative Appeals Tribunal (AAT) and the Office of the Australian Information Commissioner's (OAIC) own records. Australian Government agencies and ministers are required to provide, among other details, information about:

- the number of FOI requests made to them
- the number of decisions they made granting, partially granting or refusing access, and the number and outcome of applications for internal review
- the number and outcome of requests to them to amend personal records
- charges collected by them.[1]

The data given by ministers and agencies for the preparation of this appendix is published on data.gov.au.[2]

1 Australian Government ministers and agencies, and Norfolk Island authorities, are required by s 93 of the FOI Act and r 8 of the *Freedom of Information (Prescribed Authorities, Principal Offices and Annual Report) Regulations 2017* to submit statistical returns to the OAIC every quarter and provide a separate annual report on FOI and IPS costs.

2 The data reported in this appendix has been rounded to two decimal places.

Requests for access to documents

Types of FOI requests

The term 'FOI request' means a request for access to documents made under s 15 of the FOI Act. Applications for amendment or annotation of personal records under s 48 are dealt with separately below.

A request for personal information means a request for documents that contain information about a person who can be identified (usually the applicant, although not necessarily). A request for 'other' information means a request for all other documents, such as documents concerning policy development or government decision-making.

The FOI Act requires that agencies and ministers provide access to documents in response to requests that meet the requirements of s 15 of the FOI Act. The figures in this report do not take account of applications that did not satisfy those requirements.

Number of FOI requests received

Table E.1 provides a comparison of the number of FOI requests received in each of the past five reporting years, including the percentage increase or decrease from the previous financial year.

Table E.1: FOI requests received over the past five years

	2014–15	2015–16	2016–17	2017–18	2018–19
Number of FOI requests received	35,550	37,966	39,519	34,438	38,879
% change from previous financial year	+24.90%	+6.88%	+4.01%	-12.86%	+12.90%

The number of FOI requests made to Australian Government agencies increased by 12.90% in 2018–19. The number of FOI requests received over the past five years has varied considerably from year to year largely driven by significant changes in the number of requests for personal information received each year.

The increase in the overall number of FOI requests in 2018–19, was principally driven by a significant increase in the number of FOI requests for personal information received by the Department of Home Affairs (+24.18%). The Department of Home Affairs receives the most FOI requests of any Australian Government agency, with the bulk of those being personal information requests, so any increase (or decrease) in request numbers to that agency influences overall FOI request numbers across the Australian Government.

In 2018–19, 32,440 FOI requests (or 83.44% of all requests received) were for documents containing personal information. This is a higher proportion than in 2017–18 (81.88%) and 2016–17 (81.94), but a lesser proportion than in 2015–16 (86.55%).

In 2018–19, there were 6,439 FOI requests (or 16.56% of all requests) for 'other' information. This is a lower proportion than in 2017–18 (18.12%) and 2016–17 (18.06%), but an increase when compared with 2015–16 (13.45%).

Number of FOI requests received by an agency or minister

The Governor-General authorised three Administrative Arrangements Orders (AAOs) in 2018–19: on 28 August 2018, 4 April 2019 and 29 May 2019. These AAOs changed the functions and administrative responsibilities of some agencies and resulted in changes to the number and composition of FOI requests received by affected agencies during the year.

In 2018–19, the Department of Home Affairs, the Department of Human Services (DHS)[3] and the Department of Veterans' Affairs (DVA) together continued to receive the majority of FOI requests received by Australian Government agencies (69.13% of the total). Nearly all of these requests (95.19%) are from individuals seeking access to personal information.

The 20 agencies that received the largest number of requests in 2018–19 are shown in Table E.2, with a comparison to the number of requests each of those agencies received in 2017–18.

Although the Department of Home Affairs received 24.18% more personal FOI requests in 2018–19 than in the previous financial year (from 13,557 to 16,828), it experienced a 44.68% increase in 'other' FOI requests (from 620 in 2017–18 to 897 in 2018–19). The increased number of FOI requests, for both personal and other information, may reflect the increased number of functions for which the Department of Home Affairs is responsible for due to the AAOs during the year, and an increased interest in the policies and operations of the Department of Home Affairs.

However, trends in FOI request numbers are not uniform across the Australian Government. For example, other agencies in the top five agencies either received fewer FOI requests this financial year (the DVA experienced a 9.75% decrease) or experienced modest increases (4.87% for the AAT and 2.95% for the Australian Taxation Office (ATO)). The DHS received a similar number of FOI requests to 2017–18 (6,210 compared with 6,238 in 2017–18).

3 Although the AAO of 29 May 2019 changed the name of DHS to Services Australia, DHS has not yet implemented this change and has been referred to as the DHS throughout this report.

Some agencies in the top 20 agencies experienced increases in FOI request numbers far exceeding the overall increase of 12.90%. For example, the Australian Postal Corporation (170.69%), the National Disability Insurance Agency (155.66%) and our own agency, the OAIC (a 171.11% increase).

There was also variance across government in the number and proportion of personal and other information FOI requests in 2018–19.

While the DVA experienced a decline in overall request numbers in 2018–19, there was a 129% increase in other information FOI requests (from 62 in 2017–18 to 142 this year) and for the ATO, it experienced a 28.32% decline in other information FOI requests in 2018–19, in the context of a 2.95% overall increase in request numbers.

Two agencies in last year's top 20 agencies experienced decreases in the numbers of FOI requests received in 2018–19 and no longer appear in the top 20 agencies: the Department of Jobs and Small Business[4] (a 32.42% decrease) and the Commonwealth Ombudsman (a 32.63% reduction).

4 As a result of the AAO issued on 29 May 2019, the Department of Jobs and Small Business is now called the Department of Employment, Skills, Small and Family Business.

Table E.2: Agencies by number of FOI requests received

	2017–18					2018–19					
Agency	Rank	Personal	Other	Total	% of all FOI requests	Rank	Personal	Other	Total	% of all FOI requests	Change in total
Department of Home Affairs	1	13,557	620	14,177	41.17	1	16,828	897	17,725	45.59	3,548
Department of Human Services	2	6,008	230	6,238	18.11	2	5,955	255	6,210	15.97	-28
Department of Veterans' Affairs	3	3,199	62	3,261	9.47	3	2,801	142	2,943	7.57	-318
Administrative Appeals Tribunal	4	1,445	13	1,458	4.23	4	1,519	10	1,529	3.93	71
Australian Taxation Office	5	862	392	1,254	3.64	5	1,010	281	1,291	3.32	37
National Disability Insurance Agency	11	270	57	327	0.95	6	782	54	836	2.15	509
Australian Federal Police	6	473	209	682	1.98	7	588	138	726	1.87	44
Immigration Assessment Authority	7	536	–	536	1.56	8	512	–	512	1.32	-24
Australian Transaction Reports and Analysis Centre	9	248	168	416	1.21	9	264	245	509	1.31	93

Table E.2: Agencies by number of FOI requests received (continued)

Agency	2017–18 Rank	Personal	Other	Total	% of all FOI requests	2018–19 Rank	Personal	Other	Total	% of all FOI requests	Change in total
Department of Defence	8	185	308	493	1.43	10	166	275	441	1.13	-52
Department of Health	10	2	374	376	1.09	11	62	372	434	1.12	58
Comcare	14	155	73	228	0.66	12	181	179	360	0.93	132
Attorney-General's Department	18	50	135	185	0.54	13	215	121	336	0.86	151
Australian Securities and Investments Commission	16	77	141	218	0.63	14	122	174	296	0.76	78
Office of the Australian Information Commissioner*	–	35	55	90	0.26	15	150	94	244	0.63	154
Department of Foreign Affairs and Trade	13	97	173	270	0.78	16	90	147	237	0.61	-33
Department of Education†	19	55	127	182	0.53	17	95	140	235	0.61	53
Department of the Environment and Energy*	–	–	123	123	0.36	18	–	234	234	0.60	111
Department of the Prime Minister and Cabinet	12	5	271	276	0.80	19	1	169	170	0.44	-106

Table E.2: Agencies by number of FOI requests received (continued)

Agency	2017–18 Rank	2017–18 Personal	2017–18 Other	2017–18 Total	2017–18 % of all FOI requests	2018–19 Rank	2018–19 Personal	2018–19 Other	2018–19 Total	2018–19 % of all FOI requests	Change in total
Australian Postal Corporation*	–	42	58	100	0.29	20	116	41	157	0.40	57
Total top 20	**–**	**27,301‡**	**3,589‡**	**30,890‡**	**89.69**	**–**	**31,457**	**3,968**	**35,425**	**91.12**	**4,268**
Remaining agencies	–	898	2,650	3,548	10.31	–	983	2,471	3,454	8.88	5.24
Total	**–**	**28,199**	**6,239**	**34,438**	**100.0**	**–**	**32,440**	**6,439**	**38,879**	**100.0**	

* Denotes an agency not in the top 20 agencies in 2017–18.

† Denotes an agency whose name or functions changed as a result of AAOs issued on 28 August 2018, 4 April 2019 and 29 May 2019. For example, the Department of Education was formerly the Department of Education and Training, and see footnote 3 about DHS's change of name.

‡ Shows the total for the top 20 agencies in 2017–18 (that is, includes figures for three agencies not in the top 20 agency list in 2018–19).

FOI requests finalised

Agencies and ministers commenced 2018–19 with significantly fewer FOI requests on hand requiring a decision than the previous financial year (47.32% fewer than at the beginning of 2017–18) (Table E.3).

There was a large increase in the number of FOI requests withdrawn by applicants (39.26% more than in 2017–18), a large increase in FOI requests received during this reporting period (12.90%) and a slight reduction in the number of requests decided (4.83% less than in 2017–18). At the end of the financial year, there were 30.31% more requests on hand than at the beginning of the financial year (4,317).

Reasons for the higher number of requests being withdrawn during this reporting period may include:

- increased referral to, or use of, administrative access to provide access to documents outside the FOI Act
- documents already being available on agency disclosure logs or published on agency IPS entries or in annual reports
- applicants accepting verbal assurances that no documents exist within the scope of their request
- requests sent to the wrong agency in the first instance which are then withdrawn and sent to the correct agency.[5]

Despite three AAOs during 2018–19, the number of requests transferred from one agency or minister to another in 2018–19 remained stable, with 639 transferred in 2018–19, compared with 641 in 2017–18.

5 Although an agency or minister can transfer a wrongly directed FOI request under s 16(1) of the FOI Act, this can only be done with the agreement of the receiving agency. If the applicant makes the request directly to the agency, it must be processed.

Table E.3: Overview of FOI requests received and finalised

FOI request processing	2017–18	2018–19	% change
On hand at the beginning of the year	6,279	3,308	-47.32
Received during the year	34,438	38,879	+12.90
Requiring decision*	40,717	42,187	+3.61
Withdrawn	5,089	7,087	+39.26
Transferred	641	639	-0.31
Decided†	31,674	30,144	-4.83
Finalised‡	37,404	37,870	+1.25
On hand at the end of the year	3,313	4,317	+30.31

* Total of FOI requests on hand at the beginning of this reporting period and requests received during this reporting period.

† Covers access granted in full, part or refused.

‡ The sum of requests withdrawn, transferred and decided.

The percentage of requests granted in full increased in 2018–19, from 49.81% of all requests in 2017–18, to 51.83% in 2018–19 (Table E.4). Despite the increase during this reporting period, the figure is still lower that the 2016–17 figure of 55.47%.

The percentage of FOI requests granted in part was 34.97%; a rate similar to 2017–18 when 34% of all requests were granted in part (Table E.4). The number of FOI requests refused in 2018–19 (which includes requests refused because the documents sought do not exist or cannot be found or a practical refusal reason exists, as well as when exemptions have been applied) decreased from 16.19% in 2017–18 to 13.20% in 2018–19. Note that the number of requests refused in full in 2016–17 was only 9.95%.

Table E.5 lists the top 20 agencies by the number of FOI decisions made.

There are differences in the outcome of FOI requests between those agencies processing the largest number of requests in 2018–19. Eight of the top 20 agencies refused access to documents at levels higher than the average across all Australian Government agencies (37.3%). These agencies process proportionally higher numbers of other information FOI requests. Agencies processing higher proportions of FOI requests for personal information have higher rates of FOI requests granted in full than the Australian Government average (25.93%): for example, the DVA, the Department of Home Affairs, the DHS, the AAT and the Immigration Assessment Authority.

Table E.4: Outcomes of FOI requests decided

Decision	Personal 2017–18	Other 2017–18	Total 2017–18	%	Personal 2018–19	Other 2018–19	Total 2018–19	%
Granted in full*	14,889	889	15,778	49.81	14,577	1,046	15,623	51.83
Granted in part†	9,037	1,730	10,767	34.00	8,835	1,706	10,541	34.97
Refused	2,042	3,087	5,129	16.19	2,147	1,833	3,980	13.20
Total	**25,968**	**5,706**	**31,674**	**100**	**25,559**	**4,585**	**30,144**	**100**

* The release of all documents within the scope of the request, as interpreted by the agency or minister.

† A document is granted in part when a part, or parts, of a document have been redacted to remove any exempt or conditionally exempt matter.

Table E.5: Top 20 agencies by numbers of FOI requests decided in 2018–19

Agency	Granted in full	%	Granted in part	%	Refused	%	Total
Department of Home Affairs	9,395	59.93	5,375	34.28	908	5.79	15,678
Department of Veterans' Affairs	2,607	94.12	70	2.53	93	3.36	2,770
Department of Human Services	845	32.45	1,231	47.27	528	20.28	2,604
Australian Taxation Office	186	17.61	579	54.83	291	27.56	1,056
Administrative Appeals Tribunal	778	75.10	228	22.01	30	2.90	1,036
National Disability Insurance Agency	258	32.78	478	60.73	51	6.48	787
Australian Federal Police	43	6.02	481	67.37	190	26.61	714
Australian Transaction Reports and Analysis Centre	48	9.58	284	56.69	169	33.73	501
Immigration Assessment Authority	381	84.48	66	14.63	4	0.89	451
Department of Defence	54	16.02	187	55.49	96	28.49	337
Attorney-General's Department	116	41.13	46	16.31	120	42.55	282
Comcare	84	32.68	77	29.96	96	37.35	257
Australian Securities and Investments Commission	41	16.94	70	28.93	131	54.13	242

Table E.5: Top 20 agencies by numbers of FOI requests decided in 2018–19 (continued)

Agency	Granted in full	%	Granted in part	%	Refused	%	Total
Department of Health	54	24.11	83	37.05	87	38.84	224
Department of the Environment and Energy	15	9.20	112	68.71	36	22.09	163
Australian Postal Corporation	18	12.41	26	17.93	101	69.66	145
Commonwealth Ombudsman	28	20.44	56	40.88	53	38.69	137
Office of the Australian Information Commissioner	34	25.56	69	51.88	30	22.56	133
Department of the Treasury	29	22.66	35	27.34	64	50.00	128
Department of Prime Minister and Cabinet	22	18.80	38	32.48	57	48.72	117
Top 20	**15,036**	**54.16**	**9,591**	**34.55**	**3,135**	**11.29**	**27,762**
Remaining agencies	587	24.64	950	39.88	845	35.47	2,382
Total	**15,623**	**51.83**	**10,541**	**34.97**	**3,980**	**13.20**	**30,144**

Use of exemptions

Table E.6 shows how Australian Government agencies and ministers claimed exemptions under the FOI Act when processing FOI requests in 2018–19. More than one exemption may be applied in processing an FOI request.

Exemptions were not claimed or were not relevant in relation to 6,718 FOI requests decided in 2018–19 (22.29% of all FOI requests decided).

The personal privacy exemption (s 47F) remains the most claimed exemption. It was applied in 38.28% of all FOI requests in which exemptions were claimed in 2018–19. However, this is a decline in the use of s 47F from 42.68% in 2017–18 and 47.90% in 2016–17.

The next most claimed exemptions were s 47E (certain operations of agencies — 21.26%, up from 19.75% in 2017–18), s 37 (documents affecting enforcement of law and protection of public safety — 9.88%, a slight increase from 2017–18 when it accounted for 9.17% of all exemptions applied), s 38 (documents to which secrecy provisions apply — 6.77%, slightly up on 2016–17's 6.64%) and s 47C (deliberative processes — 6.51%, an increase on 2017–18 when it comprised 5.20% of all exemptions applied).

Overall there was very little change in the application of the remaining exemptions. The only exemption that showed any real difference in 2018–19, was s 47 (documents disclosing trade secrets or commercially valuable information) which comprised 1.34% of all exemptions applied, up from 0.93% in 2017–18.

Table E.6: Use of exemptions in FOI decisions in 2018–19

FOI Act reference	Exemption	Personal	Other	Total	% of all exemptions applied
s 33	Documents affecting national security, defence or international relations	578	159	737	4.85
s 34	Cabinet documents	3	126	129	0.85
s 37	Documents affecting enforcement of law and protection of public safety	1,322	179	1,501	9.88
s 38	Documents to which secrecy provisions of enactments apply	853	176	1,029	6.77
s 42	Documents subject to legal professional privilege	228	178	406	2.67
s 45	Documents containing material obtained in confidence	74	179	253	1.67
s 45A	Parliamentary Budget Office documents	1	1	2	0.01
s 46	Documents disclosure of which would be contempt of Parliament or contempt of court	31	7	38	0.25
s 47	Documents disclosing trade secrets or commercially valuable information	44	159	203	1.34
s 47A	Electoral rolls and related documents	5	–	5	0.03
s 47B	Commonwealth-state relations	98	90	188	1.24
s 47C	Deliberative processes	599	390	989	6.51

Table E.6: Use of exemptions in FOI decisions in 2018–19 (continued)

FOI Act reference	Exemption	Personal	Other	Total	% of all exemptions applied
s 47D	Financial or property interests of the Commonwealth	85	18	103	0.68
s 47E	Certain operations of agencies	2,550	680	3,230	21.26
s 47F	Personal privacy	4,979	836	5,815	38.28
s 47G	Business	189	368	557	3.67
s 47H	Research	–	3	3	0.02
s 47J	The economy	1	2	3	0.02

Use of practical refusal

Section 24AB of the FOI Act sets out that a 'request consultation process' must be undertaken if a 'practical refusal reason' exists (s 24AA). A practical refusal reason exists if the work involved in processing the FOI request would substantially and unreasonably divert the agency's resources from its other operations, or the FOI request does not adequately identify the documents sought.

The request consultation process involves the agency sending a written notice to the FOI applicant advising them that the agency intends to refuse the request and providing details of how the FOI applicant can consult the agency. The FOI Act imposes an obligation on the agency to take reasonable steps to help the FOI applicant revise their request so that the practical refusal reason no longer exists.

Table E.7 provides information about how Australian Government agencies and ministers engaged in request consultation processes under s 24AB of the FOI Act in 2018–19 and the outcome of those processes.

Table E.7: Use of practical refusal in 2018–19

Practical refusal processing step	Personal	Other	Total	%*
Notified in writing of intention to refuse request	1,381	844	2,225	–
Request was subsequently refused or withdrawn	1,137	572	1,709	76.81
Request was subsequently processed	244	272	516	23.19

* Percentage of the total number of notices advising of an intention to refuse a request for a practical refusal reason.

Agencies sent 47.25% fewer notices of an intention to refuse an FOI request for a practical refusal reason in 2018–19 than in 2017–18. However, 2017–18 was a year in which an unusually large number of notices were issued (a 163.28% increase over the previous financial year) due to the Northern Australia Infrastructure Facility refusing 1,332 FOI requests in 2017–18 for a practical refusal reason. This circumstance largely accounts for the number of notices issued in 2018–19 returning to the pre 2017–18 level.

In 2018–19, 76.81% of the FOI requests subject to a notice of intention to refuse a request were subsequently refused or withdrawn: the proportion was 84.25% in 2017–18 and 66% in 2016–17.

The lower the proportion of FOI requests subsequently refused or withdrawn after a practical refusal notice is issued, the better agencies have been in assisting applicants to revise the scope of their requests so they can be processed. Therefore, taking into account 2017–18 was an atypical year for practical refusal, there has been a significant deterioration in this statistic with less requests subsequently processed in 2018–19 than in 2016–17.

Four agencies issued 66.25% of all notices of an intention to refuse a request for a practical refusal reason in 2018–19: the Department of Home Affairs (792 notices), the DHS (489), the Australian Securities and Investments Commission (ASIC) (104), and the ATO (89).

The Department of Home Affairs issued 34.24% more notices of an intention to refuse a request in 2018–19, than in 2017–18 (when it issued 590) and the DHS issued 91.77% more (489 in 2018–19; 255 in 2017–18). However, the DHS (30.27%), ASIC (41.37%) and the ATO (40.45%) were all more likely to subsequently process an FOI request after issuing a notice of intention to refuse than the Department of Home Affairs (who subsequently processed only 2.27% of requests after a notice was issued).

In June 2019, the Information Commissioner issued a series of decisions under s 55K reviewing practical refusal decisions of agencies. These decisions provide additional guidance for agencies and ministers, in particular their obligation to assist applicants revise the scope of their requests so they can be processed. The OAIC hopes to see a decrease in the proportion of requests refused or withdrawn after a notice of intention to refuse a request is sent in 2019–20.[6]

Time taken to respond to FOI requests

Agencies and ministers have 30 days within which to make a decision under the FOI Act. The FOI Act allows for the timeframe to be extended in certain circumstances.[7]

If a decision is not made on an FOI request within the statutory timeframe (including any extension period) then s 15AC of the FOI Act provides that a decision refusing access is deemed to have been made. Nonetheless, agencies have an obligation to continue to process a request that has been deemed to be refused.

In 2018–19, 82.58% of all FOI requests determined were processed within the applicable statutory time period: 83.14% of all personal information requests and 79.83% of non-personal requests. This represents a slight decrease in timeliness of decision-making from 2017–18 (when 84.86% were decided within time).

The Department of Home Affairs compliance with statutory timeframes remained relatively stable at 74.16% in 2018–19 (it was 74.88% in 2017–18); however, this is a significant improvement over 2016–17, when only 25.22% of FOI requests to the Department of Home Affairs were finalised within the statutory time period.

A number of agencies that process substantial numbers of FOI requests decided them all within the statutory time period in 2018–19. These agencies include the Department of Health (224 requests decided in 2018–19), the Department of the Environment and Energy (163), the OAIC (133), the Department of Employment, Skills, Small and Family Business (DESSFB) (111), the Department of Education (94), the Australian Skills Quality Authority (94), IP Australia (87), the Department of Agriculture (72) and the Department of Finance (64).

6 These decisions will be reflected in the FOI Guidelines.

7 An agency may extend the period of time to make a decision by agreement with the applicant (s 15AA) or to undertake consultation with a third party (ss 15(6)-(8)). An agency can also apply to the Information Commissioner for more time to process a request when the request is complex or voluminous (s 15AB), or when access has been deemed to have been refused (ss 15AC and 51DA) or deemed to have been affirmed on internal review (s 54D). These extension provisions acknowledge there are circumstances when it is appropriate for an agency to take more than 30 days to process a request. When an agency has obtained an extension of time to deal with an FOI request and finalises the request within the extended time, the request is recorded as having been determined within the statutory time period.

There was also an overall reduction in the number of requests decided more than 90 days over the applicable statutory time period (Table E.9) when compared with 2017–18 (2.46% in 2018–19; 6.63% in 2017–18).

Table E.9: Response times greater than 90 days after the expiry of the applicable statutory period in 2018–19

Agency	Total requests decided	Requests decided more than 90 days after statutory period	% FOI requests received by agency or minister
Australian Competition Tribunal	1	1	100
Minister for Indigenous Affairs	2	2	100
Australian Broadcasting Corporation	55	13	23.64
National Archives of Australia	8	1	12.5
Department of Prime Minister and Cabinet	117	12	10.26
Department of Industry, Innovation and Science	65	6	9.23
Veterans' Review Board	12	1	8.33
Office of the Commonwealth Director of Public Prosecutions	37	3	8.11
Australian Federal Police	714	55	7.70
Australian Sports Anti-Doping Authority	23	1	4.35
Department of Home Affairs	15,678	634	4.04
Department of the Treasury	128	3	2.34
Australian Digital Health Agency	49	1	2.04
Australian Criminal Intelligence Commission	53	1	1.89
National Disability Insurance Agency	787	2	0.25
Immigration Assessment Authority	451	1	0.22
Department of Human Services	2,461	1	0.04
Department of Veterans' Affairs	2,770	1	0.04

Applications for amendment of personal records

Section 48 of the FOI Act confers a right on a person to apply to an agency or to a minister to amend a document to which lawful access has been granted, when the document contains personal information about the applicant:

- that is incomplete, incorrect, out of date or misleading and
- that has been used, is being used, or is available for use by the agency or minister for an administrative purpose.

In 2018–19, 10 agencies received 673 amendment applications (no applications were received by ministers). This is a 31.96% increase in applications from 2017–18 when 510 applications were received. However, in 2017–18 there was a 53.64% decrease in applications compared with the previous year (1,100 amendment applications were made in 2016–17).

The increase in amendment applications is largely due to an increase in applications received by the Department of Home Affairs (35.60% more in 2018–19 than in 2017–18). Increases in amendment applications were also experienced by the Department of Defence (a 50% increase, from 10 to 15 applications) and the DHS (a 21.43% increase, from 14 to 17 applications).[8]

Table E.10 compares the decision-making for amendment applications with 2017–18. In 2018–19, a decision was made to amend or annotate a person's personal record in 75.86% of all decided applications, an increase in the proportion granted in 2017–18, when 72.28% of all applications were granted. Because the Department of Home Affairs accounts for 91.38% of all amendment applications received, overall trends in amendment decision-making are largely determined by decisions made by the Department of Home Affairs.

8 The other agencies to receive amendment application in 2018–19 were the Australian Federal Police, the Australian National University, the Australian Nuclear Science and Technology Organisation, Comcare, the Commonwealth Ombudsman, the DESSFB and the DVA.

Table E.10: Decisions on amendment applications

Decision	2017–18	% of total	% change*	2018–19	% of total
Requests granted: amend record	314	57.83	24.14	407	63.40
Requests granted: annotate record	70	12.89	14.29	80	12.46
Requests granted: amend and annotate record	2	0.37	-100	–	–
Requests refused	157	28.91	-1.27	155	24.14
Total decided	**543**	**100**	**–**	**642**	**100**

* Percentage increase or decrease over 2017–18.

Time taken to respond to amendment applications

An agency is required to notify an applicant of a decision on their application to amend personal records as soon as practicable, but, in any case, not later than 30 days after the day the request is received, or a longer period as extended under the FOI Act.

In 2018–19, 89.51% of all amendment applications were decided within the applicable statutory time period compared to 85.82% in 2017–18.

Charges

Section 29 of the FOI Act provides that an agency or minister may impose charges in respect of FOI requests, except requests for personal information, and sets out the process by which charges are assessed, notified and adjusted.

Table E.11 shows the amounts collected by the 20 agencies that collected the most in charges under the FOI Act in 2018–19. These top 20 agencies are responsible for 86.55% of all charges collected by Australian Government agencies and ministers.

In 2018–19, agencies notified a total of $357,039 in charges with respect to 822 FOI requests, but collected only $122,774 (34.39% of the total notified). This difference is due to agencies exercising their discretion under s 29 of the FOI Act not to impose the whole charge, or applicants withdrawing their FOI request and not paying the notified charge.

Agencies notified less in charges in 2018–19 than in 2017–18, but collected more.
As noted above, in 2018–19, agencies notified a total of $357,039 in charges, 6.91% less than in 2017–18, when $383,531 was notified, and collected $122,774, a 5.97% increase over 2017–18 when $115,863 was collected.

Table E.11: Top 20 agencies by charges collected in 2018–19

Agency	Requests received	Requests where charges notified	Total charges notified ($)	Total charges collected ($)
Department of Health	434	161	49,640	18,341
Department of Defence	441	11	12,975	12,449
Department of the Environment and Energy	234	30	12,800	10,822
Department of Agriculture	117	38	12,731	10,328
Department of Education	235	67	17,052	8,093
Civil Aviation Safety Authority	146	36	11,330	6,638
Department of Industry, Innovation and Science	96	23	10,981	5,178
Department of Finance	135	26	11,708	3,531
Clean Energy Regulator	21	11	23,422	3,426
Airservices Australia	65	18	10,208	3,128
Australian Maritime Safety Authority	74	18	5,027	3,119
Australian Competition and Consumer Commission	72	16	9,779	2,769
IP Australia	119	13	5,093	2,666
Department of Infrastructure, Transport, Cities and Regional Development	99	9	4,710	2,400
Australian Securities and Investments Commission	296	10	3,108	2,393
Australian Communications and Media Authority	24	5	17,618	2,285

Table E.11: Top 20 agencies by charges collected in 2018–19 (continued)

Agency	Requests received	Requests where charges notified	Total charges notified ($)	Total charges collected ($)
Department of Foreign Affairs and Trade	237	24	14,074	2,251
Department of Communications and the Arts	64	4	5,738	2,248
Department of the Treasury	153	17	5,784	2,196
National Competition Council	3	3	3,125	2,003
Top 20	3,065	540	246,903	106,264
Remaining agencies	3,5814	282	110,136	16,510
Total	**38,879**	**822**	**357,039**	**122,774**

Disclosure log

All Australian Government agencies and ministers subject to the FOI Act are required to maintain an FOI disclosure log on a website. The disclosure log lists information that has been released to FOI applicants, subject to some exceptions (such as personal or business information). Information about agency and ministerial compliance with disclosure log requirements has been collected since 2012–13.

A total of 104 agencies and ministers provided information about their disclosure log activity in 2018–19. Collectively, they reported 1,200 new entries on disclosure logs during 2018–19; including documents available for download directly from the agency or minister's website in relation to 713 requests, documents available from another website in relation to 52 requests, and 435 entries in which the documents are available by another means (usually upon request).

The total number of new entries published on disclosure logs in 2018–19 is 8.70% higher than 2017–18, when 1,104 entries were added.

However, despite their being an increase in the proportion of documents which members of the public can access directly from agency websites (in 2018–19 it was 59.42% compared to 56.52% in 2017–18) the 2018-19 proportion is lower than the 66.87% in 2015–16. As explained in the FOI Guidelines, publication of documents directly through the disclosure log, rather than providing a description of the documents

and how they can be obtained on request from the agency or minister, is consistent with the FOI Act object of facilitating public access to government information.[9] In 2019–20, the OAIC intends to revise Part 14 of the FOI Guidelines (Disclosure Log) to emphasise the benefit to the community, and to agencies, of making documents released in response to FOI requests readily available on agency websites and to provide guidance to assist agencies in achieving this objective.

In 2018–19, agencies and ministers reported a total of 268, 861 unique visits to disclosure logs and 215,209 page views, which represents a 607.64% increase in unique visits since 2017–18 and a 289.47% increase in total page views reported in 2017–18. It is not clear whether this increase was the result of actual increases or better recording and reporting of website visits occurred in 2018–19 than in previous years.

Review of FOI decisions

Under the FOI Act, an applicant who is dissatisfied with the decision of an agency or minister on their initial FOI request has a number of avenues of review. The applicant can seek internal review with the agency or minister or external merits review by the Information Commissioner (IC review). Information Commissioner decisions under s 55K are reviewable by the AAT. AAT decisions may be appealed on a question of law to the Federal Court. In addition, an applicant can complain at any time to the Information Commissioner about an agency's actions under the FOI Act.

Third parties who have been consulted in the FOI process also have review rights if an agency or minister decides to release documents contrary to their submissions. Consultation requirements apply for state governments (s 26A), commercial organisations (s 27) and private individuals (s 27A).

Internal review

Although there is no obligation to do so, the Information Commissioner recommends and encourages FOI applicants to apply for an internal review before applying for an IC review.

In 2018–19, 893 applications were made for an internal review of FOI decisions: 12.05% more than in 2017–18 (when 797 internal review applications were made).

Of the 893 applications for an internal review, 543 (60.81%) were for review of decisions made in response to requests for personal information and 350 (39.19%) were for review of decisions on other information requests.

9 FOI Guidelines [14.32].

Agencies finalised 829 decisions on internal review in 2018–19: 26.60% more than in 2017–18 (733). Of these, 429 (51.75%) affirmed the original decision, 91 (10.98%) set aside the original decision and granted access in full, 232 (27.99%) granted access in part, seven (0.84%) granted access in another form, 14 (1.69%) resulted in lesser access and applicants withdrew 39 applications (4.71%) without concession by the agency. Agencies reduced the charges levied as a result of internal review in 17 cases (2.05%).

There were eight applications for internal review of decisions on amendment applications, 20% fewer than in 2017–18 (when 10 applications were made). Agencies made 10 internal review decisions on amendment applications: in eight (80%) the original decision was affirmed and in two (20%) the original decision was set aside. In 2017–18, 77.78% of original decisions were affirmed and 22.22% set aside.

IC review

Table E.12 provides a breakdown by agency and minister of IC review applications received in 2018–19, where the agency or minister was the subject of more than one IC review. In total, there were 928 applications for IC review (up 15.86% from 801 in 2017–18).

In general, the agencies that received the most FOI requests have the most IC review applications lodged against their decisions. In 2018–19, of the 20 agencies experiencing the most IC reviews, 15 also appear in the list of top 20 agencies in terms of the number of FOI requests received.

However, some agencies that did not receive large numbers of FOI requests were the subject of a comparatively large number of IC review applications given their FOI caseload. In 2018–19, the agencies with a large number of IC reviews lodged, expressed as a proportion of the total number of FOI requests received included the Australian Broadcasting Corporation (15.71%), ASIC (11.49%) and the DESSFB (11.49%).

Table E.12 IC review — top 20 by review applications received

Agency/minister	FOI requests received	Access refusal decisions	Access grant decisions	Total IC reviews	% of FOI requests
Department of Home Affairs	17,725	198	–	198	1.11
Department of Human Services	6,210	107	–	107	1.72
Department of Veterans' Affairs	2,943	47	–	47	1.60
Australian Federal Police	726	44	2	46	6.34
Department of Defence	441	41	3	44	9.98
Australian Taxation Office	1,291	41	–	41	3.18
Australian Securities and Investments Commission	296	34	–	34	11.49
Attorney-General's Department	336	28	–	28	8.33
Comcare	360	24	–	24	6.67
Department of Employment, Skills, Small and Family Business	148	17	–	17	11.49
National Disability Insurance Agency	836	17	–	17	2.03
Department of Foreign Affairs and Trade	237	16	–	16	6.75
Department of Prime Minister and Cabinet	170	15	–	15	8.82
Department of Health	434	13	2	15	3.46
Minister for Resources and Northern Australia	6	13	–	13	216.67
Australian Broadcasting Corporation	70	11	–	11	15.71
Australian Skills Quality Authority	101	10	–	10	9.90

Table E.12 IC review — top 20 by review applications received (continued)

Agency/minister	FOI requests received	Access refusal decisions	Access grant decisions	Total IC reviews	% of FOI requests
Australian Transaction Reports and Analysis Centre	509	9	–	9	1.77
Department of the Environment and Energy	234	9	2	11	4.70
NBN Co Limited	119	7	–	7	5.88
Subtotal	33,192	701	9	710	2.14
Remaining agencies/ ministers	5,687	203	15	218	3.83
Total	**38,879**	**904**	**24**	**928**	**2.39**

There was an 8.03% increase in the number of IC reviews finalised by the OAIC in 2018–19 (659), compared with 2017–187 (when 610 were finalised).

In 2018–19, 599 IC reviews were finalised without a formal decision being made under s 55K of the FOI Act (90.90% of all IC reviews finalised during this reporting period). This is a higher percentage than in 2017–18 (79.84%) and 2016–17 (79.81%).

The number of IC review applications declined under s 54W[10] of the FOI Act increased as a percentage of the total IC reviews finalised in 2018-19. In 2018–19, 196 IC reviews were declined under s 54W (29.74%) (2017–18, 26.89%; 2016–17, 27.38%).

Of the 196 IC review applications decisions taken not to review or not to continue to review the application under s 54W of the FOI Act: 64.29% were declined under s 54W(a)(i) (either frivolous, vexatious, misconceived, lacking in substance, or not made in good faith), 17.35% were declined under s 54W(a)(ii) (failure to cooperate), 2.55% under s 54W(a)(iii) (lost contact) and 15.82% under s 54W(b) (allow to go direct to AAT).

In 2018–19, the Information Commissioner made 60 decisions under s 55K of the FOI Act. Of the 60 decisions, 19 affirmed the decision under review (31.67%), 37 set aside the reviewable decision (61.67%) and four decisions were varied (6.67%). In 2017–18, the Information Commissioner affirmed 55.28% of decisions, set aside 36.59% and varied 8.13%.

10 Section 54W of the FOI Act contains a number of grounds under which the Information Commissioner may decide not to undertake an IC review or not to continue to undertake an IC review.

Of the 19 decisions affirmed by the Information Commissioner, two decisions (10.5%) were revised by the agency or minister under s 55G of the FOI Act during the IC review, giving greater access to the documents sought. Of the 37 decisions set aside and substituted by the Information Commissioner, in 10 (27%), the agency withdrew certain exemption contentions during the course of the IC review.

The percentage of applications received by the OAIC which were out of jurisdiction or invalid decreased from 13.28% in 2017–18, to 11.10% in 2018–19 (Table E.13).

Table E.13: IC review outcomes

Information Commissioner decisions	2017–18	% of 2017–18 total	2018–19	% of 2018–19 total
Section 54N — out of jurisdiction or invalid	81	13.28	103	15.63
Section 54R — withdrawn	131	21.48	199	30.20
Section 54R — withdrawn/conciliated	64	10.49	76	11.53
Section 54W(a) — deemed acceptance of preliminary view/appraisal	–	–	–	–
Section 54W(a)(i) — frivolous, vexatious, misconceived, lacking in substance, or not in good faith	79	12.95	126	19.12
Section 54W(a)(ii) — failure to cooperate	59	9.67	34	5.46
Section 54W(a)(iii) — lost contact	10	1.64	5	0.76
Section 54W(b) — refer to AAT	16	2.62	31	4.70
Section 54W(c) — failure to comply	–	–	–	–
Section 55F — set aside by agreement	15	2.46	13	1.97
Section 55F — varied by agreement	27	4.43	12	1.82
Section 55F — affirmed by agreement	–	–	–	–
Section 55G — substituted	5	0.82	–	–
Section 55K — affirmed by IC	68	11.15	19	2.88
Section 55K — set aside by IC	45	7.38	37	5.62
Section 55K — varied by IC	10	1.64	4	0.61
Total	**610**	**100.1***	**659**	**100.3**

* This total reflects rounding to two decimal places.

AAT review

An application can be made to the AAT for review of the following FOI decisions:

- a decision of the Information Commissioner under s 55K
- an IC reviewable decision (that is, an original decision or an internal review decision), but only if the Information Commissioner decides, under s 54W(b), that the interests of the administration of the FOI Act make it desirable that the IC reviewable decision be considered by the AAT directly.

In 2018–19, 21 applications for review of FOI decisions were made to the AAT. This is a 30% decrease on the 30 applications made in 2017–18.

Table E.14 provides a breakdown, by agency, of applications to the AAT in FOI matters in 2018–19. This data has been provided by the AAT.

In 2018–19, two agencies sought review in the AAT of decisions made by the Information Commissioner under s 55K of the FOI Act: the Australian Bureau of Statistics and the Department of Prime Minister and Cabinet.

Table E.14: AAT review by agency (respondent)

Respondent	Applications
Office of the Australian Information Commissioner	4
Department of Home Affairs	3
Australian Taxation Office	3
Department of Foreign Affairs and Trade	2
Department of Prime Minister and Cabinet	1
Department of Social Services	1
Department of Health	1
Department of Human Services	1
Department of Defence	1
Aged Care Quality and Safety Commissioner	1
Australian Federal Police	1
Australian Prudential Regulation Authority	1
Other (appeals by agencies against IC review decisions)	1
Total	**21**

Twenty-one applications remain outstanding with the AAT at the end of 2018–19.

Table E.15 shows the outcome of the 20 FOI reviews finalised by the AAT in 2018–19. AAT provided this data.

Table E.15: Outcomes of FOI reviews finalised by the AAT

AAT outcomes	Number in 2017–18	% of total 2017–18	Number in 2018–19	% of total 2018–19
Affirmed by consent	1	3.03	1	5.00
Varied/set aside/remitted by consent	5	15.15	4	20.00
Dismissed by consent	2	6.06	–	–
Withdrawn by applicant	10	30.30	4	20.00
Decision affirmed	5	15.15	6	30.00
Decision varied/set aside	7	21.21	1	5.00
Dismissed by AAT — frivolous or vexatious/fail to comply with direction	2	6.06	–	–
Dismissed — no application fee paid	1	3.03	1	5.00
Dismissed — non-reviewable decision	–	–	3	15.00
Total	**33**	**99.99***	**20**	**100.00**

* This total reflects rounding to two decimal places.

Of the 20 FOI reviews finalised by the AAT, seven (35.00%) resulted in published decisions in 2018–19.

The AAT affirmed the agency's decision in six (30.00%) of the 20 AAT reviews, compared with five (15.15%) in 2017–18.

Of the 20 FOI reviews finalised in 2018–19, three involved applications made by Australian Government agencies following decisions made by the Information Commissioner under s 55K of the FOI Act. Of these three reviews, one application was affirmed (by decision), one was varied with consent, and the other set aside and substituted by consent.

Federal Court

In January 2019, the Federal Circuit Court of Australia (Jarrett J) set aside a decision by a delegate of the Information Commissioner not to continue to undertake an IC review between the applicants and the second respondent, the Australian Human Rights Commission, and remitted the application to the OAIC for further consideration and determination according to law (see *Powell & Anor v Australian Information Commissioner & Anor* [2019] FCCA 39 (9 January 2019)).

Impact of FOI on agency resources

To assess the impact on agency resources of their compliance with the FOI Act, agencies are asked to estimate the hours staff spent on FOI matters and the non-labour costs directly attributable to FOI, such as legal and specific FOI training costs. Agencies submit these estimates annually. Agency estimates may also include FOI processing work undertaken on behalf of a minister's office.

Agencies are also asked to report their costs of compliance with the IPS. To facilitate comparison with information in previous annual reports, IPS costs are not included in this analysis of the cost of agency compliance with the FOI Act, but are discussed separately below.

The total reported cost attributable to processing FOI requests in 2018–19 was $59.85 million, a 14.68% increase over the previous financial year's total of $52.19 million.

The reason for the increase in the overall cost of FOI activity is a 12.96% increase in the total staff hours devoted to FOI in 2018–19 (when compared with 2017–18). Total staff hours in 2017–18, were 744,350; however, that rose to 840,803 in 2018–19. As a result, the average cost of each FOI request determined during this reporting period rose to $1,985.30 (from $1,648 in 2017–18).

Table E.16 sets out the average cost per FOI request determined (granted in full, in part or refused) compared to the last two financial years. The average cost per request determined in 2018–19 was $1,985 (up 20.45% from 2017–18).

Table E.16: Average cost per request determined

Year	Requests determined	Total cost ($)	Average cost per request determined ($)
2016–17	34,029	44,787,154	1,316
2017–18	31,674	52,186,179	1,648
2018–19	30,144	59,844,953	1,985

Staff costs

All agencies are asked to supply information about staff resources allocated to FOI.

Table E.17: Total FOI staffing across all Australian Government agencies

Staffing	2017–18	2018–19	% change
Total staff hours	744,350	840,803	12.96
Total staff years	372.18	420.40	12.96

Agencies provide estimates of the number of staff hours spent on FOI to enable calculation of salary costs (and 60% related costs) directly attributable to FOI request processing (Table E.17).

A summary of staff costs is provided in Table E.18, based on information provided by agencies and ministers and is calculated using the following median base annual salaries from Australian Public Service Commission public information:[11]

- FOI contact officer (officers whose duties included FOI work) $78,092[12]
- other officers involved in processing requests:
  - Senior Executive Service (SES) officers (or equivalent) $196,609[13]
  - APS Level 6 and Executive Levels (EL) 1–2 $113,866[14]
  - Australian Public Service (APS) Levels 1–5 $63,952[15]

11 Because salary levels differ between agencies, median salary levels have been used. These were published by the Australian Public Service Commission in its *APS Remuneration Report 2018*. These median levels are as at 31 December 2018.

12 APS Level 5 base salary median.

13 SES Band 1 base salary median.

14 Executive Level 1 base salary median.

15 APS Level 3 base salary median.

- minister's office:
  - minister and advisers $140,680[16]
  - minister's support staff $63,952.[17]

Table E.18: Estimated staff costs of FOI compared to last year

Type of staff	Staff years 2017–18	Total staff costs 2017–18 ($)	Staff years 2018–19	Total staff costs 2018–19 ($)	Total staff costs (% change)
FOI contact officers	277.32	33,971,341	311.71	38,946,729	14.65
SES	13.53	4,097,902	13.75	4,324,454	5.53
APS Level 6 and EL 1–2	42.38	7,569,521	50.31	9,166,395	21.10
APS Levels 1–5	36.97	3,665,451	43.07	4,406,957	20.23
Minister and advisers	1.05	231,062	0.94	211,357	-8.53
Minister's support staff	0.93	92,608	0.63	64,207	-30.67
Total	**372.18**	**49,627,885**	**420.40**	**57,120,102**	**15.10**

Total estimated staff costs in 2018–19 were $57.12 million, 15.10% more than in 2017–18. In 2017–18, total estimated staff costs rose by 17.18% over the previous financial year.

Non-labour costs

Non-labour costs directly attributable to FOI are summarised in Table E.19, including the percentage change from the previous year. The total non-labour costs in 2018–19 were $2.73 million, a 6.35% increase over the previous financial year ($2.56 million).

The largest increases in non-labour costs in 2018–19 were in relation to general legal advice costs (22.88% higher than in 2017–18) and training costs (19.07% higher). The higher general legal advice costs are primarily the result of Indigenous Business Australia and the DVA reporting higher than average legal expenses. Indigenous Business Australian explains that their increased general legal expenditure in 2018–19 relates to an application to the Information Commissioner to have a person declared vexatious. The DVA general legal advice expenditure increased by 644.71% in 2018–19 (from $18,419 in 2017–18 to $137,168 in 2018–19).

16 Executive Level 2 base salary median.

17 APS Level 3 base salary median.

There was also a 19.07% increase in training costs associated with FOI in 2018–19. This reflects training provided to new FOI staff and ongoing training for existing staff.

However, as can be seen from Table E.19, there was a substantial (-47.50%) decrease in general administrative costs (these include printing and postage). Undoubtedly, this reflects a general decline in the number of people requiring documents to be printed and sent to them in the post and increasing efficiencies in the use of digital technology.

Table E.19: Identified non-labour costs of FOI

Costs	2017–18	2018–19	% change
General legal advice costs	1,234,631	1,517,125	22.88
Litigation costs	426,145	414,635	-2.70
Total legal costs	1,660,776	1,931,760	16.32
General administrative costs	274,532	144,140	-47.50
Training	323,958	385,745	19.07
Other	299,029	263,206	-11.98
Total	**2,558,295**	**2,724,851**	**6.51**

Average cost per FOI request

The overall average number of staff days to process an FOI request in 2018–19 was 2.88 days; the same as in 2017–18 (2.87 days). As in previous years, the average staff days per FOI request differed significantly across agencies, from 0.02 days (the Australian Sports Anti-Doping Authority) to 37.60 days (the Bureau of Meteorology).

The average cost per request received also differed significantly across agencies from $10.77 to $71,441.05. The overall average cost per request received was $1,539.26, a 1.58% increase on the previous year's average of $1,515.37.

Table E.20: Agencies with average cost per FOI request greater than $10,000

Agency	Requests received	Average cost per request ($)
Northern Australian Infrastructure Facility	1	71,441.05
Australian Building and Construction	7	64,438.22
Torres Strait Regional Authority	1	34,978.50
Australian Centre for International Agricultural Research	1	33,295.11
Indigenous Business Australia	24	21,364.80
Bureau of Meteorology	6	20,793.61
High Court of Australia	7	19,803.34
Airservices Australia	65	19,071.23
Australian Transport Safety Bureau	15	15,071.81
Aged Care Complaints Commissioner	13	14,019.12
National Competition Council	3	13,742.78
Department of Defence	441	13,114.31
Cancer Australia	5	12,891.65
Australian Centre for International Agricultural Research	3	12,259.32
Department of Industry, Innovation and Science	96	10,658.53
Fair Work Ombudsman	50	10,437.70
Department of the Prime Minister and Cabinet	170	10,252.08

As a general rule, the agencies with the highest average cost per request are small agencies which do not receive many FOI requests (Table E.20). As a result, they do not have the opportunity to develop the processing efficiencies that agencies with higher volumes of FOI requests do.

However, the Department of Defence, which received 441 FOI requests in 2018–19, has a high average cost per request. This is because its average staff days per request are high (20.98 per request) and its overall costs are higher than other agencies because of its general administrative, legal and training costs in 2018–19 ($179,227).

Impact of the IPS on agency resources

Agencies are required to provide information about the costs of meeting their obligations under the IPS.

The total reported cost attributable to compliance with the IPS in 2018–19 was $1,254,293.47, 30.03% more than in 2017–18 ($964,637). This increase may be largely attributable to IPS reviews conducted by agencies as a result of the OAIC conducting a survey of agencies' IPS compliance between May and July 2018. The OAIC published its report on IPS compliance in June 2019 and intends updating guidance for agencies to assist compliance and promote proactive disclosure thereby reducing the number of FOI requests to ease the processing burden on agencies.

Staff costs

Table E.21 shows the total reported IPS staffing across Australian Government agencies compared to last year.

Table E.21: Total IPS staffing

Staffing	2017–18	2018–19	% change
Staff numbers: 75–100% time on IPS matters	7	31	342.86
Staff numbers: less than 75% time on IPS matters	418	323	-22.73
Total staff hours	15,087	19,225	27.43
Total staff years	7.54	9.61	27.45

Table E.22 shows the staff costs relating to the IPS.

Table E.22: Estimated staff costs in relation to the IPS in 2018–19

Type of staff*	Staff years	Salary costs ($)	Related costs (60%)	Total staff costs ($)
IPS contact officers	8.74	436,790.42	655,185.63	1,091,976.05
SES	0.09	11,639.25	17,458.88	29,098.13
APS Level 6 and EL 1–2	0.60	43,943.17	65,914.75	109,857.92
APS Levels 1–5	0.18	7,264.95	10,897.42	18,162.37
Total	**9.61**	**499,637.79**	**749,456.68**	**1,249,094.47**

* IPS contact officers are officers whose usual duties include IPS work. The other rows cover other officers involved in IPS work.

Non-labour IPS costs

Reported IPS non-labour costs for all agencies totalled $5,199 in 2018–19, a 49.65% decrease when compared with 2017–18.

Only three agencies (of the more than 200 agencies subject to the requirement to maintain an IPS entry) reported any expenditure on IPS during 2018–19. The Department of Foreign Affairs and Trade was the only agency to report expenditure associated with IPS training ($3,774).

Appendix F: Acronyms and abbreviations

Acronym or abbreviation	Expanded term
AAT	Administrative Appeals Tribunal
ACCC	Australian Competition and Consumer Commission
ACT	Australian Capital Territory
AFP	Australian Federal Police
AHRC	Australian Human Rights Commission
AIAC	Association of Information and Access Commissioners
AIC	Australian Institute of Criminology
AIC Act	*Australian Information Commission Act 2010*
AICmr	Australian Information Commissioner
ANAO	Australian National Audit Office
APP	Australian Privacy Principle
APPA	Asia Pacific Privacy Authorities
APS	Australian Public Service
ASIC	Australian Securities and Investments Commission
ATO	Australian Taxation Office
AustLII	Australasian Legal Information Institute
CBA	Commonwealth Bank of Australia Limited
CCTV	Closed circuit television
CDR	Consumer Data Right
CII	Commissioner initiated investigation
Coles	Coles Supermarkets Australia

Acronym or abbreviation	Expanded term
CPN	Consumer Privacy Network
CR Code	*Privacy (Credit Reporting) Code 2014 (v2)*
Data-matching Act	*Data-matching Program (Assistance and Tax) Act 1990*
DESSFB	Department of Employment, Skills, Small and Family Business
DHS	Department of Human Services
DIPB	Department of Immigration and Border Protection
DVA	Department of Veterans' Affairs
DVS	Document Verification Service
EOT	Extensions of time
FOI	Freedom of information
FOI Act	*Freedom of Information Act 1982*
FTE	Full-time equivalent
GST	Goods and Services Tax
IC	Information Commissioner
ICIC	International Conference of Information Commissioners
ICDPPC	International Conference of Data Protection and Privacy Commissioners
ICON	Information Contact Officer Network
ICT	Information and communications technology
Information Commissioner	Australian Information Commissioner, within the meaning of the *Australian Information Commissioner Act 2010*.
Information Privacy Act	*Information Privacy Act 2014* (ACT)
IPS	Information Publication Scheme
KMP	Key management personnel
MOU	Memorandum of Understanding

Acronym or abbreviation	Expanded term
MYEFO	Mid-Year Economic and Fiscal Outlook
My Health Records Act	*My Health Records Act 2012*
National Health Act	*National Health Act 1953*
National Health (Privacy) Rules	*National Health (Privacy) Rules 2018*
NDB	Notifiable Data Breaches
NEIDM	Non-Employment Income Data Matching
NFBMC	National Facial Biometric Matching Capability
NSW	New South Wales
NPP	National Privacy Principle
OAIC	Office of the Australian Information Commissioner
PAA	Privacy Authorities Australia
PAW	Privacy Awareness Week
PAYG	Pay-As-You-Go
PGPA Act	*Public Governance, Performance and Accountability Act 2013*
PGPA Rule	*Public Governance, Performance and Accountability Rule 2014*
PID	Public interest determination
PPN	Privacy Professionals' Network
Privacy Act	*Privacy Act 1988*
Privacy Code	*Privacy (Australian Government Agencies — Governance) APP Code 2017*
RACGP	Royal Australian College of General Practitioners
Registrar	Student Identifiers Registrar
SA	South Australia
SES	Senior Executive Service

Acronym or abbreviation	Expanded term
SME	Small and medium enterprises
TPPs	Territory Privacy Principles
USI	Unique Student Identifiers
WHS	Workplace health and safety
Woolworths	Woolworths Limited

Appendix G: Correction of material errors

Below are corrections of errors in the *Office of the Australian Information Commissioner Annual Report 2017–18*.

Page 98 — Workplace relations

The sentence: 'In 2017–18, seven Executive members and other staff received performance pay or were under individual flexibility arrangements, Australian workplace agreements or common law contracts'; should read as follows: 'In 2017–18, seven Executive members and other staff were under individual flexibility arrangements, Australian workplace agreements or common law contracts.'

Page 145 — Australian Digital Health Agency

The sentence: 'For the 2017–18 financial year, the value of the MOU was $2,076,649.94 (GST exclusive)'; should read as follows: 'For the 2017–18 financial year, the OAIC received $1,688,343.88 (GST exclusive).'

Appendix H: List of requirements

PGPA Rule reference	Description	Requirement	Part of report
17AD(g)	**Letter of transmittal**		
17AI	A copy of the letter of transmittal signed and dated by accountable authority on date final text approved, with statement that the report has been prepared in accordance with s 46 of the Act and any enabling legislation that specifies additional requirements in relation to the annual report.	Mandatory	1
17AD(h)	**Aids to access**		
17AJ(a)	Table of contents.	Mandatory	2
17AJ(b)	Alphabetical index.	Mandatory	214
17AJ(c)	Glossary of abbreviations and acronyms.	Mandatory	200
17AJ(d)	List of requirements.	Mandatory	205
17AJ(e)	Details of contact officer.	Mandatory	Inside cover
17AJ(f)	Entity's website address.	Mandatory	Inside cover
17AJ(g)	Electronic address of report.	Mandatory	Inside cover
17AD(a)	**Review by accountable authority**		
17AD(a)	A review by the accountable authority of the entity.	Mandatory	8–11
17AD(b)	**Overview of the entity**		
17AE(1)(a)(i)	A description of the role and functions of the entity.	Mandatory	6
17AE(1)(a)(ii)	A description of the organisational structure of the entity.	Mandatory	16
17AE(1)(a)(iii)	A description of the outcomes and programmes administered by the entity.	Mandatory	27–93

PGPA Rule reference	Description	Requirement	Part of report
17AE(1)(a)(iv)	A description of the purposes of the entity as included in corporate plan.	Mandatory	7
17AE(1)(aa)(i)	Name of the accountable authority or each member of the accountable authority.	Mandatory	16
17AE(1)(aa)(ii)	Position title of the accountable authority or member of the accountable authority within the reporting period	Mandatory	16
17AE(1)(aa)(iii)	Period as the accountable authority or member of the accountable authority within the reporting period.	Mandatory	16
17AE(1)(b)	An outline of the structure of the portfolio of the entity.	Portfolio departments – mandatory	6, 16, 96
17AE(2)	Where the outcomes and programs administered by the entity differ from any Portfolio Budget Statement, Portfolio Additional Estimates Statement or other portfolio estimates statement that was prepared for the entity for the period, include details of variation and reasons for change.	If applicable, mandatory	N/A
17AD(c)	**Report on the performance of the entity**		
	Annual performance statements		
17AD(c)(i); 16F	Annual performance statement in accordance with paragraph 39(1)(b) of the Act and s 16F of the Rule.	Mandatory	27–93
17AD(c)(ii)	*Report on financial performance*		
17AF(1)(a)	A discussion and analysis of the entity's financial performance.	Mandatory	109–147
17AF(1)(b)	A table summarising the total resources and total payments of the entity.	Mandatory	150–152

PGPA Rule reference	Description	Requirement	Part of report
17AF(2)	If there may be significant changes in the financial results during or after the previous or current reporting period, information on those changes, including: the cause of any operating loss of the entity; how the entity has responded to the loss and the actions that have been taken in relation to the loss; and any matter or circumstances that it can reasonably be anticipated will have a significant impact on the entity's future operation or financial results.	If applicable, mandatory	109–147, 150–152
17AD(d)	**Management and accountability**		
	Corporate governance		
17AG(2)(a)	Information on compliance with s 10 (fraud systems)	Mandatory	106
17AG(2)(b)(i)	A certification by accountable authority that fraud risk assessments and fraud control plans have been prepared.	Mandatory	1
17AG(2)(b)(ii)	A certification by accountable authority that appropriate mechanisms for preventing, detecting incidents of, investigating or otherwise dealing with, and recording or reporting fraud that meet the specific needs of the entity are in place.	Mandatory	1
17AG(2)(b)(iii)	A certification by accountable authority that all reasonable measures have been taken to deal appropriately with fraud relating to the entity.	Mandatory	1
17AG(2)(c)	An outline of structures and processes in place for the entity to implement principles and objectives of corporate governance.	Mandatory	92

PGPA Rule reference	Description	Requirement	Part of report
17AG(2)(d) – (e)	A statement of significant issues reported to Minister under paragraph 19(1)(e) of the Act that relates to noncompliance with finance law and action taken to remedy noncompliance.	If applicable, mandatory	N/A
	External scrutiny		
17AG(3)	Information on the most significant developments in external scrutiny and the entity's response to the scrutiny.	Mandatory	N/A
17AG(3)(a)	Information on judicial decisions and decisions of administrative tribunals and by the Australian Information Commissioner that may have a significant effect on the operations of the entity.	If applicable, mandatory	N/A
17AG(3)(b)	Information on any reports on operations of the entity by the AuditorGeneral (other than report under s 43 of the Act), a Parliamentary Committee, or the Commonwealth Ombudsman.	If applicable, mandatory	N/A
17AG(3)(c)	Information on any capability reviews on the entity that were released during the period.	If applicable, mandatory	N/A
	Management of human resources		
17AG(4)(a)	An assessment of the entity's effectiveness in managing and developing employees to achieve entity objectives.	Mandatory	99, 101
17AG(4)(aa)	Statistics on the entity's employees on an ongoing and non-ongoing basis, including the following: ▪ statistics on full-time employees ▪ statistics on part-time employees ▪ statistics on gender ▪ statistics on staff location.	Mandatory	99–100

PGPA Rule reference	Description	Requirement	Part of report
17AG(4)(b)	Statistics on the entity's APS employees on an ongoing and nonongoing basis; including the following: ▪ statistics on staffing classification level ▪ statistics on fulltime employees ▪ statistics on parttime employees ▪ statistics on gender ▪ statistics on staff location ▪ statistics on employees who identify as Indigenous.	Mandatory	99–100
17AG(4)(c)	Information on any enterprise agreements, individual flexibility arrangements, Australian workplace agreements, common law contracts and determinations under subsection 24(1) of the *Public Service Act 1999*.	Mandatory	102
17AG(4)(c)(i)	Information on the number of SES and nonSES employees covered by agreements etc identified in paragraph 17AG(4)(c).	Mandatory	100
17AG(4)(c)(ii)	The salary ranges available for APS employees by classification level.	Mandatory	100
17AG(4)(c)(iii)	A description of non-salary benefits provided to employees.	Mandatory	102
17AG(4)(d)(i)	Information on the number of employees at each classification level who received performance pay.	If applicable, mandatory	N/A
17AG(4)(d)(ii)	Information on aggregate amounts of performance pay at each classification level.	If applicable, mandatory	N/A
17AG(4)(d)(iii)	Information on the average amount of performance payment, and range of such payments, at each classification level.	If applicable, mandatory	N/A

PGPA Rule reference	Description	Requirement	Part of report
17AG(4)(d)(iv)	Information on aggregate amount of performance payments.	If applicable, mandatory	N/A
	Assets management		
17AG(5)	An assessment of effectiveness of assets management where asset management is a significant part of the entity's activities.	If applicable, mandatory	N/A
	Purchasing		
17AG(6)	An assessment of entity performance against the *Commonwealth Procurement Rules*.	Mandatory	104–105
	Consultants		
17AG(7)(a)	A summary statement detailing the number of new contracts engaging consultants entered into during the period; the total actual expenditure on all new consultancy contracts entered into during the period (inclusive of GST); the number of ongoing consultancy contracts that were entered into during a previous reporting period; and the total actual expenditure in the reporting year on the ongoing consultancy contracts (inclusive of GST).	Mandatory	104
17AG(7)(b)	A statement that "*During [reporting period], [specified number] new consultancy contracts were entered into involving total actual expenditure of $[specified million]. In addition, [specified number] ongoing consultancy contracts were active during the period, involving total actual expenditure of $[specified million]*".	Mandatory	104

PGPA Rule reference	Description	Requirement	Part of report
17AG(7)(c)	A summary of the policies and procedures for selecting and engaging consultants and the main categories of purposes for which consultants were selected and engaged.	Mandatory	104
17AG(7)(d)	A statement that '*Annual reports contain information about actual expenditure on contracts for consultancies. Information on the value of contracts and consultancies is available on the AusTender website.*'	Mandatory	105
	Australian National Audit Office access clauses		
17AG(8)	If an entity entered into a contract with a value of more than $100,000 (inclusive of GST) and the contract did not provide the AuditorGeneral with access to the contractor's premises, the report must include the name of the contractor, purpose and value of the contract, and the reason why a clause allowing access was not included in the contract.	If applicable, mandatory	N/A
	Exempt contracts		
17AG(9)	If an entity entered into a contract or there is a standing offer with a value greater than $10,000 (inclusive of GST) which has been exempted from being published in AusTender because it would disclose exempt matters under the FOI Act, the annual report must include a statement that the contract or standing offer has been exempted, and the value of the contract or standing offer, to the extent that doing so does not disclose the exempt matters.	If applicable, mandatory	N/A

PGPA Rule reference	Description	Requirement	Part of report
	Small business		
17AG(10)(a)	A statement that "*[Name of entity] supports small business participation in the Commonwealth Government procurement market. Small and Medium Enterprises (SME) and Small Enterprise participation statistics are available on the Department of Finance's website.*"	Mandatory	105
17AG(10)(b)	An outline of the ways in which the procurement practices of the entity support small and medium enterprises.	Mandatory	105
17AG(10)(c)	If the entity is considered by the Department administered by the Finance Minister as material in nature—a statement that "*[Name of entity] recognises the importance of ensuring that small businesses are paid on time. The results of the Survey of Australian Government Payments to Small Business are available on the Treasury's website.*"	If applicable, mandatory	105
	Financial statements		
17AD(e)	Inclusion of the annual financial statements in accordance with subsection 43(4) of the Act.	Mandatory	109–147
	Executive remuneration		
17AD(da)	Information about executive remuneration in accordance with Subdivision C of Division 3A of Part 2–3 of the Rule.	Mandatory	153–156

PGPA Rule reference	Description	Requirement	Part of report
17AD(f)	**Other mandatory information**		
17AH(1)(a)(i)	If the entity conducted advertising campaigns, a statement that "*During [reporting period], the [name of entity] conducted the following advertising campaigns: [name of advertising campaigns undertaken]. Further information on those advertising campaigns is available at [address of entity's website] and in the reports on Australian Government advertising prepared by the Department of Finance. Those reports are available on the Department of Finance's website.*"	If applicable, mandatory	106
17AH(1)(a)(ii)	If the entity did not conduct advertising campaigns, a statement to that effect.	If applicable, mandatory	N/A
17AH(1)(b)	A statement that "*Information on grants awarded by [name of entity] during [reporting period] is available at [address of entity's website].*"	If applicable, mandatory	106
17AH(1)(c)	Outline of mechanisms of disability reporting, including reference to website for further information.	Mandatory	106
17AH(1)(d)	Website reference to where the entity's Information Publication Scheme statement pursuant to Part II of FOI Act can be found.	Mandatory	107
17AH(1)(e)	Correction of material errors in previous annual report	If applicable, mandatory	204
17AH(2)	Information required by other legislation	Mandatory	160–199

Appendix I: Index

D

E

F

G

H

I

K

L

M

oaic.gov.au

Office of the Australian Information Commissioner

1300 363 992
enquiries@oaic.gov.au
@OAICgov