

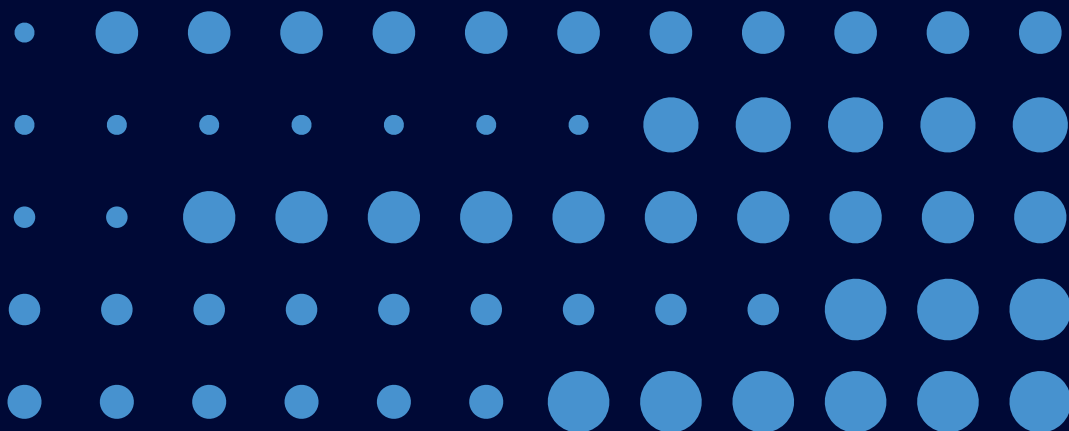


IGIS

OFFICE OF THE
INSPECTOR-GENERAL
OF INTELLIGENCE
AND SECURITY

ANNUAL REPORT

2022-23



Contact information

Office of the Inspector-General of Intelligence and Security
3-5 National Circuit
Barton, ACT 2600

General enquires

Phone: (02) 6141 3330
Email: info@igis.gov.au
Website: www.igis.gov.au

Complaints

Phone: (02) 6141 4555
Email: complaints@igis.gov.au
Website: www.igis.gov.au/complaints

Non-English speakers

If you speak a language other than English and need help, please call the Translating and Interpreting Service on 131450 and ask for the Inspector-General of Intelligence and Security on (02) 6141 3330. This is a free service.

Acknowledgement

Design and Typesetting: Typeyard Design & Advertising

Printing: Elect Printing

ISSN: 1030-4657

© Commonwealth of Australia 2023



All material presented in this publication is provided under a Creative Commons Attribution 3.0 Australia licence. For the avoidance of doubt, this means this licence only applies to material as set out in this document. The details of the relevant licence conditions are available on the Creative Commons website www.creativecommons.org.au

Acknowledgement of Country

The Office of the Inspector-General of Intelligence and Security acknowledges the Traditional Custodians of Country throughout Australia and their connections to land, sea and community. We pay our respect to elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples.



OFFICE OF THE
INSPECTOR-GENERAL
OF INTELLIGENCE
AND SECURITY

The Hon Mark Dreyfus KC MP
Attorney-General
Parliament House
CANBERRA ACT 2600

Dear Attorney-General

Office of the Inspector-General of Intelligence and Security Annual Report 2022–2023

I am pleased to present the Inspector-General of Intelligence and Security annual report for the period 1 July 2022 to 30 June 2023.

This report has been prepared for the purposes of s 46 of the *Public Governance, Performance and Accountability Act 2013* and s 35 of the *Inspector-General of Intelligence and Security Act 1986*.

Each of the intelligence agencies within my jurisdiction has confirmed that the components of the report that relate to them will not prejudice security, the defence of Australia, Australia's relations with other countries, law enforcement operations or the privacy of individuals.

The report is therefore suitable to be laid before each House of Parliament.

The report includes my Office's audited financial statements prepared in accordance with the *Public Governance, Performance and Accountability (Financial Reporting) Rule 2015*.

As required by s 10 of the *Public Governance, Performance and Accountability Rule 2014*, I certify that my Office has undertaken a fraud risk assessment and has a fraud control plan, both of which are reviewed periodically. I further certify that appropriate fraud prevention, detection, investigation and reporting mechanisms are in place that meet the specific needs of my agency and that I have taken all reasonable measures to deal appropriately with fraud relating to the agency.

Yours sincerely

The Hon Christopher Jessup KC
Inspector-General of Intelligence and Security
25 September 2023

Contents

Contact information	ii
Letter of transmittal	iii
About this report	vi
Glossary	vii
Section One: Review by the Inspector-General	1
Inspector-General's review	2
Year at a glance 2022-23	4
Section Two: Overview	5
Purpose	6
Our approach	7
About us	8
Our key activities	9
Organisation chart	10
Providing assurance	11
Section Three: Annual Performance Statement	15
2022-23 Annual Performance Statement	16
Reporting framework	17
2022-23 Performance Review	18
Section Four: Management and accountability	31
Our staff and culture	32
Organisational profile	36
Corporate governance	41
Stakeholders	44
Risk oversight and management	47
External scrutiny	49

Section Five: Financial statements	53
Financial statements	54
Appendix A: Entity resource statements and resource for outcomes	80
Section Six: Review of intelligence agencies	83
The intelligence agencies	84
Agency oversight activities 2022–23	91
Office of National Intelligence	92
Australian Security Intelligence Organisation	94
Australian Secret Intelligence Service	106
Australian Signals Directorate	110
Australian Geospatial-Intelligence Organisation	115
Defence Intelligence Organisation	117
Australian Criminal Intelligence Commission and Australian Federal Police	119
Cross-agency inspection and inquiry activities	120
Complaints and Public Interest Disclosures	123
Section Seven: Annexures	129
Annexure 7.1: Other mandatory information	130
Annexure 7.2: Requirements for annual reports	132
Index	143

About this report

This report provides information on the activities, achievements and performance of the Office of the Inspector-General of Intelligence and Security (IGIS/the Office) for the 2022–23 reporting period.

This report has been prepared in accordance with legislative requirements. These include the annual reporting requirements set out in the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), the associated *Public Governance, Performance and Accountability Rule 2014* (PGPA Rule), *Public Governance, Performance and Accountability (Financial Reporting) Rule 2015*, s 35 of the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) and other legislation.

Guide to the report

Section One contains the Inspector-General’s review of the reporting period and outlook for 2022–23.

Section Two outlines the role and functions of the Inspector-General and the Office.

Section Three contains the Annual Performance Statement, detailing the Office’s performance during the reporting period against the indicators identified in the IGIS Corporate Plan 2022–23.

Section Four reports on the Office’s governance and accountability, including corporate governance, management of human resources, procurement and other relevant information.

Section Five contains a summary of the financial management and audited financial statements.

Section Six contains a review of the Office’s oversight of the intelligence agencies within its jurisdiction.

Section Seven contains the annexures to this report. The annexures contain a range of additional information about the Office and an index to this report.

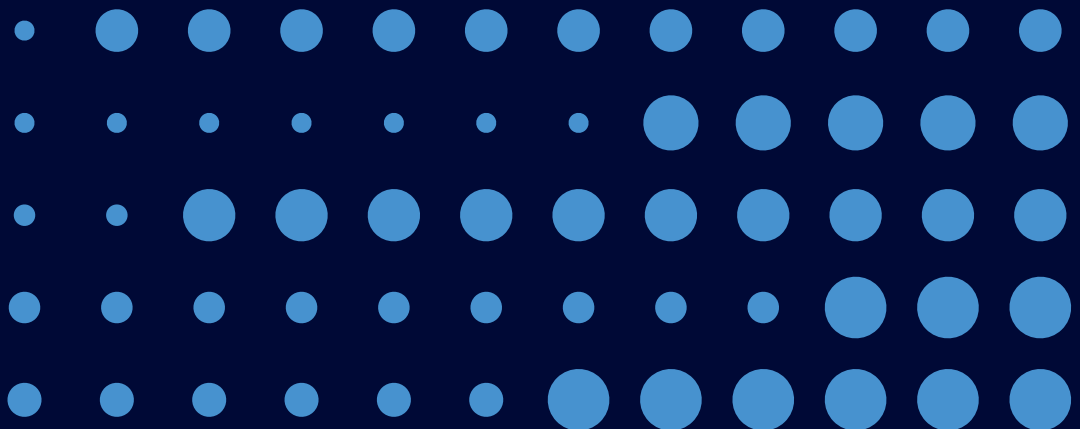
Glossary

AAT	Administrative Appeals Tribunal
ACIC	Australian Criminal Intelligence Commission
ACSC	Australian Cyber Security Centre
ACLEI	Australian Commission for Law Enforcement Integrity
ACT	Australian Capital Territory
ADF	Australian Defence Force
AFP	Australian Federal Police
AGD	Attorney-General's Department
AGO	Australian Geospatial-Intelligence Organisation
ANAO	Australian National Audit Office
APS	Australian Public Service
Archives Act	<i>Archives Act 1983</i>
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ASIO Act	<i>Australian Security Intelligence Organisation Act 1979</i>
ASIS	Australian Secret Intelligence Service
ASL	Average staffing level
AUSTRAC	Australian Transaction Reports and Analysis Centre
CAP	Census Action Plan
Crimes Act	<i>Crimes Act 1914</i>
Criminal Code	<i>Criminal Code Act 1995</i>
D&I	Diversity and inclusion
DIO	Defence Intelligence Organisation
FIORC	Five-Eyes Intelligence Oversight and Review Council
Five-Eyes	The intelligence partnership comprising Australia, Canada, New Zealand, the United Kingdom and the United States
FOI Act	<i>Freedom of Information Act 1982</i>
KMP	Key Management Personnel
ICT	Information and communications technology
IGIS/the Office	The statutory agency of the Inspector-General of Intelligence and Security
IGIS Act	<i>Inspector-General of Intelligence and Security Act 1986</i>
IPS	Information Publication Scheme

IS Act	<i>Intelligence Services Act 2001</i>
L&D	Learning and development
NAW	Network activity warrant
NIC	National Intelligence Community
ONI	Office of National Intelligence
ONI Act	<i>Office of National Intelligence Act 2018</i>
PBS	Portfolio Budget Statements
PGPA Act	<i>Public Governance, Performance and Accountability Act 2013</i>
PGPA Rule	<i>Public Governance, Performance and Accountability Rule 2014</i>
PID	Public interest disclosure
PID Act	<i>Public Interest Disclosure Act 2013</i>
PJCIS	Parliamentary Joint Committee on Intelligence and Security
Privacy Act	<i>Privacy Act 1988</i>
PS Act	<i>Public Service Act 1999</i>
REDSPICE	Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers
SES	Senior Executive Service
SIO	Special intelligence operation
The intelligence agencies	ONI, ASIO, ASIS, ASD, AGO and DIO
TIA Act	<i>Telecommunications (Interception and Access) Act 1979</i>
Telecommunications Act	<i>Telecommunications Act 1997</i>
WHS Act	<i>Work Health and Safety Act 2011</i>

Section One

Review by the
Inspector-General



Inspector-General's review



In accordance with s 35 of the *Inspector-General of Intelligence and Security Act 1986*, this report provides details of my Office's inquiry and inspection activities during the year, and on agency compliance with certain privacy rules. It also provides details of the structure, performance and financial position of the Office.

This year, while anticipating and preparing for legislative change affecting the functions of the Office and of the agencies in relation to which we have oversight responsibility, the Office has focused on its core activities of conducting inquiries, making regular inspections, and receiving complaints and public interest disclosures.

Regular inspection work is a daily, fundamental, activity for the Office. During the year under review, 4 inquiries commenced and 2 were completed. Our agency oversight teams completed and issued findings for 89 inspections. Together with senior officers, I held at least biannual meetings with all agencies in our jurisdiction, and kept relevant ministers informed of the Office's plans, progress and findings in relation to the agencies in their respective portfolios. The Office's practice of handling complaints and public interest disclosures continues to grow and evolve. Further particulars of this year's completed inquiries, inspections and complaint and disclosure matters are set out in Section 6 of this report.

Our inspection teams encounter – either through our planned activities, or through reporting by the relevant agencies themselves – material in the files of agencies which provide evidence of non-compliance, either with the law or with appropriate standards of propriety. In the great majority of such instances, the matters are towards the less serious end of the spectrum, and are readily put to rights upon being drawn to the attention of the agencies concerned. The Office undertakes inspections of the implementation of findings to ensure that the identified compliance issues have been addressed, and practices and policies are in place to reduce the likelihood of recurrence.

In general terms, over the past year the agencies treated regular inspection and oversight by the Office as a conventional feature of their ongoing operations. Here it is important to stress that this disposition on the part of the agencies implied no compromise of the independence of the Office or of the rigour of its oversight; rather, the assumption implied by it was that the agencies welcomed the impact upon their own compliance discipline which that oversight involved. This state of affairs – and the generally high level of compliance produced by it – made its own contribution to the activity of the Office.

Over 2022–23, the Office has had to adapt to a changing operating environment. After years of disruptions to our operational activity due to the COVID-19 pandemic and associated lockdowns, this year the Office has been able to resume 'business-as-usual'; IGIS officers returned to the office, conducted on-site activities at the agencies, and travelled interstate and overseas to undertake the work of the Office.

Legislative changes this reporting period – such as the passing of the *National Anti-Corruption Commission Act 2022*, the *Anti-Discrimination and Human Rights Legislation Amendment (Respect at Work) Act 2022*, and the *Public Interest Disclosure Amendment (Review) Act 2023* – will expand the powers and role of the national intelligence community and increase IGIS's oversight responsibilities.

The Office was consulted on the development of these proposals for legislative change, and continues to contribute significantly to the consultation processes regarding further proposed change. Often the legislation governing intelligence work can be legally and technically complex; this consultation is an important feature of legislative design and development as it assists in ensuring that structures supporting effective oversight are recognised and included in legislation.

Over the year, the Office contributed to inquiries conducted by the Parliamentary Joint Committee on Intelligence and Security by appearing before the Committee, as well as by responding to questions taken on notice at the various hearings on a range of bills.

Engagement with our portfolio department, the Attorney-General's Department, and other integrity and oversight agencies continues to be strong. Together with the heads of other Commonwealth integrity agencies, I attended the meetings of the Integrity Agencies Group chaired by the Australian Public Service Commissioner, and met with other integrity agency heads individually as required during the year. Additionally, meetings were held with integrity agency partners at the officer and executive level on a number of different issues.

The Office continued its international engagement with other Five-Eyes oversight bodies throughout the year. After last year's virtual annual meeting, the Five-Eyes Intelligence Oversight and Review Council returned to its in-person format, in Washington in November 2022. This meeting provided an important opportunity to exchange views, compare best practices and explore areas for cooperation on this year's themes of oversight resilience, information sharing and transparency.

This year, following the finalisation of the Office's Information Governance Framework in 2021-22, the Office continued to strengthen its information governance practices, and undertook an appropriate refresh of relevant ICT assets. The Office's corporate governance framework continued to be strengthened as several key projects were completed over the year, such as the Office's refreshed Fraud and Corruption Control Plan and Guidance. The work of further developing and embedding corporate and information governance systems and processes will continue into the next reporting period, as the Office continues to grow.

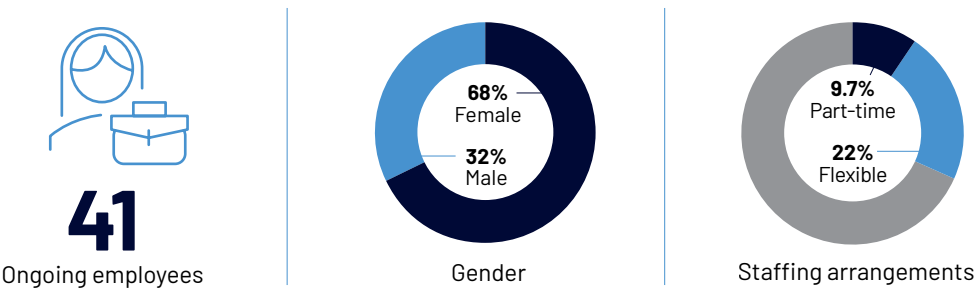
Staffing levels continue to be a challenge that the Office is working to address. The planned expansion to the Office's full complement of staff has not been reached for a number of reasons, including those related to the necessary but lengthy security clearance process and the extremely competitive external labour market. We, like many public sector agencies, continue to feel the challenges of recruiting and retaining subject matter experts across a range of skillsets. The Office continues to implement strategies to improve workforce retention and, over the coming year, will continue its focus on strategic HR initiatives to continue to attract talent, retain high quality staff and provide a rewarding and intellectually stimulating work environment.

Finally, I am very pleased to advise that my Office has initiated the Margaret Stone Conversation Series, in tribute to the previous Inspector-General, the Hon Margaret Stone AO FAAL, who was a much-admired figure in the Office and in the broader legal, oversight and intelligence communities. This series brings together IGIS officers with leaders across a range of disciplines to gain different perspectives and challenge and deepen their knowledge.

I thank all staff of my Office for their professionalism and dedication over the year. The work of this Office is important, and it is critical to independent and credible oversight of the intelligence community. It will only become more so in the coming years as the national conversation has become more highly attuned to matters of intelligence integrity and oversight, particularly with the proposed expansion and further development of the intelligence community.

Year at a glance 2022-23

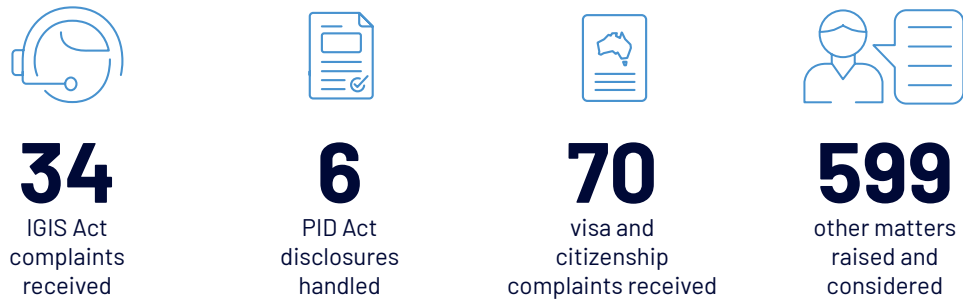
Staffing profile as at 30 June 2023



Oversight activities

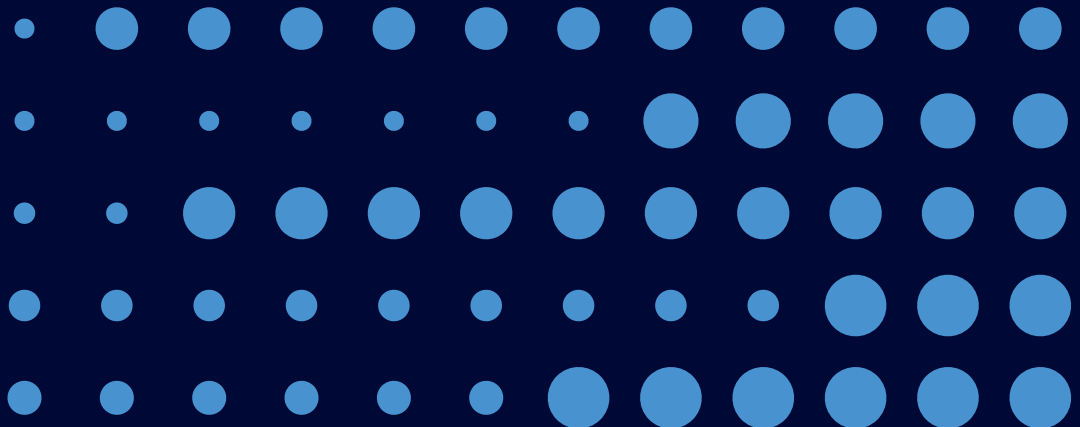


Complaints and public interest disclosures (PIDs)



Section Two

Overview



Purpose

Our purpose is to provide independent assurance to ministers, the parliament, and the public as to whether Australia's intelligence and security agencies within our jurisdiction are acting with legality, propriety and consistency with human rights.

The Office's purpose reflects the objects set out in s 4 of the IGIS Act, which states that the IGIS's role is:

- To assist ministers in the oversight and review of:
 - the compliance with the law by, and the propriety of particular activities of, the intelligence agencies
 - the effectiveness and appropriateness of the procedures of those agencies relating to the legality or propriety of their activities
 - certain other aspects of the activities and procedures of those agencies.
- To assist ministers in ensuring that the activities of those agencies are consistent with human rights.
- To assist ministers in investigating intelligence or security matters relating to Commonwealth agencies, including agencies other than intelligence agencies.
- To allow for review of certain directions given to the Australian Security Intelligence Organisation (ASIO) by the responsible minister for ASIO.
- To assist the Government in assuring the parliament and the public that intelligence and security matters relating to Commonwealth agencies are open to scrutiny, in particular the activities and procedures of the intelligence agencies.

Our approach

Independent and impartial



Independence is fundamental to the Inspector-General's role and the role of the Office of the Inspector-General of Intelligence and Security. This includes independence in selecting matters for inspection or inquiry, as well as in undertaking and reporting on those activities. We have direct access to intelligence agency systems and are able to retrieve and check information independently. Our approach is impartial and our assessments are unbiased.

Astute and informed

Each of the intelligence agencies we oversee has its individual mandate. To target our inspections and inquiries effectively and efficiently, we need to understand the purpose and functions of each of the intelligence agencies as well as their operational planning, risk management and approach to compliance. We also need to have a sound understanding of the techniques and technologies used by the agencies to obtain, analyse and disseminate intelligence. Being well-informed allows us to target our oversight resources to the areas of greatest risk.



Measured



We appreciate the complex environment in which intelligence agencies operate and we accept that at times errors may occur. We identify errors and possible problems, and encourage agencies to self-report breaches and potential breaches of legislation and propriety. Our risk-based approach targets activities of high risk and activities with the potential to adversely affect the lives or rights of Australians. We consider an agency's internal control mechanisms as well as its history of compliance and reporting. The focus is on identifying serious, systemic or cultural problems in the activities of agencies within our jurisdiction.

Open

We make as much information public as possible, however, a large part of the information that IGIS deals with is classified and cannot be released publicly. Nevertheless, we include as much information as we can about our activities, including oversight of intelligence agency activities, in our annual report, unclassified inquiry reports on our website, and in responses to complaints.



Influential



IGIS oversight is a key part of the oversight framework within which intelligence agencies operate. Inspections and inquiries make a positive contribution to compliance; they lead to effective changes in agency processes and assist in fostering a culture of compliance. Important to these outcomes is that we work cooperatively with other oversight bodies to work effectively in areas of overlap. Our submissions to parliamentary committees contribute to informed debate about the activities of the agencies as well as the policies reflected in those activities.

About us

Established under the IGIS Act, the role of the Inspector-General is to assist ministers in overseeing and reviewing the activities of the six intelligence agencies under IGIS jurisdiction (the intelligence agencies) for legality, propriety, and consistency with human rights.

We provide independent assurance for the Prime Minister, senior ministers, parliament and the public as to whether the intelligence agencies are acting in accordance with these principles. We do this by inspecting, inquiring into and reporting on agency activities.

As set out in the IGIS Act, the intelligence agencies IGIS oversees are:

- Office of National Intelligence (ONI)
- Australian Security Intelligence Organisation (ASIO)
- Australian Secret Intelligence Service (ASIS)
- Australian Signals Directorate (ASD)
- Australian Geospatial-Intelligence Organisation (AGO)
- Defence Intelligence Organisation (DIO)

In addition, the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* expanded IGIS's jurisdiction to include oversight of the use of network activity warrants (NAWs) by the Australian Criminal Intelligence Commission (ACIC) and the Australian Federal Police (AFP).

We undertake regular, proactive inspections of the intelligence agencies, and conduct inquiries. Inquiries can be undertaken in response to complaints, of the Inspector-General's own motion, or at the request of ministers. When undertaking inquiries, IGIS has investigative powers similar to those of a Royal Commission, including the power to compel persons to answer questions and produce documents, and to take sworn evidence.

As part of our oversight of the activities of intelligence agencies and public assurance role, we can also inquire into complaints made about ASIS, ASIO, AGO and ASD, or the use of NAWs by the AFP and ACIC. Complaints can be made by a member of the public, or by a current or former employee of an intelligence agency, about the activities of an intelligence agency. Details about individual complaints and their resolution are not made public by our Office for privacy reasons.

The Inspector-General has functions and responsibilities under the *Public Interest Disclosure Act 2013* (PID Act) relating to disclosures about the intelligence agencies. In addition, the Inspector-General has a specific role under the *Freedom of Information Act 1982* (FOI Act) and the *Archives Act 1983* (Archives Act) to provide evidence on the damage that may be caused by the disclosure of certain material in disputed matters.

We recognise that our oversight processes must be as visible and transparent as possible to provide assurance that agency activities are open to robust scrutiny. Providing this assurance relies on us being respected as a credible and independent oversight authority. Accordingly, we continue to make public as much of our work as is possible within appropriate security constraints.

Our key activities

We deliver on our purpose through our key activities. The key activities reflect our prescribed role as set out in the IGIS Act. The Office is supported in undertaking these key activities by our corporate, legal and governance teams.



Inquiries and preliminary inquiries

Conducting inquiries is a core function and is the most formal activity we undertake to review the operations of intelligence agencies. An inquiry may be initiated by the Inspector-General of their own motion (which may in some cases be in response to a complaint or a public interest disclosure [PID]) or at the request of the Attorney-General, the relevant responsible minister or the Prime Minister. A preliminary inquiry may be initiated by the Inspector-General into the action of an intelligence agency, either in connection with a complaint, a PID, or of the Inspector-General's own motion. This process provides the means for the Inspector-General to make preliminary investigations and to determine whether further inquiry into the action is necessary. An inquiry or preliminary inquiry can look proactively at an issue or area of agency activity that may pose a significant risk, or reactively based on a previous inspection, compliance incident or complaint.

Risk-based proactive inspections

Conducting regular, proactive, and independent inspections of the legality, propriety and human rights implications of intelligence agency activities and compliance incidents is a key part of our approach to oversight. We prioritise these inspections based on risk. We consider many factors when assessing this risk including the impact on Australian persons or on Australia's domestic and foreign relationships, and whether similar activity has raised previous concerns. In practice, this means that focus is often on an agency's most intrusive and sensitive activities. Our inspections are carried out by inspection teams, each specialising in the oversight of one or more of the intelligence agencies. To support these inspections, the intelligence agencies self-report instances of potential non-compliance and provide us with advice of the context in which the activities were conducted. Reports of key inspections and other activities are provided to each relevant responsible minister.



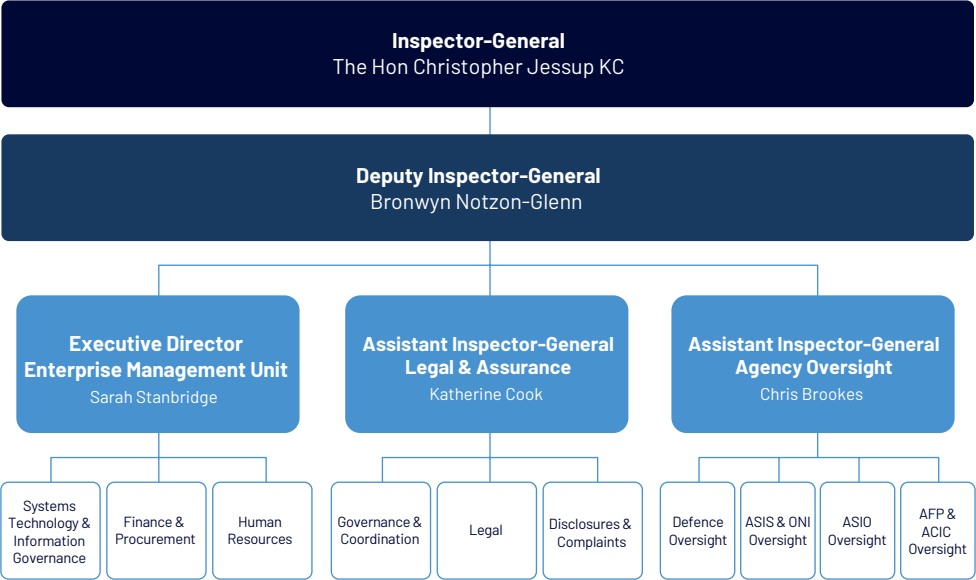
Complaints and public interest disclosures

We receive contacts from a range of people – including current or former staff of the intelligence agencies, people who have had dealings with the agencies, and others. These contacts are mostly initiated through our website. Once a contact is assessed as a complaint within our jurisdiction, it is examined in accordance with set procedures. A complaint may be resolved informally, be subject to a preliminary inquiry or may proceed to an inquiry.

In the case of conduct that relates to an intelligence agency, certain officers of the IGIS are authorised internal recipients for the purposes of the PID Act. These officers, and the Inspector-General, are able to receive disclosures of information concerning such conduct, and then determine if it is appropriate either to allocate the handling of the disclosure to one or more of the agencies, or to the Inspector-General, to handle the investigation of the disclosure.

Organisation chart

Figure 2.1: IGIS organisational structure at 30 June 2023



Providing assurance

“To assist the Government in assuring the Parliament and the public that intelligence and security matters relating to Commonwealth agencies are open to scrutiny, in particular the activities and procedures of intelligence agencies.” – IGIS Act

Assisting ministers

Before commencing an inquiry into an intelligence agency, the Inspector-General is required under the IGIS Act to notify the minister responsible for that agency. A copy of the final inquiry report must be provided to the responsible minister. The IGIS Act also provides that the Inspector-General may report to ministers if the actions taken by an agency in response to recommendations set out in an inquiry report are not adequate, appropriate and sufficiently timely. In 2022–23, no occasion arose for a report on inadequate action.

Under s 25A of the IGIS Act, the Inspector-General may report to the responsible minister on a completed inspection of an intelligence agency. In 2022–23, the Inspector-General provided one s 25A inspection report to a minister.

Additionally, the Inspector-General wrote twice to each responsible minister to provide updates regarding the Office’s inspection and review, disclosures and complaints, and legislative development activities relevant to the agency or agencies in their portfolio. The Inspector-General also wrote twice to the Attorney-General to provide a similar update on the Office’s activities related to all agencies within our jurisdiction.

The Inspector-General and IGIS officers also met with responsible ministers and their staff to discuss the work of the Office and how it conducts inspection and review activities.

During 2022–23, no requests were made by the Prime Minister or ministers for the Inspector-General to conduct an inquiry under the IGIS Act.

Assuring parliament

The Inspector-General regularly makes submissions to parliamentary inquiries and reviews of national security legislation and other matters. Consistent with established practice, the Inspector-General’s submissions make observations in the context of the Office’s oversight and review role, but do not comment on the policies underpinning the bills.

Parliamentary Joint Committee on Intelligence and Security (PJCIS)

During 2022–23, the Inspector-General and senior staff appeared before the PJCIS in public hearings into the review of:

- the *Counter-Terrorism (Temporary Exclusion Orders) Act 2019*
- the Inspector-General of Intelligence and Security and Other Legislation Amendment (Modernisation) Bill 2022
- the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 2) Bill 2023.

Table 2.1: 2022–23 IGIS submissions to PJCIS

IGIS submissions to PJCIS
Submission 1 to the <i>Review of the Inspector-General of Intelligence and Security and Other Legislation Amendment (Modernisation) Bill 2022</i> by the Parliamentary Joint Committee on Intelligence and Security.
Submission 7 to the <i>Review of Administration and Expenditure No. 20 (2021–2022)</i> by the Parliamentary Joint Committee on Intelligence and Security.
Submission 4 to the <i>Review of the Australian Security Intelligence Organisation Amendment Bill 2023</i> by the Parliamentary Joint Committee on Intelligence and Security.
Submission 5 to the <i>Review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 2) Bill 2023</i> by the Parliamentary Joint Committee on Intelligence and Security.

Legal and Constitutional Affairs Legislation Committee

In 2022–23, the Office made 2 submissions to the Legal and Constitutional Affairs Legislation Committee, both of which are available on the Parliament of Australia website. One can be found at Submission 10 to the Committee’s inquiry into the Anti-Discrimination and Human Rights Legislation Amendment (Respect at Work) Bill 2022. The other can be found at Submission 3 to the Committee’s inquiry into the Public Interest Disclosure Amendment (Review) Bill 2022.

Evidence to the AAT and the Australian Information Commissioner

Under the Archives Act and the FOI Act, the Inspector-General may be called on to provide the Administrative Appeals Tribunal (AAT) and the Australian Information Commissioner with expert evidence concerning national security, defence, international relations and confidential foreign government communications.

The FOI Act provides a number of exemptions to the requirement for government agencies to provide documents. One of the exemptions applies to documents affecting national security, defence, or international relations. Before deciding that a document is not exempt under this provision, the AAT and the Australian Information Commissioner are required to seek evidence from the Inspector-General. There are equivalent provisions in the Archives Act for the AAT. The Inspector-General is not required to give evidence if, in the Inspector-General’s opinion, they are not appropriately qualified to do so.

During 2022–23, the Inspector-General received one request for evidence from the Australian Information Commissioner, in relation to FOI exemptions.

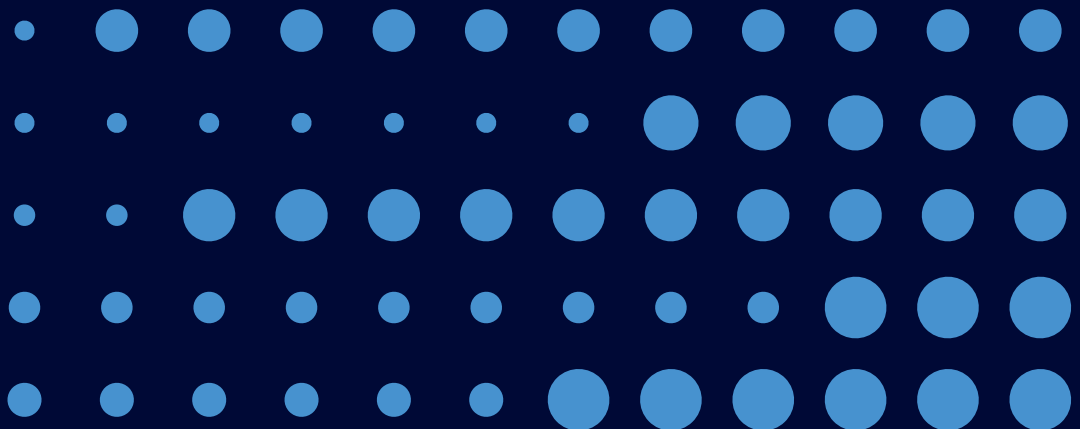
Informing the public

A purpose of the Inspector-General under the IGIS Act is to assist the government in assuring the public that intelligence and security matters relating to Commonwealth agencies are open to scrutiny, in particular the activities and procedures of intelligence agencies. We do this by making unclassified information about our activities publicly available where possible – such as on our website and through other activities such as our engagement program.

We conduct a program of presentations to the broader community. This includes presentations to groups who have an interest in national security and intelligence matters, such as those who study and research in the area. In 2022–23, senior staff presented at a number of public forums, including university lectures, on the role of the Office.

Section Three

Annual Performance Statement



2022–23 Annual Performance Statement

Statement by the accountable authority

As the Inspector-General and accountable authority for the Office of the Inspector-General of Intelligence and Security, I present IGIS's annual performance statement for the financial year 2022–23, as required under paragraph 39(1)(a) of the PGPA Act and incorporating the additional requirements under s 35 of the IGIS Act.

In my opinion, these annual performance statements are based on properly maintained records, accurately reflect the performance of the entity, and comply with subsection 39(2) of the PGPA Act.



The Hon Christopher Jessup KC
Inspector-General of Intelligence and Security

Results

The Office of the IGIS's performance framework is set out in our Corporate Plan 2022–23 and the Portfolio Budget Statements (PBS). In preparing the annual performance statement, we draw data from our corporate record keeping systems.

Reporting framework

The PBS set out the outcome that government seeks from IGIS in meeting the objects of the IGIS Act.

The Office of the Inspector-General of Intelligence and Security outcome is:

Independent assurance for the Prime Minister, ministers, parliament and public as to whether Australia's intelligence and security agencies act legally and with propriety by inspecting, inquiring into and reporting on their activities.

The 'Office of the Inspector-General of Intelligence and Security' is the only program identified in the PBS as contributing to this outcome.





Figure 3.1: IGIS reporting framework



2022–23 Performance Review

In 2022–23, the Office fully achieved 4 of its 6 objectives, and identified room for improvement against the other 2 objectives. The Office fully or substantially achieved 8 of the 9 performance measures identified in the 2022–23 Corporate Plan. Underlying the Office’s assessed performance on each Key Performance Indicator is qualitative and quantitative data, evidence, and explanations outlining the circumstances that contributed to each assessment. This data and reasoning informs the analysis provided for each Objective.





The Office is confident that this approach has resulted in an accurate and meaningful representation of our performance against our objectives, and accounts for the highly varied and complex nature of the inquiry, inspection, complaints and PID work undertaken by this Office.

<div></div> <div>Objective 1: Inquiries Through in-depth inquiries into specific issues or activities, provide assurance to ministers, parliament, and to the extent possible the public that operational activities of agencies are undertaken legally, with propriety and consistent with human rights obligations.</div>		
Performance Measure	Key Performance Indicators	Result
1.1 Conduct inquiries efficiently and effectively	The draft report for an inquiry is provided to the responsible minister and/or the head of the relevant agency and/or the Secretary of Defence in a timely manner following completion of information gathering.	 Substantially Achieved
	The final report for an inquiry, incorporating comments (or after the passing of a reasonable time without the receipt of comments) is provided to the responsible minister and/or the head of the relevant agency and/or the Secretary of Defence in a timely manner.	 Achieved
	The final report for an inquiry clearly identifies any findings and recommendations, and promotes meaningful reviews of policy, process, procedure, training or technology in an agency to improve legality and propriety.	 Achieved
	Overall assessment	Achieved



Objective 1: Inquiries

Through in-depth inquiries into specific issues or activities, provide assurance to ministers, parliament, and to the extent possible the public that operational activities of agencies are undertaken legally, with propriety and consistent with human rights obligations.

Performance Measure	Key Performance Indicators	Result
1.2 Conduct inquiries consistent with the IGIS Act	Before the commencement of an inquiry, the responsible minister and/or the head of the relevant agency and/or the Secretary of Defence (as required) were informed. [IGIS Act, s 15]	 Achieved
	Before the commencement of an inquiry, regard was had to the functions of, and consideration was given to consulting, the Auditor-General and/or the Ombudsman. [IGIS Act, s 16]	 Achieved
	When preparing a report, any opinions that are critical of an individual or agency's actions or activities was provided to the individual, agency head or responsible minister for comment before completion. [IGIS Act, s 17]	 Achieved
	The final report from an inquiry was provided to the agency head and responsible minister. [IGIS Act, s 22]	 Achieved
	Overall assessment	Achieved

Analysis

During 2022–23, the Office achieved its objective to provide ministers, parliament, and to the extent possible the public, with assurance gained through in-depth inquiries into specific issues and activities that the operational activities of intelligence agencies are undertaken legally, with propriety and consistent with human rights.

Measure 1.1 is overall assessed as achieved. Inquiry reports that have been finalised in 2022–23 have been provided to the responsible minister or head of agency in 7 working days or under, following feedback on the draft report, and the reports have clearly identified findings and recommendations, promoting meaningful reviews of policy and procedures in the agencies to which they refer. Draft reports for inquiries have been provided to agency heads; however, this provision occurred slower than intended for both of the inquiries completed in the reporting period.

Measure 1.2 is assessed as achieved. Before the commencement of each inquiry completed in 2022–23, the responsible minister or head of agency was informed, and consultation with the Auditor-General and the Ombudsman was considered. As required by the IGIS Act, agency heads were given the opportunity to comment on relevant draft reports before completion. The final reports from all inquiries completed in the reporting period were provided to both the relevant agency heads and ministers.

Section 6 provides a detailed overview of the Office's inquiries during the reporting period.



Objective 2: Inspections

Through risk-based independent inspections, provide assurance to ministers, parliament and to the extent possible the public that operational activities of agencies are undertaken legally, with propriety and consistent with human rights obligations.

Performance Measure	Key Performance Indicators	Result
2.1 Conduct inspections efficiently and effectively	Annual risk-based inspection plans are developed by July for each agency in jurisdiction.	Achieved
	All inspection activities in the inspection plan are delivered during the annual cycle.	Substantially Achieved
	Preliminary investigations into proactively reported compliance incidents are completed in a timely manner.	Achieved
	Inspection outcomes, including findings and recommendations, are clearly communicated to the agency and promote meaningful reviews of policy, process, procedure, training or technology to improve legality and propriety.	Achieved
Overall assessment		Achieved
2.2 Conduct inspections consistent with the IGIS Act	Responsible ministers are provided with a biannual report outlining the key inspection activities each year. [IGIS Act, s 25A]	Achieved
	Agency heads are provided with an annual inspection plan outlining planned inspection activities in July. [IGIS Act, s 9A(1)]	Achieved
Overall assessment		Achieved

Analysis

During 2022–23, the Office achieved its objective to provide ministers, parliament, and to the extent possible the public, with assurance gained through risk-based independent inspections that the operational activities of Australia’s intelligence agencies are undertaken legally, with propriety, and consistent with human rights obligations.

Measure 2.1 is holistically assessed as achieved; annual inspection plans for each agency were developed by July 2022, and preliminary investigations into proactively reported compliance incidents were completed in a timely manner. To confirm that inspection outcomes were communicated clearly and promoted meaningful agency reviews, the Office undertook follow-up inspections of agencies’ implementation of recommendations and in the majority of cases identified meaningful action to address prior findings.

The indicator regarding delivery of all inspection activities in the inspection plan during the annual cycle is assessed as substantially achieved because one planned inspection in one of the 6 agencies the Office oversees was not completed due to the prioritisation of resources to the conduct of an inquiry. The decision to reallocate resources was made after careful consideration of organisational priorities and risk tolerance.





Measure 2.2 is assessed as achieved; each agency head was provided with an annual inspection plan in July 2022, and responsible ministers were provided with biannual reports in September 2022 and June 2023.

Section 6 provides a detailed overview of the Office’s inspection activity during the reporting period.



Objective 3: Complaints

Investigate complaints made by the public, or by current or former staff of an intelligence agency, about the activities of an intelligence agency.

Performance Measure	Key Performance Indicators	Result
3.1 Investigate complaints efficiently and effectively, and consistent with the IGIS Act	Where there has been no, or no further, inquiry into a complaint the complainant has been informed in a timely manner. [IGIS Act, s 12]	 Achieved
	Following an inquiry, a response relating to the inquiry is given to the complainant and to the responsible minister in a timely manner. [IGIS Act, s 23]	 Achieved
	A timely decision is made after receipt of a matter that: <ul style="list-style-type: none">• the matter is not within authority; or• the complaint is within authority, but there will be no inquiry; or• there will be an inquiry. [IGIS Act, s 11]	 Substantially Achieved
	The agency head, and the responsible minister, are informed at least once in the relevant year of the complaints where there were no, or no further, inquiries. [IGIS Act, s 12]	 Achieved
	Overall assessment	Achieved

Analysis

During 2022–23, the Office achieved its objective to investigate complaints made by the public, or by current or former staff of an intelligence agency, about the activities of an intelligence agency. Measure 3.1 is overall assessed as achieved.

The Office received 34 complaints during the year that were within IGIS's jurisdiction. The Office also received 70 visa or citizenship complaints. In addition, the Office considered more than 599 additional matters to determine whether they fell within the Inspector-General's jurisdiction.

In 2022–23, one inquiry in response to a complaint was commenced. The inquiry was ongoing at the end of the reporting period.

For the complaints that were finalised in the reporting period, an outcome was provided to the complainant in a timely manner.

Agency heads were informed of complaints where there were no, or no further, inquiries, while responsible ministers are informed of the same via biannual ministerial letters.

The Office continues to improve its complaints handling and triaging processes.



Objective 4: Public interest disclosures

Receive and, where appropriate, investigate authorised disclosures about suspected wrongdoing within an intelligence agency.

Performance Measure	Key Performance Indicators	Result
4.1 Public interest disclosures are handled efficiently and effectively, and consistent with the PID Act	After the receipt of a disclosure, a decision whether there is a reasonable basis on which to consider the disclosure to be an internal disclosure is made within a timely manner. [PID Act, s 43(2)]	 Substantially Achieved
	After receipt of a disclosure, best endeavours are made to allocate the handling of the disclosure in a timely manner. [PID Act, s 43(5)]	 Substantially Achieved
	After the allocation of a disclosure to the Inspector-General, the discloser is informed in a timely manner that: <ul style="list-style-type: none">• the disclosure will be investigated, and whether under the PID Act or the IGIS Act; or• the disclosure will not be investigated. [PID Act, ss 48, 49, 50]	 Achieved
	After the allocation of a disclosure to the Inspector-General and decision to investigate the matter under the PID Act, the investigation is completed in a timely manner. [PID Act, ss 48, 49, 52]	 Achieved
	After preparation of the report, a copy is given to the discloser in a timely manner. [PID Act, s 51(4)]	 Achieved
	Overall assessment	Substantially Achieved

Analysis

During 2022–23, the Office substantially achieved its objective to receive and, where appropriate, investigate disclosures about suspected wrongdoing within an intelligence agency.

In 2022–23, the Office directly received 6 disclosures relating to the intelligence agencies under the PID Act, 2 of which it allocated to itself, and 4 it allocated to other agencies. The Office received notification of 5 disclosures made to intelligence agencies, as required by the PID Act, but none of these were allocated to the Office.

In cases where disclosures were allocated to the Office, the discloser was notified in a timely manner (where possible; anonymous disclosers are unable to be notified) that the disclosure would or would not be investigated. Of the 2 disclosures that were allocated to the Inspector-General in 2022–23, both investigations remained underway at the end of the reporting period.

One disclosure investigation that was allocated in 2021–22 was completed in the current reporting period. A copy of the report was provided to the discloser.

The often complex interplay between the IGIS Act and the PID Act and the intricate and sensitive nature of many of the complaints made to the Office, including the need to obtain additional information after the initial complaint is made, means it can take some time for a disclosure to be allocated and investigated under the PID Act.






Further, given the seriousness and sensitivity with which the Office treats disclosure investigations, the volume of materials gathered, and logistical matters that can arise in obtaining classified information (including from disclosers), it can take an extended period for the Office to undertake an investigation. The Office makes every effort to provide disclosers with regular updates as to the progress of the relevant investigation, where applicable.

The Office continues to streamline and strengthen its disclosure processes.



Objective 5: Assurance

Provide ministers, parliament and to the extent possible the public, assurance that intelligence and security matters relating to Commonwealth agencies are open to scrutiny, in particular the activities and procedures of intelligence agencies.

Performance Measure	Key Performance Indicators	Result
5.1 Provide effective and impartial advice on matters relating to the activities of intelligence agencies	Provide submissions to parliamentary inquiries, hearings and other reviews of national security matters.	 Achieved
	Provide comment on the appropriate oversight and accountability requirements relating to the powers of intelligence and security agencies in draft legislation.	 Achieved
	Produce a publicly available annual report that provides transparency of inspection, inquiry, complaint and PID activities and findings, with consideration for protective security requirements, for each agency.	 Achieved
	Deliver presentations and engage with the public and national security experts in Australia and internationally.	 Achieved
	IGIS executive participate in at least biannual meetings with each agency's senior officers to understand agency priorities and share oversight key issues and findings.	 Achieved
Overall assessment		Achieved

Analysis

During 2022–23, the Office achieved its objective to provide ministers, parliament and – to the extent possible – the public assurance that the activities and procedures of intelligence agencies are open to scrutiny. In the reporting period, the Office provided multiple submissions to parliamentary inquiries, hearings and other reviews of national security matters, as detailed on pages 11–12 of Section 2. The Office also provided comment on draft legislation relating to the powers of intelligence and security agencies, and relating to the introduction or reform of oversight and accountability structures.

The Office's Annual Report for 2021–22 is publicly available on the Office's website and transparency.gov.au. The report provided as much detail as possible – with consideration for protective security requirements – regarding inspection and inquiry activities into each agency, as well as complaint and PID findings.

During 2022–23, senior IGIS officers delivered a number of presentations to the public or national security experts in Australia. On the international stage, the Office delivered presentations and led working groups in multilateral fora such as the Five-Eyes Intelligence Oversight and Review Council (FIORC), and hosted short-term visits for bilateral partners.

In the reporting period, the Office participated in biannual meetings with 2 agencies and triannual meetings with the other 4 agencies in our jurisdiction. These meetings included visits to domestic offices and facilities, and the provision of briefings to the Office on a range of topics relevant to agency priorities. Both of these elements assist the Office to better target oversight activities based on a deeper understanding of the agencies' activities and operating environment.



Objective 6: Organisational capabilities

Enhance organisational capabilities to enable an expanding workforce to undertake the key activities of inquiries, inspections, complaints and public interest disclosures.

Performance Measure	Key Performance Indicators	Result
6.1 Develop an expanded, diverse and skilled workforce	Development and implementation of a detailed recruitment and retention plan to attract and retain specialist expertise in a competitive market.	 Partially Achieved
	Development and implementation of a learning and development (L&D) program that will integrate existing in-house and National Intelligence Community (NIC) L&D activities with broader academic and specialist training opportunities.	 Substantially Achieved
	Continued commitment to diversity and inclusion (D&I) initiatives including an active D&I Committee, development of a Reconciliation Action Plan, and commitment to practical D&I training and recruitment initiatives.	 Achieved
Overall assessment		Partially Achieved
6.2 Organisational capabilities to meet future requirements	Physical and ICT infrastructure continue to evolve in step with the agency's growth.	 Substantially Achieved
	Implementation of a new information governance framework and supporting architecture, including a dedicated intranet, and continued transition from hard-copy to digital records in line with National Archives of Australia policies.	 Substantially Achieved
Overall assessment		Substantially Achieved

Analysis

In 2022–23, the Office achieved mixed results for its objective to enhance organisational capabilities to enable its expanding workforce to undertake key activities.

Measure 6.1 is assessed as partially achieved. Progress towards developing an expanded, diverse and skilled workforce has been made against some elements, but these efforts have not yet delivered measurable recruitment and retention results in a competitive market. The Office has taken significant steps towards attracting and retaining the required expertise, such as: launching a talent register on the Office's website; implementing a recruitment calendar for annual recruitment rounds for critical, hard to fill roles; and engaging a specialist recruitment agency to implement new approaches to identifying and recruiting candidates.

However, the Office's limited resourcing and high volume of business as usual activity has meant that further work is required to bring these recruitment and retention initiatives to fruition, and to develop a Recruitment and Retention Plan.

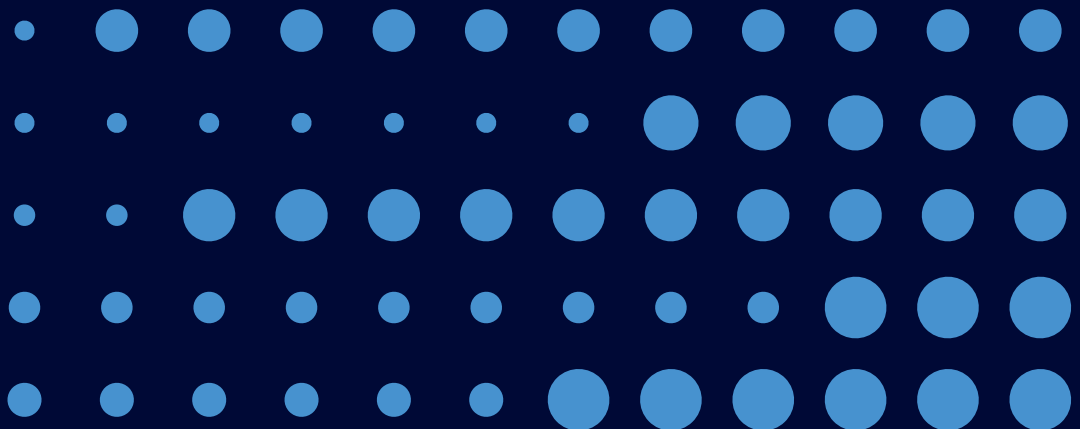
In the L&D space, the Office's Participating Agency status at the Australian National University's National Security College has already started delivering benefits, with a number of staff attending executive development programs in early 2023, and further training is scheduled for FY 2023–24.

In the reporting period, the Office demonstrated continued commitment to D&I initiatives, having held more than 10 Diversity and Inclusion Committee meetings and coordinated the Office's participation in a variety of activities celebrating and acknowledging diversity, such as NAIDOC Week, Wear it Purple Day, International Day of People with a Disability, and International Women's Day. The Office's Reconciliation Action Plan has been consulted with staff and Reconciliation Australia, and is due for delivery early in FY 2023–24. To embed values of diversity and inclusion in the Office, it is mandatory for staff to complete at least one D&I training course per year. Consideration of D&I recruitment initiatives has begun in FY 2022–23, and the Office will pursue these further in the next financial year.

Measure 6.2 is assessed as substantially achieved. The Office's physical and ICT infrastructure is continuing to evolve with the Office's growth – for example, the Office's PROTECTED laptop fleet has been refreshed, and a review of other network systems is underway – however, some intended activities have been delayed due to vacancies in critical ICT roles. Similarly, progress on implementing a new information governance framework was delayed as the Office was without an Assistant Director Information Governance until the last quarter of the reporting period. Despite this, the Office successfully built and delivered a dedicated PROTECTED intranet for the Office. The Office continues to undertake enhancements to its governance and management of digital information assets on both the PROTECTED network and the classified Local Area Network.

Section Four

Management and accountability



Our staff and culture

We have a strong commitment to individual and organisational excellence. We invest in our people, and foster and actively promote an inclusive and diverse workplace.

IGIS officers are subject to Australian Public Service (APS) values, employment principles and the Code of Conduct. This underpins what is expected of all staff in terms of behaviour and conduct. IGIS officers understand their responsibilities as Australian public servants and representatives of the Office.

Diversity and inclusion

The Office has a strong commitment to D&I, reflecting the importance we place on our people and on creating a workplace culture in which every employee is valued and respected for their contribution.

To support this, the Diversity and Inclusion Committee (the Committee) progresses initiatives in the Office that aim to strengthen and reinforce a workplace culture where all forms of diversity are valued and respected. The Committee is co-chaired by the D&I Champion and D&I Chair, and includes volunteer members from across the Office. The Committee plays a key role in providing strategic advice on the Office's inclusion and diversity strategy.

The Committee works closely with the IGIS Women's Network as well as with colleagues in the Attorney-General's Department (AGD), the NIC, and the wider APS, drawing on these larger networks to support, enable and add to our existing efforts.

During 2022-23, the Committee focused on finalising the Office's Reconciliation Action Plan, embedding D&I into office culture and planning, and building the Office's understanding of D&I issues through events, resource packs and education. A key driver of the Committee's activities in 2022-23 was the office-wide D&I Health Check the Committee ran in early 2022. The D&I Health Check highlighted positives regarding the Office's culture but – more importantly – identified key areas for improvement. The Committee has used this information to provide recommendations to the Office's Executive Board to inform and prioritise organisational change and efforts, and has continued to embrace a consultative approach with staff through drop-in days and other initiatives. As a small Committee in a small organisation, it is important that initiatives are targeted to deliver maximum impact.

This last year has laid the groundwork for 2023-24 and beyond; the Committee has prioritised formalising procedures, strengthening relationships with AGD and other agencies, continuing to embed D&I in the Office's day-to-day work, and building a strong foundation for the future.

Learning and development

The Office of the IGIS is a specialised agency whose people are central to achieving its strategic priorities. We appreciate the value of a diverse and inclusive workplace culture and the need to foster excellence and expertise in our staff.

Particular importance is placed on the retention of staff, flexible working arrangements, and workplace training to promote leadership skills and capability development. The Office's People Capability Framework details the skills, behaviours and attributes expected of IGIS officers and informs a range of workforce planning and management activities, including L&D, broadbanding and performance management. Internal training and professional development workshops for IGIS officers are supplemented by programs offered by the APS Academy, National Intelligence Academy and a range of other providers. In addition, the Office's "participating agency" status with the Australian National University's National Security College provides access to their highly sought-after executive development programs, in addition to their range of shorter professional development programs.

IGIS officers' individual performance agreements link roles and development goals with organisational needs and provide a mechanism for supervisors to guide and develop staff performance.

Census Action Plan

In early 2023, the Office developed a Census Action Plan (CAP) in response to results from IGIS's 2022 Australian Public Service Census (available on the IGIS website). This CAP was formulated in concert with feedback from the Office's Staff Consultative Committee, as well as strategic HR horizon scanning.

The CAP comprehensively responds to staff concerns across 5 core themes:

- leadership
- communication
- innovation
- productivity and work practices
- retention.

The Office is implementing strategies ranging from an IGIS Retention and Recruitment Plan through to a new Innovation Trial. To complement the CAP, the Office will be conducting periodic pulse surveying to evaluate staff responses to the various solutions. The Office will continue publishing its APS Census highlights report on the IGIS website annually, and will explore options to publish its annual CAP under APSC guidance and within information security requirements.

Innovation Trial

As part of the Office's Census Action Plan, staff requested a greater focus on innovation. In response, IGIS has commenced developing initiatives to improve and strengthen how the Office recognises innovation in a risk-embracing culture. Over 2024, initiatives are expected to be rolled out in consultation with staff.

Conversation series

The Margaret Stone Conversation Series, 'In conversation with ...', is a new initiative to showcase a series of informal conversations about a range of key issues relevant to the Office as an integrity agency, such as independence, issues relating to legality and propriety, and other matters. The conversation series brings IGIS officers together to engage with a variety of speakers to gain different perspectives, deepen their knowledge and develop their skills.

Oversight Capability Review

In the second half of 2021-22, the Office allocated a senior member of staff to undertake an Oversight Capability Review (the Review) to examine the practices, procedures and capabilities of the agency oversight area and provide practicable recommendations as to how it could remain fit-for-purpose. The Review recognised that the Office has been through a rapid period of expansion, and the nature of its work had evolved accordingly to be more risk-based and proactive in nature. In addition, the size, capability and operational breadth of the intelligence community has expanded and continues to evolve, and provides further impetus for our oversight capability to be as efficient and effective as possible.

The Review has been delivered and its recommendations endorsed by the Office's Executive Board. The Review found that our oversight capability was effective, while providing 23 recommendations to enhance efficiency and maximise effectiveness. Key recommendations identified opportunities to:

- enhance formal training and foundational guidance for new and existing oversight officers
- improve the Office's internal policies and procedures in order to enable more effective and efficient oversight activities
- further strengthen mechanisms of access to, and disclosure of, information with agencies to ensure the Office has consistent and timely accesses to enable its oversight activities
- enhance information sharing on oversight activities undertaken, and lessons learned, across the Office.

Implementation has begun, and a number of recommendations are already complete or underway. The Office's executive will maintain oversight of the review implementation through regular reporting. Delivery of the Review's recommendations has been identified as a key performance target in the 2023-24 Corporate Plan.

Technical Advisor role

Recommendation 173 of the *Comprehensive Review of the Legal Framework of the National Intelligence Community* (the Richardson Review) recommended that an independent panel should be established to provide technical expertise and assistance to the IGIS. In response to this recommendation, the Office has established and filled a dedicated Technical Advisor role, on an initial 12-month basis. The role will provide an interim technical advisory function to deliver advice and guidance to the Office's oversight activities, and inform decision-making regarding the Office's approach to engaging with technical advice, including how to best obtain technical advice independent from the agencies we oversee.

The interim Technical Advisor has already delivered value to the work of the Office. This has included contributing to a number of inspections and inquiries outlined in Section 6 of this Annual Report, and to the development of the Office's 2023-24 inspection plans for each agency in our jurisdiction. The Technical Advisor has also provided specialised advice in relation to some complaints received by the Office.

The Office will review the outcomes provided by the interim Technical Advisor position in the middle of the upcoming financial year and determine the most efficient and effective way to engage with independent technical advice in the future.

Organisational profile



41

ongoing employees*



9.7%

on part-time arrangements#



22%

on other flexible arrangements



100%

of staff are in Canberra

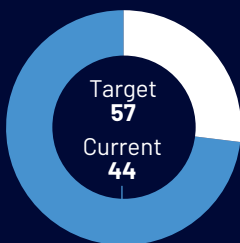
* Including 4.9% on long-term leave.

In 2021-22, 14% of employees were on part-time arrangements.

In 2022-23 and 2021-22, no staff were employed on a non-ongoing basis, no employees identified as indigenous, and no staff were based outside Canberra.

The Inspector-General is a statutory officer and therefore not an employee.

Average staffing level (ASL)



The Office did not reach its target ASL of 57 in the reporting period, due to a combination of:

- external labour market shortages
- challenges with the TSPV clearance pipeline
- staff separations.

A number of strategies and initiatives (detailed below) were implemented to address recruitment and retention challenges.

Recruitment environment

The Office continues to experience the impact of labour market shortages across a range of critical skill sets in both corporate and operational areas. The changing nature of work, digital transformation and increasing demand for skills has contributed to a competition for talent, which for the Office is made more challenging by the lengthy clearance process.

Workforce analytics and planning across the Office have enabled strategic discussions on how to address recruitment and retention challenges. Exploring and implementing new approaches to these challenges will enable the Office to grow to meet organisational requirements.

Recruitment activities:

This year, the Office conducted a significant number of recruitment campaigns to strengthen its workforce of specialist oversight and corporate officers.

- Several recruitment rounds were advertised and run for a variety of roles across the APS4-6 and EL1-2 levels.
- Bulk recruitment for operational roles was conducted.

These recruitment activities attracted large numbers of candidates and led to a surge in security clearance pipeline activity.

Exploring new approaches:

The Office has implemented creative recruitment strategies, such as:

- a temporary employment register
- a s 26 transfer website portal
- secondments across the NIC
- employee referral programs
- alternative recruitment pathways
- creative advertising.

The use of a multiclassification workforce is also being explored, with trial implementation proposed to begin in corporate teams.

Table 4.1: Overview of substantive IGIS staffing profile

APS classification (salary range 2022-23)	At 30 June 2023				As at 30 June 2022			
	Male	Female	Uses a different term	Total	Male	Female	Uses a different term	Total
APS Classification								
APS 4 (\$73,095 - \$79,529)	0	0	0	0	0	2	0	2
APS 5 (\$81,369 - \$88,265)	1	2	0	3	0	1	0	1
APS 6 (\$92,860 - \$104,354)	2	7	0	9	4	7	0	11
Executive Level 1 (\$112,169 - \$125,043)	7	10	0	17	11	12	0	23
Executive Level 2 (\$130,556 - \$155,380)	2	7	0	9	3	4	0	7
SES Band 1 (\$192,085 - \$220,245)	1	1	0	2	2	1	0	3
SES Band 2 (\$247,393 - \$280,752)	0	1	0	1	1	1	0	2
Total	13	28	0	41	21	28	0	49

N.B Some employee remuneration exceeded the nominal salary range for the employee's classification. Under the IGIS Enterprise Agreement, an existing Australian Government employee moving to the Office at the same classification level whose current base rate of pay exceeds the maximum IGIS pay point for that classification will be maintained on that base rate of pay until it is absorbed by IGIS's pay increases at the relevant classification level.

Employment frameworks

All IGIS officers are employed under the *Public Service Act 1999* (PS Act). Since 6 May 2020, all non-SES officer salaries and conditions were made under the *IGIS Enterprise Agreement 2020-2023*. Upon the expiry of this agreement on 6 May 2023, the Inspector-General signed into effect a Determination to vary the terms of the existing agreement to provide additional remuneration increases to non-SES officers. The Determination operates in conjunction with the *IGIS Enterprise Agreement 2020-2023*, relevant Commonwealth legislation, and the Office's policies and guidelines to define the terms and conditions of employment for non-SES officers. There are currently 3 SES officers employed in accordance with individual determinations under subsection 24(1) of the PS Act.

All IGIS officers receive a taxable annual allowance in recognition of the requirement to undergo regular and intrusive security clearance processes necessary to maintain a Positive Vetting clearance. The annual allowance is \$1,266.

Employees had access to a range of non-salary benefits such as salary sacrifice of additional superannuation and leased motor vehicles, flexible work arrangements, a study assistance program, a health and wellbeing allowance, and standard leave entitlements.

Executive remuneration

The Inspector-General is a statutory office holder. The Office has 3 SES positions: one SES Band 2 position and two SES Band 1 positions. The Office also has one Executive Director (EL 2) position leading the Enterprise Management Unit. All of these positions are designated as Key Management Personnel (KMP).

The terms and conditions of all SES officer employment, including salary, are set out in individual determinations. General performance discussions between the Inspector-General and SES occur during the year. The Inspector-General's remuneration is determined by the Remuneration Tribunal.

Key management personnel (KMP)

Executive remuneration

Table 4.3: Information about remuneration for key management personnel

Key management personnel									
Short-term benefits		Post-employment benefits		Other long-term benefits		Termination benefits			
Name	Position title	Base salary ¹	Other benefits and allowances ²	Superannuation contributions	Long service leave ³	Other long-term benefits	Termination	Termination benefits	Total remuneration
The Hon Christopher Jessup KC									
Inspector-General	(1 July 2022 to 30 June 2023)	453,689	108,027	25,292	-	-	-	-	587,007
Bronwyn Notzon-Glenn									
Deputy Inspector-General	(1 July 2022 to 30 June 2023)	270,682	29,597	49,498	6,705	-	-	-	356,482
Chris Brookes									
Assistant Inspector-General	(1 July 2022 to 30 June 2023)	178,157	29,597	39,855	4,878	-	-	-	252,488
Katherine Cook									
Assistant Inspector-General	(1 July 2022 to 30 June 2023)	234,631	29,597	47,253	5,734	-	-	-	317,215
Sarah Stanbridge									
Acting / Executive Director	(5 September 2022 to 30 June 2023)	149,389	3,501	26,545	3,849	-	-	-	183,284
Brad Fallen									
Acting / Executive Director	(1 July 2022 to 4 September 2022)	30,381	5,271	5,223	758	-	-	-	41,632

1. Base salary includes leave taken and the movement in annual leave provision—i.e. 4 weeks accrued annual leave less annual leave taken.

2. Other benefits and allowances include a motor vehicle allowance and car parking as part of SES remuneration packages, and housing and reunion allowances as part of the Inspector-Generals remuneration package.

3. Long service leave represents the movement in long service leave provision—i.e. 9 days accrued per annum less long service leave taken.

4. RMG 138 point 70 - "The total remuneration disclosed in accordance with the PGPA Rule should match the total remuneration disclosed in the notes to the financial statements."

All IGIS SES and Executive Director positions are key management personnel. No key management personnel or other highly paid staff received bonuses or termination benefits during the period.

Performance pay

The Office does not have a performance pay scheme.

Workplace health and safety

The Office is committed to promoting and sustaining a safe and healthy workplace, one that values inclusion and ensures a healthy, resilient and capable workforce. The Office encourages cooperation to promote and develop strategies to ensure health, safety and welfare at work. Workplace health and safety matters are addressed at the Executive Board, Leadership Group meetings, Audit Committee meetings and, as the need arises, directly with the Inspector-General through the Health and Safety Representative, SES, Directors and staff.

Throughout 2022–23, the Office continued to provide a range of health and wellbeing initiatives to staff, including:

- a wellbeing allowance
- undertaking ergonomic workstation assessments
- access to the annual AGD influenza vaccination program
- access to an Employee Assistance Program
- providing a range of flexible arrangements where possible.

No notifiable incidents resulting from undertakings carried out by the Office that would require reporting under the *Work Health and Safety Act 2011* (WHS Act) have occurred during the reporting period. No investigations were conducted relating to undertakings carried out by the Office and no notices were given to the Office under Part 10 of the WHS Act.

Disability reporting mechanism

Australia's Disability Strategy 2021–2031 is Australia's overarching framework for disability reform. It acts to ensure the principles underpinning the United Nations Convention on the Rights of Persons with Disabilities are incorporated into Australia's policies and programs that affect people with disability, their families and carers. Its vision is for an inclusive Australian society in which people with disability can fulfil their potential and it sets out practical changes that will assist people living with disability.

All levels of government will continue to be held accountable for the implementation of the strategy. As a very small agency the Office does not, for privacy reasons, publish statistical data on workforce diversity, including disability, but our data is included in APS reporting. Disability reporting is included in the APS Commission's State of the Service reports and the *APS Statistical Bulletin*. These reports are available at www.apsc.gov.au.

Corporate governance

The Office is committed to good governance and the highest standards of accountability, transparency and integrity.

The Office's corporate governance framework guides good governance and sound business practices across the Office. During 2022–23, the Office focused on embedding the governance framework that was implemented in May 2022 following a comprehensive governance review earlier that year.

Key components of our corporate governance framework include:

- strategic corporate planning
- performance monitoring and reporting processes
- governance committee structure
- audit and assurance activities
- risk management framework, systems and controls
- fraud prevention and control
- business continuity framework, policy and response.

To meet the objectives of each component, a number of committees have been established to support the Inspector-General and senior executives to fulfil their corporate and governance responsibilities. The committees provide a range of advice, and support the Office's operations to assist in key decision-making.

The Executive Board is the primary decision-making body of the Office. It is composed of the Office's senior executives and assists and supports the Inspector-General in managing: the delivery of strategy, budget and operational functions; oversight of risk and ensuring an appropriate system of internal control; and coordination of people and projects for the Office. The Executive Board also provides an opportunity for members to discuss the ongoing oversight activities carried out by the Office. In doing so, the Executive Board supports the Inspector-General in discharging their responsibilities as the accountable authority under the PGPA Act.

In addition to the Executive Board, committees have been established to support the Executive Board to meet their objectives and responsibilities. These committees are focused on core business areas, as well as enabling functions such as staff consultation, leadership, audit, and D&I. The ongoing cooperation and coordination of these committees with the Executive Board enables the effective governance of the Office and efficient business operations.

IGIS Audit Committee

The IGIS Audit Committee is established in accordance with the PGPA Act. The Audit Committee's role is to provide independent assurance and advice to the Inspector-General on the appropriateness of the Office's financial and performance reporting responsibilities, system of risk oversight and management, and system of internal control.

The membership and functions of the IGIS Audit Committee are structured according to the PGPA Act. The IGIS Audit Committee charter is available at:

https://www.igis.gov.au/sites/default/files/2022-07/IGIS_Audit_Committee_Charter_2021_0.pdf

The Inspector-General, Deputy Inspector-General, IGIS officers and Australian National Audit Office (ANAO) representatives may attend Audit Committee meetings to provide updates or observe. The Audit Committee meets at least 4 times a year.

Table 4.4: IGIS Audit Committee membership

Audit Committee member	Qualifications, knowledge, skills and experience	Meetings attended ¹	Total annual remuneration
Current members			
Ms Sarah Vandebroek Chair (External member)	Ms Vandebroek holds a Bachelor of Information Management, a Graduate Diploma in Accounting and is a Fellow of CPA Australia. Ms Vandebroek has held a range of senior roles in the Commonwealth Public Service including as a Chief Financial Officer and a Chief Operating Officer. Ms Vandebroek is the First Assistant Secretary of the Territories Division in the Department of Infrastructure, Transport, Regional Development, Communications and the Arts.	29 July 2022 17 October 2022 13 December 2022 16 February 2023 17 May 2023	Nil

Audit Committee member	Qualifications, knowledge, skills and experience	Meetings attended ¹	Total annual remuneration
Mr Stephen Moore (External member)	Mr Moore holds a Bachelor of Economics (Honours), Econometrics and Quantitative Economics and a Graduate Diploma (with merit) in Econometrics and Quantitative Economics, and is a fellow of the Australia and New Zealand School of Government Executive Fellows Program. Mr Moore has experience as a senior leader in public service agencies working on ICT security and applications, governance and customer experience, as well as experience in the private sector.	29 July 2022 17 October 2022 13 December 2022 16 February 2023 17 May 2023	\$3,630
Mr Peter Quiggin KC (External member)	Mr Quiggin holds a Bachelor of Laws, a Graduate Diploma in Professional Accounting, a Bachelor of Science, Computing and Maths and is a fellow of the Australian Institute of Company Directors. Mr Quiggin is a highly experienced former Commonwealth agency head (First Parliamentary Counsel) with extensive senior board member experience across government and not-for-profits.	29 July 2022 17 October 2022 13 December 2022 16 February 2023 17 May 2023	\$18,750

1. The Audit Committee meeting scheduled for 20 September 2022 was rescheduled due to unforeseen external circumstances. The meeting was subsequently held on 17 October 2022.

Internal audit

Internal audit provides independent and objective assurance and advice to the Inspector-General – through the Audit Committee – that the Office's system of internal control and risk management framework are operating in an efficient, effective, economical and ethical manner in respect of the areas reviewed. Much of the Office's focus during this reporting period was engaging with AGD in a joint procurement process to contract an external audit services provider to conduct an internal audit program. A contract was entered into during June 2023 and the initial focus will be on developing an internal audit plan in consultation with the Executive Board and the Audit Committee.

Stakeholders

We maintain strong and cooperative relationships with a range of agencies and entities both domestic and international.

Domestic engagement

Attorney-General's Department

The Office is part of the Attorney-General's portfolio and works collaboratively with AGD on a range of policy and legal issues. As a small agency, we are physically co-located within the AGD building and have a shared services arrangement with the department that supports some of our corporate capability. This includes some facilities maintenance, some physical security, and some ICT systems and capabilities.

Corporate support

In addition to the corporate support provided by AGD, ASD also provides some ICT system support. The Office accesses some financial services via the Cultural and Corporate Shared Services Centre provided by the National Museum of Australia.

Accountability and integrity agencies

The Office liaises with other Commonwealth accountability and integrity agencies to discuss matters of mutual interest, such as oversight processes, complaint handling, administrative improvement, implementation of legislative changes, and significant developments in relevant domestic and global issues. The Inspector-General attends Integrity Agencies Group meetings, which include the heads of integrity agencies and other relevant Commonwealth departments (with a similar forum held at the deputy level). The purpose of the Integrity Agencies Group is to lead coordination and enhancement of institutional integrity across the Commonwealth.

Australian Commission for Law Enforcement Integrity

The Office continued to liaise with the Australian Commission for Law Enforcement Integrity (ACLEI) regarding cooperative and complementary oversight arrangements in anticipation of any proposed changes to the Inspector-General's jurisdiction and in anticipation of ACLEI becoming part of the National Anti-Corruption Commission as of 1 July 2023, as well as on general oversight issues.

Australian Human Rights Commission

The Australian Human Rights Commission is required by ss 11(3) of the *Australian Human Rights Commission Act 1986* to refer to the Inspector-General any human rights and discrimination matters relating to an act or practice of security agencies. During 2022-23, the Australian Human Rights Commission did not refer any such matters to the Office.

Office of the Australian Information Commissioner

During 2022–23, the Office provided its final six-monthly report to the Australian Information Commissioner that covered the incidental collection, access, use and deletion of COVIDSafe app data by relevant intelligence agencies, and their policies and procedures in place relating to Part VIIIA of the *Privacy Act 1988* (Privacy Act). The COVIDSafe app has now been decommissioned and Part VIIIA of the Privacy Act has been repealed.

IGIS officers and Office of the Australian Information Commissioner discussed matters of mutual interest during the reporting period.

Office of the Commonwealth Ombudsman

The Office continued to engage regularly and meet with the Office of the Commonwealth Ombudsman on a wide range of issues. The responsibilities of the 2 offices are considered complementary and a memorandum of understanding exists between the two offices.

International engagement

The Office engages with international accountability and integrity agencies to discuss emerging issues and keep informed of developments in other jurisdictions.

Five-Eyes Intelligence Oversight and Review Council

In 2022–23, the Inspector-General and IGIS officers deepened engagement with the FIORC. FIORC is comprised of the following intelligence oversight, review and security entities of the Five-Eyes countries:

- the Office of the Inspector-General of Intelligence and Security of Australia
- the Office of the Intelligence Commissioner of Canada
- the National Security and Intelligence Review Agency of Canada
- the Commissioner of Intelligence Warrants of New Zealand
- the Office of the Inspector-General of Intelligence and Security of New Zealand
- the Investigatory Powers Commissioner's Office of the United Kingdom
- the Office of the Inspector General of the Intelligence Community of the United States.

Council members exchange views on subjects of mutual interest and concern. They compare best practices in review and oversight methodology, and explore areas where cooperation is appropriate. The Council encourages transparency to the greatest extent possible to enhance public trust, and maintains contact with political offices, oversight and review committees, and non-Five-Eyes countries, as appropriate.

The Council aims to meet in person at least once each year. After the 2021 annual meeting was held virtually due to COVID-19 restrictions, this reporting period Council members returned to an in-person meeting held over 4 days in November 2022, hosted in Washington DC by the Office of the Inspector General of the Intelligence Community of the United States. Sessions were held on topics including:

- oversight in a critical environment
- raising public awareness of the oversight mission
- whistleblowing and complaint processes.

Council members continue to meet every few months via teleconference, and progress opportunities for collaboration and knowledge-sharing through working groups. The next annual conference is planned to be held in Canada in late 2023.

Bilateral engagement

During the reporting period, the Office engaged bilaterally with international counterparts in a variety of ways and on a range of issues affecting the Office. For example, virtual discussions were held with Five-Eyes oversight agencies on recruitment and retention initiatives, and the Office hosted a member of Canada's National Security and Intelligence Review Agency (NSIRA) for a short-term visit in October 2022. The visit was valuable in building institutional links between the Office and NSIRA and identifying similarities, differences and opportunities in Australia's and Canada's operating environments and oversight approach.

Risk oversight and management

IGIS is committed to embedding a positive risk-aware culture that promotes proactive risk management and informed decision-making.

The identification and effective management of risk is an integral part of business planning and governance processes. The Office manages risk through its Risk Management Policy and Framework, which provides a structured and consistent approach to identifying, analysing and mitigating risk. Identifying risks and determining what the Office needs to have in place to reduce them to an acceptable level is vitally important in developing fraud and corruption control measures, business continuity arrangements and strategic plans for the Office.

The Office’s risk oversight and management tools include its Risk Management Framework, risk appetite and risk tolerance statements, Risk Register, Audit Committee reviews, Fraud & Corruption Control Plan, Business Continuity Plan, and Security Plan. The Risk Management Framework has been developed to make risk management efficient, effective and consistent.



The Risk Management Framework requires risk owners to be responsible for risks identified in the risk register, which includes responsibility for related controls and mitigation strategies. The Governance Directorate coordinates biannual reviews with risk owners which are considered by the Executive Board. In addition, the Audit Committee provides advice to the Inspector-General about the Office’s risk framework, governance, compliance and financial accountability. As mentioned on page 43, the Audit Committee will be informed by an internal audit plan that is tailored to the size and functions of a small agency, and will be supplied through externally contracted arrangements.

The Office monitors and reviews risk against the following categories:



The Office will continue to integrate, strengthen and embed risk management into its work. It is anticipated that the strategic risks being managed will change as a result of a range of factors including an expanding workforce, evolving jurisdiction, and changes in the national security environment. The Office will manage these risks through strong planning, building effective stakeholder relationships, strengthening the control framework, and review and updating of the risk register.

Ethical standards

During 2022–23, the Office continued its commitment to high ethical standards. High ethical standards across the Office are maintained through:

- APS integrity and values training
- mandatory online fraud training
- modelling of appropriate behaviours by the Office’s SES officers
- a requirement that all officers maintain a high-level security clearance
- annual declaration of known conflicts of interest by all officers
- incorporation of APS Values and Code of Conduct expectations in the Office’s Performance Agreement process.

The Office is a member of the APS Commission’s Ethics Contact Officer Network, and information and resources from this network are incorporated into broader agency communications.

Fraud control

The Office’s fraud control strategies comply with the Commonwealth Fraud Control Framework 2017 and the legislative requirements as defined in the PGPA Act.

The IGIS Fraud & Corruption Control Plan and Guidance 2022–24 provides the foundations of the Office’s fraud control framework. The Office completed a review of its fraud control measures in February 2023.

The Fraud & Corruption Control Plan and Guidance outlines the Office’s approach to managing fraud and corruption risks and ensures that IGIS establishes and maintains appropriate systems of risk oversight and management to prevent, detect, record and respond to fraud and corruption.

Any reports of possible fraud within or affecting the Office are examined promptly, confidentially, diligently and – where necessary – referred for investigation by an appropriate authority.

The Office had no reports of fraud in 2022–23.

External scrutiny

Reports of the Auditor-General, parliamentary committees or the Commonwealth Ombudsman

The ANAO completed an audit of the Office's financial statements for 2022–23. The independent auditor's report is presented in the financial statements section of this Annual Report.

The Office appeared before the Senate Legal and Constitutional Affairs Legislation Committee at its Estimates hearings in October 2022 and May 2023. The Office also attended public and private hearings of the PJCS and provided submissions on a range of inquiries to it. Where security classifications permit, the Office's submissions, responses to questions taken on notice (written and taken during hearings), and the transcripts of committee hearings are available on the Parliament of Australia website.

During the reporting period, the Office worked collaboratively with the ANAO and the Commonwealth Ombudsman.

Asset management

The management of Office assets is governed by internal policies and procedures on asset management that are based on government best practice. The Office maintains an asset register and a capital management plan. An annual stocktake is performed and frequent revaluation exercises are undertaken to maintain the accuracy of the information in the asset register, which is reported in the financial statements. The Office's fixed assets include office fit outs, purchased software and leasehold improvements.

Purchasing and procurement

Purchasing

The Commonwealth Procurement Rules, the Office's Accountable Authority Instructions, the PGPA Act and PGPA Rule provide the framework for the Office's decisions concerning the purchase of goods and services.

The Office's purchasing framework seeks to ensure:

- procurement methods are efficient, cost-effective and take account of the Office's security needs, specialised role and size
- value for money is always the primary guiding principle
- participation in mandatory whole-of-government coordinated procurement, such as travel and property services
- support for small and medium enterprise participation

- use of the Commonwealth Contracting Suite for low-risk procurements valued under \$200,000
- use of corporate credit cards when possible and appropriate, to allow more timely payment to suppliers.

The Office is committed to the continued development and support of Indigenous businesses, under the Commonwealth Indigenous Procurement Policy.

The Office 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.

Consultants

Consultants are engaged to investigate or diagnose a defined issue or problem, carry out defined reviews or evaluations, or provide independent advice or information to assist in the Office's decision-making. When deciding to engage a consultant, the Office requires decision-makers to consider the abilities and resources required for the task, the skills available internally, and the cost-effectiveness of engaging external expertise. The decision to engage a consultant is made in accordance with the PGPA Act and PGPA Rule, the Commonwealth Procurement Rules and relevant internal policies, including the Accountable Authority Instructions.

Annual reports contain information about actual expenditure on reportable consultancy contracts. Information on the value of reportable consultancy contracts is available on the AusTender website.

Details of the reportable new and ongoing consultancy contracts entered into during 2022–23 are shown in the following tables.

Table 4.5: Reportable consultancy contracts 2022–23

Reportable consultancy contracts 2022–23	Number	Expenditure (\$, GST inc.)
New contracts entered into during the reporting period	3	171,280.99
Ongoing contracts entered into during a previous reporting period	3	455,144.75
Total	6	626,425.74

Table 4.6: Reportable consultancy contract expenditure 2022–23

Name of organisation	Expenditure (\$, GST inc.)
Yardstick Advisory Pty Ltd (ABN 38 158 309 150)	418,244.75
Remote Pty Ltd (ABN 21 086 319 146)	80,470.49
Gillian Beaumont Recruitment Pty Ltd (ABN 58 107 780 683)	47,300.00
Humanify HR Consulting Pty Ltd (ABN 80 651 424 869)	43,510.50
PQQC Consulting (ABN 94 484 818 597)	18,750.00
Couch Creative (ABN 87 096 282 496)	18,150.00

During 2022–23, 3 new reportable consultancy contracts were entered into involving total actual expenditure of \$171,280.99. In addition, 3 ongoing reportable consultancy contracts were active during the period, involving total actual expenditure of \$455,144.75.

Contracts

Annual reports contain information about actual expenditure on reportable non-consultancy contracts. Information on the value of reportable non-consultancy contracts is available on the AusTender website.

Details of the new and ongoing reportable non-consultancy contracts entered into in 2022–23 are shown in the following tables.

Table 4.7: Reportable non-consultancy contracts 2022–23

Contract types	Number	Expenditure (\$, GST inc.)
New contracts entered into during the reporting period	8	234,485.32
Ongoing contracts entered into during a previous reporting period	2	64,949.22
Total	10	299,434.54

Table 4.8: Reportable non-consultancy contract expenditure 2022–23

Name of organisation	Expenditure (\$, GST inc.)
National Security College (ABN 52 234 063 906)	172,300.00
Planex (ABN 55 921 612 267)	41,523.90
The trustee of Typeyard Design and Advertising (ABN 98 488 952 348)	25,949.22
Reed International Books Australia Pty Ltd (ABN 70 001 002 357)	22,164.60
The Australian Institute of Company Directors (ABN 11 008 484 197)	20,298.00
Acronym IT (ABN 68 096 077 422)	17,198.82

Australian National Audit Office access clauses

The Office's use of the Commonwealth Contracting Suite ensures all contracts for procurements valued under \$200,000 include provisions allowing the Auditor-General to have access to contractor premises. In addition, all consultancy contracts over \$200,000 included ANAO access clauses.

Exempt contracts

IGIS publishes information on the value of contracts and consultancies on the AusTender website, but is not required to publish certain information on AusTender where it has been determined by the Inspector-General that such information would disclose exempt matters under the FOI Act. During 2022–23, IGIS exempted from publication 4 contracts with the total value of \$1,096,800.

Information Publication Scheme

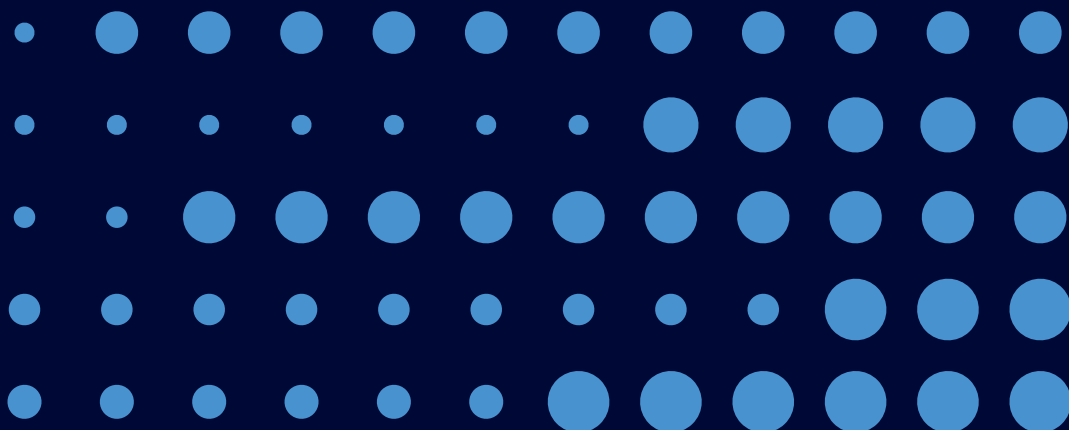
Australian Government agencies subject to the FOI Act are required to publish information to the public as part of the Information Publication Scheme (IPS). This requirement is in Part II of the FOI Act and has replaced the former requirement to publish a s 8 statement in an annual report. Each agency must display on its website a plan showing what information it publishes in accordance with the IPS requirements.

The Office of the IGIS is an exempt agency for the purposes of the FOI Act and as such the IPS does not apply to it.

Indexed file lists were published on IGIS's website in the reporting period in accordance with the Senate Continuing Order for Indexed File Lists (Harradine Order).

Section Five

Financial statements





INDEPENDENT AUDITOR'S REPORT

To the Attorney-General

Opinion

In my opinion, the financial statements of the Office of the Inspector-General of Intelligence and Security (the Entity) for the year ended 30 June 2023:

- (a) comply with Australian Accounting Standards – Simplified Disclosures 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 2023 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 as at 30 June 2023 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;
- 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 (including Independence Standards)* (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 Inspector-General of Intelligence and Security 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 – Simplified Disclosures and the rules made under the Act. The Inspector-General of Intelligence and Security is also responsible for such internal control as the Inspector-General of Intelligence and Security 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 Inspector-General of Intelligence and Security is responsible for assessing the ability of the Entity to continue as a going concern, taking into account whether the Entity's

GPO Box 707, Canberra ACT 2601
38 Sydney Avenue, Forrest ACT 2603
Phone (02) 6203 7300

operations will cease as a result of an administrative restructure or for any other reason. The Inspector-General of Intelligence and Security 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.

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



Clea Lewis

Executive Director

Delegate of the Auditor-General

Canberra

4 August 2023

CONTENTS

Certification

Primary financial statements

Statement of Comprehensive Income
Statement of Financial Position
Statement of Changes in Equity
Cash Flow Statement

Overview

Notes to the financial statements:

1. Financial Performance

1.1 Expenses
1.2 Own-Source Revenue and gains

2. Financial Position

2.1 Financial Assets
2.2 Non-Financial Assets
2.3 Payables
2.4 Interest Bearing Liabilities

3. Funding

3.1 Appropriations
3.2 Net Cash Appropriation Arrangements

4. People and relationships

4.1 Employee Provisions
4.2 Key Management Personnel Remuneration
4.3 Related Party Disclosures

5. Managing uncertainties

5.1 Contingent Assets and Liabilities
5.2 Financial Instruments
5.3 Fair Value Measurement


6. Other information

6.1 Current/non-current distinction for assets and liabilities

STATEMENT BY THE ACCOUNTABLE AUTHORITY AND CHIEF FINANCIAL OFFICER

In our opinion, the attached financial statements for the year ended 30 June 2023 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 Inspector-General of Intelligence and Security will be able to pay its debts as and when they fall due.

Signed.....

The Hon Christopher Jessup KC
Inspector-General of Intelligence and Security
4 August 2023

Signed.....

Ms Gerlinde Nicolson
Chief Financial Officer
4 August 2023

Statement of Comprehensive Income

for the period ended 30 June 2023

		2023	2022	Original Budget
	Notes	\$	\$	\$
NET COST OF SERVICES				
Expenses				
Employee benefits	1.1A	7,118,860	6,653,156	9,764,000
Suppliers	1.1B	2,984,748	2,596,181	2,862,000
Depreciation and amortisation	2.2A	920,252	912,141	1,585,000
Finance costs		6	60	-
Write-down and impairment of assets		34,720	2,406	-
Total expenses		11,058,586	10,163,944	14,211,000
Own-source revenue				
Revenue from contracts with customers	1.2A	33,665	27,422	-
Other revenue	1.2B	40,000	40,000	67,000
Total own-source revenue		73,665	67,422	67,000
Net (cost of)/contribution by services		(10,984,921)	(10,096,522)	(14,144,000)
Revenue from Government	1.2C	12,561,000	12,220,000	12,561,000
Surplus/(Deficit) attributable to the Australian Government		1,576,079	2,123,478	(1,583,000)
OTHER COMPREHENSIVE INCOME				
Items not subject to subsequent reclassification to net cost of services				
Changes in asset revaluation reserve	2.2A	229,135	-	-
Total comprehensive income/(loss)		1,805,214	2,123,478	(1,583,000)

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

Budget Variances Commentary

Statement of Comprehensive Income

Employee benefits

Employee expenses were \$2.65m (27%) lower than the original budget. OIGIS achieved an actual ASL of 44 for the year against a funded ASL of 57. Factors that contributed to this included external labour market shortages in key skill areas, challenges with completing security related pre-employment screening in a timely manner (including TSPV clearances) and staff separations due to the highly competitive market for skilled and cleared staff. Strategies and initiatives continue to be developed and adjusted to meet these challenges.

Depreciation and amortisation

Depreciation and amortisation expenses were \$0.66m (42%) lower than the original budget. Prior and current year capital acquisitions did not materialise to the extent of that budgeted due to lower than anticipated staffing levels. Accordingly, the depreciation and amortisation of a lower asset base has driven the variance.

Change in asset revaluation reserve and write-down and impairment of assets

Variance relates to the results of the Independent Valuation performed by CBRE of all IGIS Leasehold Improvements and Property, Plant and Equipment assets as at 30 June 2023.

Statement of Financial Position

as at 30 June 2023

	Notes	2023 \$	2022 \$	Original Budget \$
ASSETS				
Financial assets				
Cash and cash equivalents	2.1A	521,658	521,864	522,000
Trade and other receivables	2.1B	31,829,176	30,015,661	30,109,000
Total financial assets		32,350,834	30,537,524	30,631,000
Non-financial assets				
Leasehold improvements	2.2A	1,342,000	1,481,770	-
Property, plant and equipment	2.2A	929,342	1,070,623	4,222,000
Right-of-use	2.2A	-	2,488	-
Intangibles	2.2A	56,609	369,240	875,000
Prepayments		238,212	170,056	170,000
Total non-financial assets		2,566,163	3,094,177	5,267,000
Total assets		34,916,997	33,631,701	35,898,000
LIABILITIES				
Payables				
Suppliers	2.3A	300,008	494,034	798,000
Other payables	2.3B	449,525	302,611	-
Total payables		749,533	796,646	798,000
Interest bearing liabilities				
Leases	2.4A	-	2,523	-
Total interest bearing liabilities		-	2,523	-
Provisions				
Employee provisions	4.1A	1,722,283	2,384,806	2,478,000
Total provisions		1,722,283	2,384,806	2,478,000
Total liabilities		2,471,816	3,183,975	3,276,000
Net assets		32,445,181	30,447,726	32,622,000
EQUITY				
Contributed equity		10,747,189	10,554,949	14,313,000
Reserves		243,400	14,265	15,000
Retained surplus/(Accumulated deficit)		21,454,592	19,878,512	18,294,000
Total equity		32,445,181	30,447,726	32,622,000

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

Budget Variances Commentary

Statement of Financial Position

Trade and other receivables

Trade and other receivables balance is \$1.72m (6%) higher than the original budget. Unspent appropriations have materialised due to the surplus generated in 2022-23 as outlined in the Statement of Comprehensive Income budget variances commentary.

Non-financial assets

Aggregate non-financial assets recognised are \$2.70m (51%) lower than the original budget. Prior and current year capital acquisitions did not materialise to the extent of that budgeted due to lower than anticipated staffing levels.

Employee provisions

Employee provisions are \$0.76m (30%) lower than the original budget. This is reflective of the movement in the 10 year Government Bond rate and the difference in the provision for a funded ASL of 57 compared to an actual ASL of 44 at 30 June 2023.

Statement of Changes in Equity

for the period ended 30 June 2023

	Notes	2023 \$	2022 \$	Original Budget \$
CONTRIBUTED EQUITY				
Opening balance		10,554,949	10,446,301	10,555,000
Transactions with owners				
Distributions to owners				
Returns of capital		(3,565,760)	(165,352)	-
Contributions by owners				
Departmental capital budget		3,758,000	274,000	3,758,000
Closing balance as at 30 June		10,747,189	10,554,949	14,313,000
RETAINED EARNINGS				
Opening balance		19,878,513	17,755,035	19,877,000
Comprehensive income				
Surplus/(Deficit) for the period		1,576,079	2,123,478	(1,583,000)
Closing balance as at 30 June		21,454,592	19,878,513	18,294,000
ASSET REVALUATION RESERVE				
Opening balance		14,265	14,265	15,000
Comprehensive income				
Other comprehensive income		229,135	-	-
Closing balance as at 30 June		243,400	14,265	15,000
TOTAL EQUITY				
Opening balance		30,447,726	28,215,600	30,447,000
Surplus/(Deficit) for the period		1,576,079	2,123,478	(1,583,000)
Other comprehensive income		229,135	-	-
Transactions with owners		192,240	108,648	3,758,000
Closing balance as at 30 June		32,445,181	30,447,726	32,622,000

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 (DCBs) are recognised directly in contributed equity in that year.

Other Distributions to Owners

The FRR require that distributions to owners be debited to contributed equity unless it is in the nature of a dividend.

Budget Variances Commentary

Statement of Changes in Equity

Return of unspent appropriation

Unspent prior year appropriations totalling \$3,565,760 were quarantined under three year sunset clauses and returned to the Official Public Account on 1 July 2022.

Comprehensive Income and Other Comprehensive Income

Variance is reflective of the surplus generated in 2022-23 as outlined in the Statement of Comprehensive Income.

Cash Flow Statement

for the period ended 30 June 2023

	Notes	2023 \$	2022 \$	Original Budget \$
OPERATING ACTIVITIES				
Cash received				
Appropriations		11,137,875	9,283,186	12,468,000
Net GST received		133,388	103,356	100,000
Other		33,665	27,422	67,000
Total cash received		11,304,928	9,413,964	12,635,000
Cash used				
Employees		7,398,458	6,085,893	9,671,000
Suppliers		3,356,586	2,454,750	2,962,000
Interest payments on lease liabilities		6	60	-
Section 74 receipts transferred to OPA		547,561	573,013	-
Total cash used		11,302,610	9,113,716	12,633,000
Net cash from/(used by) operating activities		2,317	300,248	2,000
INVESTING ACTIVITIES				
Cash used				
Purchase of property, plant and equipment		129,668	5,376	3,758,000
Purchase of intangibles		-	29,578	-
Total cash used		129,668	34,954	3,758,000
Net cash (used by) investing activities		(129,668)	(34,954)	(3,758,000)
FINANCING ACTIVITIES				
Cash received				
Contributed equity		129,668	34,953	3,758,000
Total cash received		129,668	34,953	3,758,000
Cash used				
Principal payments of lease liabilities		2,523	6,687	2,000
Total cash used		2,523	6,687	2,000
Net cash from financing activities		127,145	28,266	3,756,000
Net increase/(decrease) in cash held		(206)	293,560	-
Cash and cash equivalents at the beginning of the reporting period		521,864	228,304	522,000
Cash and cash equivalents at the end of the reporting period	2.1A	521,658	521,864	522,000

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

Budget Variances Commentary

Cash Flow Statement

Any related budget variance commentary is included in the other Primary Statements.

Overview

The Office of the Inspector-General of Intelligence and Security (OIGIS) is an Australian Government controlled entity. It is a not-for-profit entity. OIGIS activities encompass the provision of independent assurance for the Prime Minister, senior ministers and Parliament as to whether Australia's intelligence agencies act legally and with propriety by inspecting, inquiring into and reporting on their activities.

The continued existence of OIGIS in its present form and with its present programs is dependent on Government policy and on continuing funding by Parliament for OIGIS's administration and programs.

The Basis of Preparation

The financial statements are required by section 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); and
- b) Australian Accounting Standards and Interpretations – including simplified disclosures for Tier 2 Entities under AASB 1060 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

Two amending standards (AASB 2021-2 and AASB 2021-6) were adopted earlier than the application date stated in the standard. These amending standards have been adopted for the 2022-23 reporting period.

Standard/ Interpretation	Nature of change in accounting policy, transitional provisions, and adjustment to financial statements
AASB 2021-2 <i>Amendments to Australian Accounting Standards – Disclosure of Accounting Policies and Definition of Accounting Estimates</i> (AASB 2021-2)	AASB 2021-2 amends AASB 7, AASB 101, AASB 108, AASB 134 and AASB Practice Statement 2. The amending standard requires the disclosure of material, rather than significant, accounting policies, and clarifies what is considered a change in accounting policy compared to a change in accounting estimate.
AASB 2021-6 <i>Amendments to Australian Accounting Standards – Disclosure of Accounting Policies: Tier 2 and Other Australian Accounting Standards</i> (AASB 2021-6)	AASB 2021-6 amends the Tier 2 reporting requirements set out in AASB 1049, AASB 1054 and AASB 1060 to reflect the changes made by AASB 2021-2. These amending standards are not expected to have a material impact on OIGIS's financial statements for the current reporting period or future reporting periods.

Taxation

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

Events After the Reporting Period

There was no subsequent event that had the potential to significantly affect the ongoing structure and financial activities of OIGIS.

Financial Performance

This section analyses the financial performance of OIGIS for the year ended 2023.

1.1 Expenses

	2023	2022
	\$	\$
1.1A: Employee benefits		
Wages and salaries	5,317,874	4,869,590
Superannuation		
Defined contribution plans	595,420	563,152
Defined benefit plans	367,828	339,182
Leave and other entitlements	723,261	881,232
Separation and redundancies	114,477	-
Total employee benefits	7,118,860	6,653,156

Accounting Policy

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

	2023	2022
	\$	\$
1.1B: Suppliers		
Goods and services supplied or rendered		
Audit Fees	35,000	35,000
Consultants	383,783	345,480
Contractors	472,215	332,843
ICT and communication	576,539	675,456
Insurance	19,069	17,632
Legal	56,889	15,329
Property	634,433	667,596
Recruitment and HR	89,001	124,978
Security vetting	92,255	160,491
Training	301,690	108,339
Travel	225,085	20,979
Other	87,646	77,178
Total goods and services supplied or rendered	2,973,605	2,581,301
Other suppliers		
Workers compensation expenses	11,143	14,880
Total other suppliers	11,143	14,880
Total suppliers	2,984,748	2,596,181

1.2 Own-Source Revenue and gains

	2023	2022
	\$	\$

Own-Source Revenue

1.2A: Revenue from contracts with customers

Rendering of services	33,665	27,422
Total revenue from contracts with customers	33,665	27,422

Accounting Policy

Revenue from contracts with customers is recognised when control has been transferred to the buyer. OIGIS determines a contract is in scope of AASB 15 when the performance obligations are required by an enforceable contract and the performance obligations within the enforceable contract are sufficiently specific to enable OIGIS to determine when they have been satisfied. OIGIS determines there to be an enforceable contract when the agreement creates enforceable rights and obligations. Performance obligations are sufficiently specific where the promises within the contract are specific to the nature, type, value and quantity of the services to be provided and the period over which the services must be transferred.

The following is a description of the principal activities from which OIGIS generates its revenue: OIGIS provides staff with access to onsite car parking facilities. Agreements are in place for the recovery of expenses on a fortnightly basis. With performance obligations having been met during fortnightly pay cycles, the revenue is recognised when received. The transaction price is based on a fixed amount per fortnight.

The transaction price is the total amount of consideration to which OIGIS expects to be entitled in exchange for transferring promised services to a customer. The consideration promised in a contract with a customer may include fixed amounts, variable amounts, or both.

	2023	2022
	\$	\$

1.2B: Other revenue

Resources received free of charge

Remuneration of auditors	35,000	35,000
Australian Signals Directorate	5,000	5,000
Total other revenue	40,000	40,000

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.

The Australian Signals Directorate provides support to OIGIS in the management of specific ICT capabilities for which they have unique experience and qualifications. This relationship is managed separate to, and has no impact on, OIGIS' oversight activities and arrangements of the Australian Signals Directorate.

	2023	2022
	\$	\$

1.2C: Revenue from Government

Appropriations

Departmental appropriations	12,561,000	12,220,000
Total revenue from Government	12,561,000	12,220,000

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 OIGIS 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 OIGIS assets used to conduct its operations and the operating liabilities incurred as a result.

2.1 Financial Assets

	2023	2022
	\$	\$
2.1A: Cash and cash equivalents		
Cash on hand or on deposit	521,658	521,864
Total cash and cash equivalents	521,658	521,864

Accounting Policy

Cash is recognised at its nominal amount. Cash and cash equivalents includes:

- a) cash on hand; and
- b) demand deposits in bank accounts with an original maturity of 3 months or less that are readily convertible to known amounts of cash and subject to insignificant risk of changes in value.

	2023	2022
	\$	\$
2.1B: Trade and other receivables		
Appropriation receivables		
Appropriation receivable	31,770,229	29,736,971
Total appropriation receivables	31,770,229	29,736,971
Other receivables		
GST receivable from the Australian Taxation Office	36,773	20,504
Inter-agency staff leave transfers	22,174	258,186
Total other receivables	58,947	278,690
Total trade and other receivables	31,829,176	30,015,661

Credit terms for goods and services were within 30 days (2022: 30 days).

Accounting Policy

Financial assets

Trade receivables and other receivables that are held for the purpose of collecting the contractual cash flows where the cash flows are solely payments of principal and interest, that are not provided at below-market interest rates, are subsequently measured at amortised cost using the effective interest method adjusted for any loss allowance.

Impairment

OIGIS recognises a loss allowance at an amount equal to lifetime expected credit losses. As OIGIS receivables relate to outstanding debts with other Commonwealth entities, no impairment has been recognised for 2023 (2022: Nil).

2.2 Non-Financial Assets

2.2A: Reconciliation of the Opening and Closing Balances of Property, Plant and Equipment and Intangibles

	Leasehold improvements	Property, plant and equipment	Right-of-use	Intangibles	Total
	\$	\$	\$	\$	\$
As at 1 July 2022					
Gross book value	1,852,212	1,292,978	21,837	937,893	4,104,920
Accumulated depreciation, amortisation and impairment	(370,443)	(222,355)	(19,349)	(568,653)	(1,180,800)
Total as at 1 July 2022	1,481,769	1,070,623	2,488	369,240	2,924,120
Additions					
Purchase or internally developed	-	129,668	-	-	129,668
Revaluations and impairments recognised in:					
Other comprehensive income	229,135	-	-	-	229,135
Net cost of services	-	(34,720)	-	-	(34,720)
Depreciation and amortisation	(368,904)	(236,229)	-	(312,631)	(917,764)
Depreciation on right-of-use assets	-	-	(2,488)	-	(2,488)
Total as at 30 June 2023	1,342,000	929,342	-	56,609	2,327,951
Total as at 30 June 2023 represented by					
Gross book value	1,342,000	929,342	21,837	937,893	3,231,072
Accumulated depreciation, amortisation and impairment	-	-	(21,837)	(881,284)	(903,121)
Total as at 30 June 2023	1,342,000	929,342	-	56,609	2,327,951

None of the above listed assets are expected to be sold or disposed of within the next 12 months.

Revaluations of non-financial assets

All revaluations were conducted in accordance with the revaluation policy stated at Note 2.2 Non-Financial Assets Accounting Policy. A comprehensive valuation was conducted at 30 June 2023 by an independent valuer, CBRE.

Contractual commitments for the acquisition of property, plant, equipment and intangible assets

As at the reporting date, OIGIS had no significant contractual commitments for the acquisition of property, plant, equipment and intangible assets.

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 leasehold improvements and property, plant and equipment are recognised initially at cost in the statement of financial position, except for purchases costing less than \$2,000, 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).

Lease Right of Use (ROU) Assets

Lease ROU assets are capitalised at the commencement date of the lease and comprise of the initial lease liability amount, initial direct costs incurred when entering into the lease less any lease incentives received. These assets are accounted for by Commonwealth lessees as separate asset classes to corresponding assets owned outright.

Revaluations

Following initial recognition at cost, property, plant and equipment and leasehold improvements (excluding ROU assets) are carried at fair value (or an amount not materially different from fair value) less subsequent accumulated depreciation and accumulated impairment losses. 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 is eliminated against the gross carrying amount of the asset and the asset restated to the revalued amount.

All revaluations are independent and are conducted in accordance with the stated revaluation policy. An asset valuation was conducted at 30 June 2023 and included all leasehold improvements and property, plant and equipment assets. The valuation was performed by an independent valuer, CBRE.

Depreciation

Depreciable property, plant and equipment assets are written-off to their estimated residual values over their estimated useful lives to OIGIS 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:

	2023	2022
Leasehold improvements	5 years	5 years
Plant and equipment	1 - 25 years	1 - 25 years

The depreciation rates for ROU assets are based on the commencement date to the earlier of the end of the useful life of the ROU asset or the end of the lease term.

Impairment

All assets were assessed for impairment at 30 June 2023. 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 OIGIS were deprived of the asset, its value in use is taken to be its depreciated replacement cost.

Derecognition

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

Intangibles

OIGIS intangibles comprise internally developed software 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 OIGIS software is 3 years (2022: 3 years).

All software assets were assessed for indications of impairment as at 30 June 2023.

2.3 Payables

	2023	2022
	\$	\$

2.3A: Suppliers

Trade creditors and accruals	300,008	494,034
Total suppliers	300,008	494,034

Average days of settlement are 20 days (2022: 20 days).

	2023	2022
	\$	\$

2.3B: Other payables

Salaries and wages	244,258	202,050
Superannuation	38,549	23,530
Leave Balance transfers	143,106	48,148
Other	23,612	28,883
Total other payables	449,525	302,611

The liability for superannuation recognised as at 30 June represents outstanding contributions.

2.4 Interest Bearing Liabilities

	2023 \$	2022 \$
2.4A: Leases		
Lease liabilities	-	2,523
Total leases	-	2,523
Maturity analysis - contractual undiscounted cash flows		
Within 1 year	-	2,523
Total leases	-	2,523

Total cash outflow for leases for the year ended 30 June 2023 was \$2,529 (2022: \$6,746)

OIGIS had one motor vehicle lease which reached the end of its lease term in 2022-23.

The above lease disclosures should be read in conjunction with the accompanying note 2.2A.

Accounting Policy

For all new contracts entered into, OIGIS considers whether the contract is, or contains, a lease. A lease is defined as 'a contract, or part of a contract, that conveys the right to use an asset (the underlying asset) for a period of time in exchange for consideration'.

Once it has been determined that a contract is, or contains, a lease the lease liability is initially measured at the present value of the lease payments unpaid at the commencement date, discounted using the interest rate implicit in the lease, if that rate is readily determinable, or OIGIS's incremental borrowing rate.

Subsequent to initial measurement, the liability will be reduced for payments made and increased for interest. It is remeasured to reflect any reassessment or modification to the lease. When the lease liability is remeasured, the corresponding adjustment is reflected in the right-of-use asset or profit and loss depending on the nature of the reassessment or modification.

Funding

This section identifies OIGIS funding structure.

3.1 Appropriations

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

Annual Appropriations for 2023

	Annual Appropriation ¹ \$	Adjustments to appropriation ² \$	Total appropriation \$	Appropriation applied in 2023 (current and prior years) \$	Variance ³ \$
Departmental					
Ordinary annual services	12,592,000	547,561	13,139,561	(11,138,080)	2,001,480
Capital Budget ⁴	3,758,000	-	3,758,000	(129,668)	3,628,332
Total departmental	16,350,000	547,561	16,897,561	(11,267,748)	5,629,812

1. As at 30 June 2023, \$31,000 of Departmental ordinary annual services appropriation was withheld from this amount under section 51 of the PGPA Act.

2. Adjustments to appropriations includes adjustments to current year annual appropriations including PGPA Act section 74 receipts.

3. Variances between Total Appropriation and Appropriation Applied relate to underspends in Employee benefits and associated expenditure. OIGIS achieved an actual ASL of 44 for the year against a funded ASL of 57. Factors that contributed to this included external labour market shortages in key skill areas, challenges with completing security related pre-employment screening in a timely manner (including TSPV clearances) and staff separations due to the highly competitive market for skilled and cleared staff. Strategies and initiatives continue to be developed and adjusted to meet these challenges. Additionally, capital acquisitions did not materialise to the extent of that budgeted due to a range of factors including lower than anticipated staffing levels.

4. Departmental Capital Budgets are appropriated through Appropriation Acts (No.1,3,5). They form part of ordinary annual services, and are not separately identified in the Appropriation Acts. The current year departmental capital budget as per the Portfolio Budget Statements and Portfolio Additional Estimates Statements was \$3,758,000.

Annual Appropriations for 2022

	Annual Appropriation \$	Adjustments to appropriation ¹ \$	Total appropriation \$	Appropriation applied in 2022 \$	Variance ² \$
Departmental					
Ordinary annual services	12,220,000	573,013	12,793,013	(8,989,626)	3,803,387
Capital Budget ³	274,000	-	274,000	(34,953)	239,047
Total departmental	12,494,000	573,013	13,067,013	(9,024,579)	4,042,434

1. Adjustments to appropriations includes adjustments to prior year annual appropriations including PGPA Act section 74 receipts.

2. Variances between Total Appropriation and Appropriation Applied relate to underspends in Employee benefits and associated expenditure. These have materialised due to recruitment delays associated with security clearance requirements and the impact of the COVID-19 pandemic on planned activities (which also include Capital Expenditure).

3. Departmental Capital Budgets are appropriated through Appropriation Acts (No.1,3,5). They form part of ordinary annual services, and are not separately identified in the Appropriation Acts. The prior year departmental capital budget as per the Portfolio Budget Statements and Portfolio Additional Estimates Statements was \$274,000.

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

	2023	2022
	\$	\$
Departmental		
Appropriation Act (No. 1) 2019-20 - Supply Act ¹	-	1,117,713
Appropriation Act (No. 1) 2019-20 - DCB ¹	-	1,413,047
Appropriation Act (No. 1) 2019-20 - DCB - Supply Act ¹	-	1,035,000
Appropriation Act (No. 1) 2020-21	-	5,100,446
Appropriation Act (No. 1) 2020-21 - Supply Act ²	974,330	7,011,759
Appropriation Act (No. 1) 2020-21 - DCB ²	287,332	417,000
Appropriation Act (No. 1) 2020-21 - DCB - Supply Act ²	584,000	584,000
Appropriation Act (No. 1) 2021-22	12,784,006	12,784,006
Appropriation Act (No. 1) 2021-22 - DCB	274,000	274,000
Appropriation Act (No. 3) 2022-23 - Supply Act ³	7,345,000	-
Appropriation Act (No. 1) 2022-23 - Supply Act	5,794,561	-
Appropriation Act (No. 3) 2022-23 - DCB - Supply Act	2,192,000	-
Appropriation Act (No. 1) 2022-23 - DCB - Supply Act	1,566,000	-
Cash and cash equivalents	521,658	521,864
Total departmental	32,322,887	30,258,835

1. Appropriation lapsed on 1 July 2022.

2. Appropriation will lapse on 1 July 2023.

3. As at 30 June 2023, \$31,000 of Departmental ordinary annual services appropriation was withheld from this amount under section 51 of the PGPA Act.

3.2 Net Cash Appropriation Arrangements

	2023 \$	2022 \$
Total comprehensive income - as per the Statement of Comprehensive Income	1,805,214	2,123,478
<i>Plus</i> : depreciation/amortisation of assets funded through appropriations (departmental capital budget funding and/or equity injections) ¹	917,764	905,507
<i>Plus</i> : depreciation of right-of-use assets ²	2,488	6,634
<i>Less</i> : lease principal repayments ²	(2,523)	(6,687)
Net Cash Operating Surplus	2,722,943	3,028,932

1. From 2010-11, the Government introduced net cash appropriation arrangements where revenue appropriations for depreciation/amortisation expenses of non-corporate Commonwealth entities and selected corporate Commonwealth entities were replaced with a separate capital budget provided through equity appropriations. Capital budgets are to be appropriated in the period when cash payment for capital expenditure is required.

2. The inclusion of depreciation/amortisation expenses related to ROU leased assets and the lease liability principal repayment amount reflects the impact of AASB 16 *Leases*, which does not directly reflect a change in appropriation arrangements.

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

	2023	2022
	\$	\$
4.1A: Employee provisions		
Leave	1,722,283	2,384,806
Total employee provisions	1,722,283	2,384,806

Accounting policy

Liabilities for short-term employee benefits and termination benefits expected within twelve 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 OIGIS'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 model provided by the Department of Finance as at 30 June 2023. The estimate of the present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

Superannuation

OIGIS staff are members of the Commonwealth Superannuation Scheme (CSS), the Public Sector Superannuation Scheme (PSS), 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 the Department of Finance's administered schedules and notes.

OIGIS 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. OIGIS accounts for the contributions as if they were contributions to defined contribution plans.

4.2 Key Management Personnel Remuneration

Key management personnel are those persons having authority and responsibility for planning, directing and controlling the activities of OIGIS, directly or indirectly. OIGIS has determined the key management personnel to be the Inspector-General, Deputy Inspector-General, both Assistant Inspectors-General and the Executive Director, Enterprise Management Unit. Key management personnel remuneration is reported in the table below:

	2023	2022
	\$	\$
Short-term employee benefits	1,522,518	1,342,832
Post-employment benefits	193,666	171,200
Other long-term employee benefits	21,924	19,583
Total key management personnel remuneration expenses¹	1,738,108	1,533,615

The total number of key management personnel that are included in the above table are 6 (2022: 8). Substantively, 5 key management personnel positions remain in place during 2023, however there were a number of acting arrangements in place over the course of the year.

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:

OIGIS is an Australian Government controlled entity. Related parties to OIGIS are Key Management Personnel, including the Portfolio Minister 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. These transactions have not been separately disclosed in this note.

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 OIGIS, it has been determined that there are no related party transactions to be separately disclosed (2022: Nil).

Managing uncertainties

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

5.1: Contingent assets and liabilities

Quantifiable Contingencies

As at 30 June 2023 there were no contingent assets or liabilities (2022: nil).

Unquantifiable Contingencies

As at 30 June 2023 there were no unquantifiable contingent assets or liabilities (2022: nil).

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

	2023	2022
	\$	\$
5.2A: Categories of financial instruments		
Financial assets at amortised cost		
Cash and cash equivalents	521,658	521,864
Total financial assets at amortised cost	521,658	521,864
Total financial assets	521,658	521,864
Financial Liabilities		
Financial liabilities measured at amortised cost		
Suppliers	300,008	494,034
Total financial liabilities measured at amortised cost	300,008	494,034
Total financial liabilities	300,008	494,034

Accounting Policy

Financial assets

In accordance with AASB 9 *Financial Instruments*, OIGIS classifies its financial assets in the following categories:

- financial assets at fair value through profit or loss;
- financial assets at fair value through other comprehensive income; and
- financial assets measured at amortised cost.

The classification depends on both OIGIS's business model for managing the financial assets and contractual cash flow characteristics at the time of initial recognition. Financial assets are recognised when OIGIS 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.

Financial Assets at Amortised Cost

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

- the financial asset is held in order to collect the contractual cash flows; and
- 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.

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 Amortised Cost

Financial liabilities 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

5.3A: Fair value measurement

	Fair value measurements at the end of the reporting period	
	2023 \$	2022 \$
Non-financial assets		
Leasehold improvements	1,342,000	1,481,770
Property, plant and equipment	929,342	1,070,623
Total Non-financial assets	2,271,342	2,552,393

Accounting Policy

The methods utilised to determine fair value are as follows:

- Market Approach (Level 2) - In instances where there were sufficient observable transactions of similar assets to the subject asset (generally in second-hand markets), the market approach has been utilised to determine fair value. These types of assets include, but are not limited to, general IT equipment, certain servers and switches, furniture, storage equipment and general office equipment. Market evidence has primarily been sourced from national online auction markets and dealer enquiries. These inputs to the fair value measurements are considered Level 2 in the fair value hierarchy as they have been observed from the market and the Valuer utilised minimal professional judgement to adjust for differences in asset characteristics.

- Cost Approach (Level 3) - In instances where insufficient or no observable transactions of similar assets to the subject asset have been identified, the Cost approach has been utilised to determine fair value. These types of assets include the fitout. Current replacement costs have been sourced from suppliers and manufactures. Regard has been given to OIGIS's operational requirements as well as improvements in asset design, materials and technology in determining the modern equivalent asset.

Physical obsolescence has been determined using an age/life analysis which considered the asset's consumed service potential to total service potential as at the valuation date. In forming opinions of physical depreciation and obsolescence, the valuer considered a combination of inquiries made with relevant OIGIS staff, discussions with external suppliers / manufactures and professional experience with such assets.

OIGIS engaged the services of an independent valuer, CBRE to conduct a review of carrying amounts for leasehold improvements and property, plant and equipment assets as at 30 June 2023. Comprehensive valuations are carried out at least once every 3 years. An annual assessment is undertaken to determine whether the carrying amount of the assets is materially different from the fair value.

OIGIS's policy is to recognise transfers into and transfers out of fair value hierarchy levels at the end of the reporting period.

Other information

6.1 Current/non-current distinction for assets and liabilities

6.1A: Current/non-current distinction for assets and liabilities

	2023	2022
	\$	\$
Assets expected to be recovered in:		
No more than 12 months		
Cash and cash equivalents	521,658	521,864
Trade and other receivables	31,829,176	30,015,661
Prepayments	238,212	169,187
Total no more than 12 months	32,589,046	30,706,712
More than 12 months		
Leasehold improvements	1,342,000	1,481,770
Property, plant and equipment	929,342	1,070,623
Right-of-use	-	2,488
Intangibles	56,609	369,240
Prepayments	-	868
Total more than 12 months	2,327,951	2,924,989
Total assets	34,916,997	33,631,701
Liabilities expected to be settled in:		
No more than 12 months		
Suppliers	300,008	494,034
Other payables	449,525	302,611
Leases	-	2,523
Employee provisions	758,751	1,242,151
Total no more than 12 months	1,508,284	2,041,320
More than 12 months		
Employee provisions	963,532	1,142,655
Total more than 12 months	963,532	1,142,655
Total liabilities	2,471,816	3,183,975

Appendix A: Entity resource statements and resource for outcomes

Figure 5.1: Entity Resource Statement and Resource for Outcomes 2022–23

	Actual available appropriation for 2022–23 \$'000 (a)	Payments made 2022–23 \$'000 (b)	Balance remaining 2022–23 \$'000 (a) – (b)
Departmental			
Annual appropriations – prior year departmental	26,693	11,268	15,425
Annual appropriations – ordinary annual services	16,350	–	16,350
Annual appropriations – s 74 relevant agency receipts	548	–	548
Annual appropriations – other services – non-operating	–	–	–
Total departmental annual appropriations	43,591	11,268	32,323
Departmental special appropriations	–	–	–
Total special appropriations	–	–	–
Special accounts	–	–	–
Total special accounts	–	–	–
<i>Less departmental appropriations drawn from annual/special appropriations and credited to special accounts</i>	–	–	–
Total departmental resourcing (A)	43,591	11,268	32,323
Administered			
Total administered annual appropriations	–	–	–
Total administered special appropriations	–	–	–
Total special accounts receipts	–	–	–
<i>Less administered appropriations drawn from annual/special appropriations and credited to special accounts</i>	–	–	–
<i>Less payments to corporate entities from annual/special appropriations</i>	–	–	–
Total administered resourcing (B)	–	–	–
Total resourcing and payments for agency (A + B)	43,591	11,268	32,323

Figure 5.2: Expenses and resources for Outcome 1

The Office of the IGIS has one outcome and one program as disclosed below.

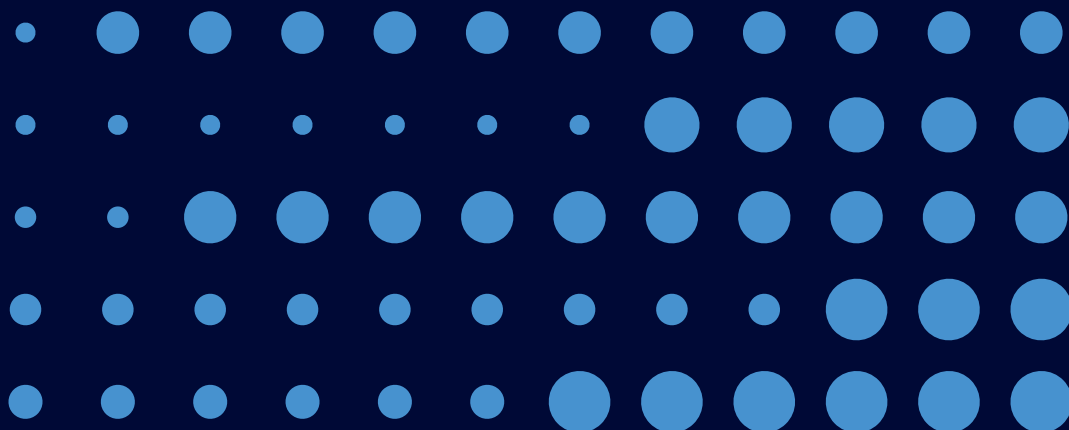
Outcome 1: Independent assurance for the Prime Minister, ministers and parliament as to whether Australia's intelligence and security agencies act legally and with propriety by inspecting, inquiring into and reporting on their activities.	Budget	Actual	Variation
	2022-23	2022-23	2022-23
	\$'000	\$'000	\$'000
	(a)	(b)	(a) – (b)
Program 1.1: Office of the Inspector-General of Intelligence and Security			
Departmental expenses			
Departmental appropriation ¹	12,559	10,098	2,461
Special appropriations	–	–	–
Special accounts	–	–	–
Expenses not requiring appropriation in the Budget year ²	1,625	960	665
Total expenses for Program 1.1	14,184	11,058	3,126
Outcome 1 totals by appropriation type			
Departmental expenses			
Departmental appropriation ¹	12,559	10,098	2,461
Special appropriations	–	–	–
Special accounts	–	–	–
Expenses not requiring appropriation in the Budget year ²	1,625	960	665
Total expenses for Outcome 1	14,184	11,058	3,126
	Budget	Actual	Variation
	2022-23	2022-23	2022-23
Average Staffing Level (number)	57	44	13

1. Full-year budget, including any subsequent adjustment made to the 2022-23 budget at Additional Estimates and estimated expenses incurred in relation to receipts retained under s 74 of the PGPA Act.

2. Expenses not requiring appropriation in the Budget year are made up of depreciation expense, amortisation expenses and resources received free of charge.

Section Six

Review of intelligence agencies



The intelligence agencies

Office of National Intelligence

Key statistics



6

Inspections
commenced



6

Inspections
completed



2

Ministerial letters
sent to relevant
minister



2

Senior-level
meetings held

Agency overview

ONI is responsible for enterprise-level management of the National Intelligence Community (NIC) and ensures a single point of accountability for the NIC to the Prime Minister and National Security Committee of Cabinet. ONI produces all-source assessments on international political, strategic and economic developments for the Australian Government. ONI uses information collected by other intelligence and government agencies, diplomatic reporting and open sources, including the media, to support its analysis.

Relevant Act: *Office of National Intelligence Act 2018* (ONI Act)

Responsible Minister: Prime Minister

Australian Security Intelligence Organisation

Key statistics



25

Inspections
commenced



28

Inspections
completed



46

Compliance
incidents reported



2

Inquiries
commenced



2

Ministerial letters
sent to relevant
minister



3

Senior-level
meetings held

Agency overview

ASIO's primary function is to protect Australia, its people and its interests from threats to security.

ASIO's functions include collecting and communicating security intelligence, providing advice to ministers and Commonwealth agencies on security matters and protective security, furnishing security assessments, and collecting and communicating foreign intelligence. In addition to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), ASIO is also bound by Minister's Guidelines that: set out principles that govern ASIO's work; provide guidance on when information obtained during an investigation is relevant to security and when ASIO can communicate certain other information; set out requirements for the collection and handling of personal information; and incorporate the current definition of politically motivated violence. Although the Minister for Home Affairs is the minister responsible for ASIO, the Attorney-General exercises certain powers and functions under the ASIO Act, including the power to authorise warrants and special intelligence operations (SIOs).

Relevant Act: *Australian Security Intelligence Organisation Act 1979*

Responsible Minister: Minister for Home Affairs

Australian Secret Intelligence Service

Key statistics



16

Inspections
commenced



18

Inspections
completed



10

Compliance
incidents
reported



2

Ministerial
letters sent
to relevant
minister



3

Senior-level
meetings held

Agency overview

The primary function of ASIS is to obtain and communicate intelligence not readily available by other means, about the capabilities, intentions and activities of individuals or organisations outside Australia. Further functions include communicating secret intelligence in accordance with government requirements, conducting counter-intelligence activities and liaising with foreign intelligence or security services. Under legislation, ASIS's activities are regulated by a series of ministerial directions, ministerial authorisations and Privacy Rules.

Relevant Act: *Intelligence Services Act 2001*

Responsible Minister: Minister for Foreign Affairs

Australian Signals Directorate

Key statistics



15

Inspections
commenced



16

Inspections
completed



11

Compliance
incidents
reported



1

Inquiry
commenced



1

Inquiry
completed



1

Preliminary
inquiry
commenced



1

Preliminary
inquiry
completed



2

Ministerial
letters sent
to relevant
minister



3

Senior-level
meetings held

Agency overview

ASD, which encompasses the Australian Cyber Security Centre (ACSC), is focused on the provision of foreign signals intelligence, cyber security and offensive cyber operations in support of the Australian Government and Australian Defence Force (ADF). The foreign intelligence ASD obtains is communicated to key policy makers and select government agencies. ASD, through the ACSC, leads the Australian Government's efforts on national cyber security. ASD's activities are regulated by a series of ministerial directions, ministerial authorisations and Privacy Rules.

Relevant Act: *Intelligence Services Act 2001*

Responsible Minister: Minister for Defence

Australian Geospatial-Intelligence Organisation

Key statistics



17

Inspections
commenced



17

Inspections
completed



2

Ministerial letters
sent to relevant
minister



2

Senior-level
meetings held

Agency overview

AGO is Australia's national geospatial intelligence agency, and is located within the Department of Defence. AGO's geospatial intelligence, derived from the fusion of analysis of imagery and geospatial data, supports Australian Government decision-making and assists with the planning and conduct of ADF operations. AGO also gives direct assistance to Commonwealth and state bodies responding to security threats and natural disasters. AGO's activities are regulated by a series of ministerial directions, ministerial authorisations and Privacy Rules.

Relevant Act: *Intelligence Services Act 2001*

Responsible Minister: Minister for Defence

Defence Intelligence Organisation

Key statistics



4

Inspections
commenced



4

Inspections
completed



2

Ministerial letters
sent to relevant
minister



2

Senior-level
meetings held

Agency overview

DIO is the Department of Defence's all-source intelligence assessment agency. Its role is to provide independent intelligence assessments, advice and services in support of: the planning and conduct of ADF operations; Defence strategic policy and wider government planning and decision-making on defence and national security issues; and the development and sustainment of Defence capability. The functions of DIO are set out in its Mandate issued by the Secretary of Defence and the Chief of Defence Force.

Relevant Act: *Intelligence Services Act 2001*

Responsible Minister: Minister for Defence

Cross-agency activities

Key statistics



1

Preliminary inquiry commenced



1

Preliminary inquiry completed



1

Inquiry commenced



1

Inquiry completed

Overview

In 2022–23, there was one inquiry and one preliminary inquiry that reviewed the activities of multiple agencies. Inspections relating to multiple agencies were also conducted; however, the statistics are reported against each agency independently.

Agency oversight activities 2022–23

Overview

The Office continues to identify a generally strong culture of compliance within the agencies. Where inspections identify any concerns, they are generally not systemic in nature. The level of cooperation from agencies that the Office receives is generally very good.

During the reporting year, among other issues, the Office has continued its focus on record keeping within the agencies, and where necessary, made recommendations that were designed to promote the significance of record keeping in a culture of compliance. Good record keeping is important for a number of reasons, but particularly for effective oversight as it provides evidence of decisions made, and by who, when and why. Good record keeping also enhances accountability and transparency within an agency, and better enables this Office to confirm what has been done and to understand the reasons for why particular action was taken, or not taken. The Office will continue this focus in the next reporting year.

Office of National Intelligence

In 2022–23, the Office has undertaken inspections of ONI's activities. The Office did not commence any inquiries under s 8 of the IGIS Act in relation to ONI.

The number of inspection activities the Office has conducted in relation to ONI reflects the Office's risk-based approach to agency oversight activities, and the fact that ONI's activities present a lower risk – particularly to the privacy of Australians – compared to the activities of other agencies.

Two biannual meetings were held between the Inspector-General, the Office's senior leadership team and ONI senior executives in November 2022 and May 2023. These meetings were a valuable opportunity to discuss organisational priorities as well as constraints and challenges.

Access to systems, personnel and information

In 2022–23, ONI provided the Office with appropriate facilities and systems access to enable our oversight activities. The Office has experienced some delays in access to information and personnel to finalise inspections in a timely manner due to limited resource availability in the relevant ONI work area.

Inspections

The Office undertook 6 inspections of ONI activities in 2022–23. Of these, 2 inspections remain under way and will be reported in the 2023–24 Annual Report. In addition, the Office completed 2 inspections commenced in 2021–22.

Of the 6 inspections completed, 3 did not identify any legality or propriety concerns. These 3 inspections covered:

- ONI's use of Australian Transaction Reports and Analysis Centre (AUSTRAC) data
- analytic integrity¹
- ONI's enterprise mission management function within the NIC.²

Of the remaining 3 inspections, a high level description of the findings and recommendations are outlined in the summaries below.

Ministerial submissions and advice

The Office reviewed ONI's submissions to the Prime Minister across all areas of its activities, as well as briefing material prepared by ONI for meetings of Cabinet.

The inspection identified that the ONI *Rules to Protect the Privacy of Australians* were not being considered for the possible communication about Australian persons by the Director-General in Cabinet meetings. ONI undertook to ensure that the Rules were applied in support of future meetings. No other concerns were identified during the inspection.

¹ ONI must conduct intelligence assessments in accordance with s 7(1)(c) and (d) of the ONI Act.

² This inspection examined ONI's conduct of its NIC coordination function under s 8 of the ONI Act.

Open source intelligence

ONI's open source intelligence functions are articulated in s 7(1)(g) of the ONI Act. The Office reviewed a sample of open source intelligence products and related documents over the inspection period, with a focus on record keeping, governance, and collection of open source intelligence on Australian persons.

The inspection found no instances of non-compliance with legislation. The Office identified one instance of non-compliance with policy on record keeping requirements. The Office provided recommendations to improve record keeping on open source intelligence-related activities and to ensure all areas in ONI are fully aware of their record keeping responsibilities.

Assumed identities

The Office reviewed the management practices enabling ONI's use of assumed identities under s 15K of the *Crimes Act 1914* (Crimes Act) and s 7(1)(g) of the ONI Act. This was the Office's first inspection of this nature for ONI.

The inspection identified no instances of non-compliance with legislation; however, the Office identified propriety issues stemming from inconsistencies between guidance documents and ONI's current practices in the use of assumed identities. The Office noted that for the majority of the inspection period, ONI's primary governance material for management of assumed identities contained references to undeveloped supporting documentation. Despite this issue, the Office found that ONI staff managed use of assumed identities appropriately. ONI developed updated policy guidance towards the end of the inspection period.

Compliance incidents

ONI did not report any compliance incidents to the Office in 2022–23.

Other reviews

In 2022–23, ONI provided the Office with copies of its updated *Rules to Protect the Privacy of Australians*. ONI also provided the Office with draft policies providing guidance on implementing the updated rules and on information use. Under s 53(4) of the ONI Act, the Inspector-General of Intelligence and Security, Attorney-General, Director-General of National Intelligence, and the Privacy Commissioner must be consulted on changes to the *Rules to Protect the Privacy of Australians*. The Prime Minister wrote to the Inspector-General seeking consultation on changes to the rules. The Office reviewed these changes and related policies, and provided comments back to ONI, which were considered and incorporated where appropriate. The new *Rules to Protect the Privacy of Australians* were endorsed by the Prime Minister on 29 September 2022 and adopted on 1 October 2022.

Australian Security Intelligence Organisation

In 2022–23, the Office has undertaken both inquiries and inspections of ASIO's activities and reviewed compliance incidents reported by ASIO.

Inquiries were undertaken into specific issues or matters identified through the Office's other oversight activities. In 2022–23, 2 inquiries in relation to ASIO were commenced under s 8 of the IGIS Act, including one initiated by a complaint made to the Office.

The Office implemented a risk-based approach to its inspections of ASIO, given the breadth of ASIO's functions under s 17 of the ASIO Act.

The Office continued to independently review all compliance incident reports relating to non-compliance with legislation or the Minister's Guidelines, or non-compliance with ASIO's internal policies and procedures.

Meetings between the Inspector-General, Director-General of Security, the Office's senior leadership team and ASIO senior executives took place during the reporting period to discuss oversight issues. Separately, the Office sought briefings from ASIO on specific matters to support its oversight activities, and ASIO provided additional briefings on matters it considered appropriate to bring to the Office's attention.

Access to systems, personnel and information

In 2022–23, ASIO provided the Office with appropriate direct access to ASIO systems and facilities to support its oversight work. Overall, for individual inspections and inquiries ASIO provided access to appropriate personnel and information in a timely manner to enable the Office's oversight activities.

Inquiries

Of the 2 inquiries undertaken by the Office in relation to ASIO in the reporting period, one is reported in this report's Complaints and PIDs section (page 123–127) and one is detailed below.

On 8 June 2023, the Inspector-General commenced an inquiry into past authorisations made by the Director-General of Security authorising the communication of information to ASD staff under s 18 of the ASIO Act and s 65(1) of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). The inquiry remained underway at the end of the reporting period. A report will be prepared at the conclusion of the inquiry and the inquiry findings will be finalised in 2023–24.

Inspections

The Office undertook 25 inspections of ASIO activities in 2022–23.

Of those 25 inspections, the Office did not identify any legality or propriety concerns in 15 inspections into the following matters:

- temporary exclusion orders
- COVID app data
- visa and citizenship complaints (2 inspections)
- investigative cases
- ASIO interviews
- human source management (3 inspections)
- PIDs
- compliance remediation
- International Production Orders
- internal security
- security assessments
- special intelligence operations (SIOs).

In some instances the Office made recommendations directed to improving the clarity of, and compliance with, ASIO's internal policies and procedures, or to promote stronger record keeping in relation to decision-making.

Out of the 25 inspections undertaken, 5 inspections that commenced in 2022–23 remained ongoing at the end of the financial year. This includes inspections relating to: foreign intelligence collection operations; assumed identities; ASIO's use of powers under the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*; liaison and exchange of information with foreign authorities; and reporting and record keeping under warrants. The Office's findings will be reported in 2023–24.

In addition to the 20 inspections commenced and completed in 2022–23, the Office completed another 8 inspections that had commenced in 2021–22 and were completed in 2022–23.

Of the 28 inspections completed in the current reporting period, the Office identified matters relating to legality or propriety in 12 inspections. A high level description of the findings and recommendations are outlined in the following summaries.

Non-warranted surveillance operations

In 2022–23, the Office conducted an inspection of ASIO's use of non-warranted surveillance devices, with a particular focus on a specific type of optical surveillance. The Office identified serious concerns with around 20 percent of these optical surveillance operations, which had continued despite not appearing to be linked to an active ASIO investigation. The Office considered ASIO had not complied with the requirements of the Minister's Guidelines in some of these cases and that ASIO's actions in some cases may have been outside its functions under s 17 of the ASIO Act. The Office assessed the underlying cause of the identified issues to be systemic deficiencies in ASIO's internal processes and policy guidance that had resulted, over a period of years, in inconsistent practices and unclear lines of responsibility and accountability.

The Office made several recommendations as a result of this inspection. In response to the Office's findings and recommendations, the Director-General of Security wrote to the Inspector-General to outline the remediation action that ASIO had already taken or would take. The Office considers this remediation to be appropriate and will monitor ASIO's implementation in future inspections.

Technical collection and retention

Each year, the Office conducts an inspection to provide assurance that data in ASIO's technical systems has been collected lawfully, and that data that is inconsistent with a warrant or otherwise collected unlawfully has been deleted. The scope of this inspection includes data identified for deletion following a compliance incident reported to the Office as well as a sample identified by the Office during inspection activities. The Office has observed improvements in ASIO's data governance and data deletion processes in recent inspections.

The inspection conducted in the current reporting period identified continued concerns with ASIO's investigation, remediation and reporting of a particular compliance incident reported to the Office that required data deletion to be undertaken. In response to the Office's findings, the Director-General of Security advised the Inspector-General that ASIO would implement several remediation measures. Subsequently, the Director-General provided the Inspector-General with advice on the progress of ASIO's remediation. The Office considered this remediation to be appropriate and will assess the effectiveness of changes to ASIO's processes in future inspections.

Analytic integrity

This inspection reviewed a sample of ASIO's published and unpublished analytic products and identified no concerns with ASIO's analytic independence. However, the inspection identified concerns relating to the clarity of language used in some products, particularly where ASIO was seeking a decision based on that language. The concerns identified are similar to the concerns reported in the Office's 2021–22 Annual Report. The Office reiterated its view of the importance of clear and consistent language to enable informed decision-making. The inspection also found multiple instances of non-compliance with one of ASIO's internal procedures related to ensuring analytic rigour through referencing in ASIO products. The Office will continue to revisit these issues in future inspections.

Human source management

The Office conducts regular inspections of ASIO's human source management. Although the majority of inspections of this matter during 2022–23 identified no legality or propriety issues, one inspection identified concerns about potentially systemic non-compliance with ASIO's internal procedures within one area responsible for human source management. The Office made recommendations directed to improving ASIO's records relating to oversight and accountability for these cases.

In 2021–22, the Office commenced 2 inspections focussed on a particular type of human source operation. The inspections, which were reported in a single set of findings, identified that the impact of COVID-19 disruptions was evident in the management of the reviewed cases. The Office identified significant variability in the quality and timeliness of records and line management oversight. The Office noted that at the time of the inspections, the relevant area in ASIO had been restructured and had commenced reviewing and updating its internal procedures, the inspection outcomes contributed to that activity. The Office will revisit the issues identified in the findings during 2023–24.

Special intelligence operations

The Office reviews SIOs both on an individual basis and as part of periodic inspections. In the 2021–22 reporting period, the Office commenced an inspection into ASIO's SIOs. The Office identified several areas of concern relating to the management of legal risk, the completeness of information provided to the Attorney-General, and record keeping relating to management of a particular SIO.

In one of the inspections of SIOs conducted during the 2022–23 reporting period, the Office concluded that although ASIO had addressed the individual issues identified in previous inspections, this remediation may not have addressed underlying systemic issues associated with the management of SIOs. The Office recommended that ASIO review its compliance management framework relating to the use of SIO powers.

ASIO's interaction with minors

In 2021–22, the Office commenced a wide-ranging inspection of ASIO's investigative and operational activities, where the subject of the activity was a minor. The inspection found that ASIO's policy and procedural guidance in respect of investigative and operational interactions with minors was disjointed, which resulted in inconsistency of approach and giving rise to a higher chance of legality or propriety risks occurring. The Office made several recommendations, including that ASIO develop overarching policy guidance and take steps to improve its consideration and recording of relevant matters. ASIO implemented the Office's recommendations during the reporting period.

Use of a particular technical capability

The focus of this inspection – commenced in 2021–22 – was a particular non-warranted technical capability used by ASIO. The inspection identified inconsistencies in ASIO's approach to these operations relating to: approvals and authorisations; application of the relevant standing operating procedure; and record keeping. The Office will conduct a follow-up inspection in 2024–25.

Warrants

In 2021–22, the Office reviewed warrant reports to the Attorney-General that contained reporting of warrant-related non-compliance. The Office identified concerns relating to one warrant about the completeness and accuracy of information provided to the Attorney-General. More generally, the Office noted variability in the type and amount of information being provided to the Attorney-General across the warrant reports. The Office noted that ASIO had commenced reviewing its internal guidance to improve clarity and consistency in its reporting. These matters were considered in a similar inspection during the reporting period. This inspection remains ongoing and will be reported in next year's annual report.

Device access orders under s 34AAD of the ASIO Act and ASIO's use of industry assistance requests under the *Telecommunications Act 1997*

The scope of this inspection, commenced in 2021–22, included ASIO's use of device access orders under s 34AAD of the ASIO Act as well as industry assistance requests issued under Part 15 of the *Telecommunications Act 1997* (Telecommunications Act). In relation to device access orders, the Office identified concerns relating to notification and reporting to the Attorney-General, and identified an inconsistency in ASIO policies relating to the inclusion of certain information in a device access order. The Office recommended that ASIO provide additional information to the Attorney-General for completeness and clarity, and suggested improvements to ASIO's policies. In addition, the Office identified that some industry assistance requests did not comply with the policies required under s 3.6 of the Minister's Guidelines. The Office suggested that ASIO undertake further work to ensure that internal policies are reflected in relevant templates and understood by operational areas.

Other reviews required under legislation

In addition to its regular inspection program, the Office reviews ASIO's use of certain powers under the ASIO Act following notification to the Inspector-General.

Special intelligence operations

SIO powers allow ASIO to seek authorisation from the Attorney-General to undertake activities, in support of its functions, that would otherwise be unlawful. The ASIO Act requires ASIO to notify the Inspector-General as soon as practicable after an authority is given. During the reporting period, in all instances the Inspector-General was notified within 24 hours of the Attorney-General granting approval for a SIO.

The ASIO Act also requires ASIO to provide the Attorney-General and the Inspector-General a written report on each SIO. The Office reviewed each authorisation and report immediately following notification to the Inspector-General. Separately, the Office conducted periodic inspections to examine the activities undertaken under SIOs in greater detail. The Office's findings are reported above.

Compulsory questioning

ASIO's compulsory questioning powers, including provisions relating to the Office's oversight of the questioning or apprehension of a person, are contained in Part III Division 3 of the ASIO Act. The Office was not notified of any use of ASIO's compulsory questioning powers and therefore the Inspector-General did not attend any questioning sessions during 2022–23.

Use of force

Warrants issued under the ASIO Act must explicitly authorise the use of force necessary and reasonable to undertake the actions specified in the warrant. Under s 31A of the ASIO Act, when force is used against a person in the execution of a warrant, ASIO must notify the Inspector-General in writing and as soon as practicable. ASIO notified the Office of one instance of use of force in 2022–23. On further investigation, ASIO determined that the reported incident did not constitute use of force. The Office reviewed ASIO's determination and agreed with ASIO's conclusion.

Compliance incidents

The Office independently reviews all compliance incidents that ASIO reports. In doing so, the Office may seek additional information or undertake further review. The Office's review includes consideration of ASIO's remediation action, which frequently entails amendments to ASIO's internal policies and procedures to provide greater clarity for ASIO officers. As an additional assurance measure, the Office conducts periodic inspections to confirm that implementation of proposed remediation action has occurred and to review the effectiveness of this action.

Matters that do not meet ASIO's threshold for reporting to the Office are included in ASIO's periodic compliance reports, and a copy of this report is provided to the Inspector-General. ASIO also reports certain matters to the Office on propriety grounds. As with other compliance incidents, the Office reviews these matters and may seek additional information or undertake further investigation.

In 2022–23, ASIO reported 46 compliance incidents to the Office. This included notification of several incidents (some of which were outside ASIO's control) that upon further assessment by ASIO were determined to be compliant and the Office agreed with that determination. Although the number of incidents reported by ASIO increased from the 2021–22 reporting period, the Office considers this reflects a continual maturing of ASIO's compliance framework, rather than a systemic increase in non-compliance.

ASIO notified the Office of 3 additional matters on either propriety grounds or in accordance with the requirements of a memorandum of understanding between ASIO and AUSTRAC regarding access to, and the use of, AUSTRAC information.

ASIO also provided notification of 9 incidents outside ASIO's control arising from the actions of another Australian intelligence agency as it exercised the authority conferred by warrants under the TIA Act managed by ASIO.

The Office reviewed matters of legislative non-compliance and propriety reported by ASIO. These incidents and the Office's findings, where the matter has been finalised in the reporting period, are outlined below. Thirteen incidents remained under assessment by ASIO at the end of 2022–23 and will be reported in 2023–24.

Telecommunications (Interception and Access) Act 1979

Non-compliance with s 63 of the TIA Act and s 4.1 of the Minister's Guidelines – communication to ASD: Section 63 of the TIA Act prohibits lawfully or unlawfully intercepted information from being used, recorded or communicated to another person, except in certain circumstances. Section 4.1 of the Minister's Guidelines requires that ASIO only collect, use, handle, retain or disclose personal information for purposes related to its functions or powers, or where otherwise authorised or required by law. ASIO notified the Office of 2 separate incidents that occurred when ASIO's technical system for receiving data under a warrant was misconfigured, leading to lawfully

intercepted information being inadvertently shared with a partner agency. The Office agreed with ASIO's assessment that it was non-compliant with s 63 of the TIA Act and s 4.1 of the Minister's Guidelines, and verified that the relevant data had been deleted. The Office also received a briefing on the technical issue that caused the incident and changes ASIO had implemented to reduce the risk of future incidents.

Non-compliance with s 7 and s 63 of the TIA Act – interception and communication: Section 7 of the TIA Act prohibits interception of communications passing over a telecommunications system except in certain circumstances, including where a warrant is in place. ASIO notified the Office of 2 instances of non-compliance with s 7 and s 63 of the TIA Act.

In the first instance, ASIO identified that, due to a technical issue, a carrier was providing data in excess of the terms of a warrant. Upon identifying the issue, ASIO immediately requested the carrier to cease interception and commenced data deletion. ASIO subsequently confirmed that the technical issue that caused the incident had been remedied by the carrier. While noting that this incident arose as a result of events outside ASIO's control, the Office agreed with ASIO's assessment it was non-compliant with s 7 and s 63 of the TIA Act. The Office will verify data deletion as part of its regular inspection program.

In the second instance, non-compliance occurred when an error in one of ASIO's technical systems resulted in the cross contamination of data obtained under 2 different warrants. The issue arose when a carrier did not action a request from ASIO to cease interception of a particular service, resulting in data continuing to be sent to ASIO. A previously undetected error in ASIO's systems caused this data to be combined with data being received under a different warrant and made available to end users within ASIO. On identifying the issue, ASIO immediately reissued its request to cease interception, instructed the relevant area not to access the data, took steps to identify and fix the technical error, and commenced data deletion. The Office received a briefing from ASIO on the technical issue and the action taken to address it. ASIO assessed that it was non-compliant with s 7 and s 63 of the TIA Act. The Office is satisfied with ASIO's assessment and remediation of this issue, and will verify data deletion as part of its regular inspection program.

Potential non-compliance with s 7 of the TIA Act – errors in warrant documentation: ASIO notified the Office of 2 instances of potential non-compliance with s 7 of the TIA Act relating to the same warrant. There were 2 errors in the warrant documentation. The first was inclusion of a service on the warrant that remained subscribed but was no longer being used by the intelligence target. The second was a typographical error in an email address. ASIO assessed that the first instance did not result in non-compliance with s 7 of the TIA Act. The Office agreed with this assessment. In the second instance, ASIO assessed that although no data was collected, it was potentially non-compliant with s 7(1)(b) of the TIA Act. The Office agreed with this assessment. The Office will verify ASIO's remediation as part of its regular inspection program.

ASIO notified the Office of another incident relating to a different warrant, where the warrant also contained a typographical error in an email address. ASIO similarly assessed that it was potentially non-compliant with s 7(1)(b) of the TIA Act. The Office agreed with this assessment and will verify ASIO's remediation as part of its regular inspection program.

Non-compliance with s 9A(2)(b) of the TIA Act – errors in warrant documentation: Section 9A(2)(b) of the TIA Act requires a warrant request by the Director-General of Security to include the details of known telecommunications services used, or likely to be used, by the target. ASIO notified the Office of an incident where a warrant request did not include a phone service that was included in the warrant instrument. Separately, the warrant request and instrument included a service that had been removed from an earlier warrant because it was no longer being used by

the target. ASIO concluded that the first matter was compliant but that the second matter was non-compliant with s 9A(2)(b) of the TIA Act. ASIO requested that the Attorney-General revoke the existing warrant and issue a new warrant in its place. The Office agreed with ASIO's assessment and will verify ASIO's remediation as part of its regular inspection program.

Potential non-compliance with s 13 of the TIA Act – warrant revocation: ASIO notified the Office of an incident relating to warrant revocation under the TIA Act. Section 13 of the TIA Act requires that where the Director-General is satisfied that the grounds on which a warrant was issued have ceased to exist, the Director-General will forthwith inform the Attorney-General and take steps to discontinue the interception of communications. In this incident, ASIO failed to send a disconnection notice to a carrier and continued to intercept communications after the Attorney-General had been notified of an intention to revoke the warrant. ASIO sought legal advice and concluded that it was compliant with s 13 of the TIA Act because the Director-General was not personally aware that the grounds on which the warrant was issued had ceased to exist. However, the matter was non-compliant with ASIO's internal policy and data deletion was initiated. ASIO subsequently implemented new warrant revocation processes, requiring areas to notify the Director-General when they believe the grounds for a warrant may have ceased. The Office was satisfied with ASIO's assessment and considers the revised warrant revocation processes to be appropriate. The Office will verify ASIO's data deletion and remediation as part of its regular inspection program.

Propriety matter – collection on an Australian permanent resident: ASIO notified the Office of an incident relating to a person who obtained Australian permanent residency during the life of a TIA Act warrant that was limited to the services of non-Australian persons. ASIO had received information that the person had obtained permanent residency but did not review or act on that information until a week after it was received. ASIO concluded that there was no non-compliance with legislation or the Minister's Guidelines, because the requirements of s 11D(5) of the TIA Act were met at the time the warrant was issued and the legislation does not require ASIO to remove the services of persons who become Australian citizens during the life of the warrant. However, ASIO considered it appropriate to report the incident as a propriety matter, as ASIO had intended to remove the person's services from the warrant when they obtained permanent residency but did not do so in a timely manner. The Office agreed with this assessment and will verify data deletion as part of its regular inspection program.

Non-compliance with s 175 of the TIA Act – telecommunications data: Section 175 of the TIA Act empowers certain ASIO personnel to authorise the disclosure to ASIO of historical telecommunications data by telecommunications carriers or carriage service providers in connection with the performance of ASIO's functions. ASIO notified the Office of 3 instances of non-compliance with s 175 of the TIA Act relating to requests for telecommunications data. In the first instance, the submitted requests included invalid end dates. There was no collection of data outside the correct dates, meaning data deletion was not required. In the second and third instances, typographical errors resulted in requests being made for phone numbers that did not exist. The Office agreed with ASIO's assessment that it was non-compliant with s 175 of the TIA Act because the eligible person had no reasonable basis to be satisfied that the disclosures were in connection with the performance of ASIO's functions.

Non-compliance with s 13 of the TIA Act and s 30 of the ASIO Act – warrant revocations: ASIO identified that under the new warrant revocation processes noted above, warrant revocation notices sent to the Attorney-General between September and December 2022 potentially did not meet legislative requirements under s 13 of the TIA Act or s 30 of the ASIO Act. The notices did not expressly inform the Attorney-General that the Director-General was satisfied that the grounds

on which the warrants had been issued had ceased to exist. ASIO corrected the deficiency in its template on identifying this issue. ASIO sought legal advice and concluded that it was non-compliant with s 13 of the TIA Act and s 30 of the ASIO Act. The Office is satisfied with ASIO's assessment and remediation action.

Australian Security Intelligence Organisation Act 1979

Potential non-compliance with s 30 of the ASIO Act – warrant revocation: Similarly to s 13 of the TIA Act, s 30 of the ASIO Act requires the Director-General to ensure that ASIO discontinues action under a warrant and informs the Attorney-General as soon as practicable if the Director-General is satisfied that the grounds on which the warrant was issued have ceased to exist. ASIO notified the Office of an incident in which ASIO initiated a process to change the description of the target computer; however, this process was not completed due to insufficient case handover between ASIO officers. ASIO identified the error when preparing documentation for a new warrant. ASIO sought legal advice and concluded that no non-compliance occurred. The Office agreed with ASIO's assessment.

Non-compliance with s 94(2A)(c) of the ASIO Act – annual report: Section 94(2A)(c) of the ASIO Act requires ASIO's Annual Report to include the number of data authorisations pertaining to s 176(3) of the TIA Act. Between 2015 and 2021, ASIO's annual reports included the total number of data authorisations made under s 176 of the TIA Act, but not the required sub-set of this figure. As a consequence, ASIO also did not comply with the requirement at s 94(2A)(d) that it report on the purposes for which authorisations made under s 176(3) were given. The omission was identified during preparation of ASIO's 2021-22 Annual Report, which includes the correct statistics for the 2019-20 to 2021-22 financial years. The Office was satisfied with ASIO's assessment and remediation of this issue.

Minister's Guidelines to ASIO

Non-compliance with s 3.7 of the Minister's Guidelines – personal information: The Minister's Guidelines are issued under s 8A of the ASIO Act and are required to be observed by ASIO in the performance of its functions. Section 3.7 of the Minister's Guidelines requires ASIO to take all reasonable steps to ensure that personal information used or disclosed by ASIO is relevant, accurate and not misleading. ASIO notified the Office of 9 instances of non-compliance with s 3.7 during 2022-23.

The first incident related to a security assessment. ASIO reported that human error in interpreting results returned from a database search resulted in ASIO conducting checks on an incorrect individual and identifying that individual in a security assessment. ASIO concluded it was non-compliant with s 3.7 of the Minister's Guidelines. The Office agreed with this assessment and noted that the error did not materially affect the security assessment because the individual was not the subject of the assessment. The Office was satisfied with the steps ASIO committed to take to remove the incorrect information from its systems. The Office will verify deletion of the relevant data through its regular inspection program.

The second incident occurred when an error led to ASIO sending a request to ASD that omitted the dates when a target – who was subject to a Ministerial Authorisation – had ceased using 2 services. ASIO concluded that it was non-compliant with s 3.7 of the Minister's Guidelines. The Office agreed with this assessment and will verify ASIO's data deletion and remediation through its regular inspection program.

ASIO notified the Office of 5 incidents related to authorisations under s 175 of the TIA Act where errors made by ASIO analysts resulted in incorrect data being sought. The Office agreed with

ASIO that these matters were non-compliant with s 3.7 of the Minister's Guidelines. The Office will verify ASIO's remediation through its regular inspection program.

ASIO notified the Office of a further incident where an error in information provided by another agency and an incorrect assumption by ASIO led to a person being included on a warrant when they should not have been. Once identified, the warrant was revoked. No interception had occurred, meaning data deletion was not required. ASIO assessed it was non-compliant with s 3.7 of the Minister's Guidelines. The Office agreed with ASIO's assessment and remediation.

The ninth incident concerned a request made under s 176 of the TIA Act for prospective telecommunications data for a person who was not of security interest. The incident arose due to an error made when interpreting subscriber checks and insufficient review. When identified, ASIO ceased data collection, cancelled the request and initiated data deletion. ASIO assessed it was non-compliant s 3.7 of the Minister's Guidelines. The Office agreed with ASIO's assessment and will review ASIO's remediation through its regular inspection program.

Non-compliance with s 3.4 of the Minister's Guidelines – intrusion into privacy: Section 3.4 of the Minister's Guidelines requires ASIO's collection of information to be proportionate and undertaken with as little intrusion into an individual's privacy as reasonably required. ASIO notified the Office of an incident where a phone service that was subscribed to but known not to be used by a target, was included in a warrant. When identified, ASIO ceased collection, revoked the warrant and requested data deletion. ASIO concluded that it was non-compliant with s 3.4(b)(i) of the Minister's Guidelines. The Office was satisfied with ASIO's assessment and will review ASIO's remediation as part of its regular inspection program.

ASIO notified the Office of another instance of non-compliance with s 3.4 of the Minister's Guidelines, in which 2 errors – including errors on the part of the telecommunications provider – relating to subscriber checks resulted in the communications of a non-security relevant individual being intercepted. On identifying the error, ASIO initiated data deletion and updated its processes to reduce the chance of similar errors occurring in future. The Office was satisfied with ASIO's assessment and will review ASIO's remediation as part of its regular inspection program.

Non-compliance with s 2.5 of the Minister's Guidelines – annual review: Section 2.5 of the Minister's Guidelines requires ASIO to review each of its ongoing investigations on an annual basis. ASIO notified the Office of one instance of non-compliance with s 2.5, where a review was completed outside the 12 month period. The Office was satisfied with ASIO's assessment and remediation action.

Criminal Code Act 1995 (Criminal Code)

Potential non-compliance with Part 10.7 of the Criminal Code – computer offences: Part 10.7 of the Criminal Code contains a range of computer offences. ASIO notified the Office of an incident where a request made in relation to a computer access warrant was actioned before the relevant device identifier was added to the warrant. On identifying the error, ASIO deleted the information obtained. ASIO concluded that while the action was defective, no non-compliance had occurred. The Office agreed with this assessment.

Crimes Act 1914

Non-compliance with the Crimes Act – assumed identities: Part IAC of the Crimes Act enables ASIO officers to create and use assumed identities for the purpose of performing ASIO's functions. ASIO notified the Office of 3 incidents relating to applications by ASIO contractors for an assumed identity. In the first incident, ASIO did not obtain the Director-General's endorsement that it would be impossible or impracticable in the circumstances for an ASIO employee to acquire or use the assumed identity for the purpose sought, as required under s 15KB(2)(c) of the Crimes Act. This incident prompted a review by the relevant area, which identified 2 similar historical incidents. ASIO concluded all 3 instances were non-compliant with s 15KB(2)(c) of the Crimes Act and ASIO's internal policy and procedure. The Office agreed with ASIO's assessment and proposed remediation.

ASIO notified the Office of an incident where a request made to the Australian Taxation Office appeared to be non-compliant with the requirements of s 15KI(4)(c) of the Crimes Act. Section 15KI(4)(c) provides that requests for evidence of an assumed identity must include details of any evidence of the assumed identity that may be acquired under the authority. ASIO sought legal advice. ASIO concluded that there was no non-compliance with s 15KI(4)(c). The Office was satisfied with ASIO's assessment and remediation action.

ASIO notified the Office of an incident where, due to errors made at the time an assumed identity was transferred between ASIO officers, the assumed identity was used without authority. ASIO concluded it was non-compliant with s 15KP of the Crimes Act and ASIO's internal policy and procedure. The Office agreed with ASIO's assessment and remediation action.

Other matters

Authorisations by the Director-General of Security: ASIO notified the Office of a matter on propriety grounds relating to authorisations made by the Director-General of Security in 2018 that authorised ASIO employees to request and receive personal information from state and territory agencies. The authorisations had not been updated to reflect organisational changes within ASIO. When the issue was identified, the Director-General signed updated authorisations and ASIO commenced work on a revised approach to its management of delegated legislation. ASIO concluded that there were potential legal vulnerabilities attached to the out-of-date authorisations and issued new authorisations. It determined that it would not undertake a legal review given these new authorisations. The Office agreed with ASIO's assessment, but notes that without a concluded legal review it would be appropriate to consider the matter to be potential non-compliance.

Finalisation of 2021–22 compliance incidents

Several compliance incidents that had been reported during 2021–22 were also finalised during the reporting year.

The following incidents were found to involve legislative non-compliance or propriety issues. Two additional incidents relating to potential non-compliance with the ASIO Act were determined on further investigation to be compliant.

Non-compliance with s 175 of the TIA Act or s 3.7 of the Minister's Guidelines –

telecommunications data: ASIO notified the Office of 12 incidents relating to the collection of telecommunications data that it considered to be actual or potential non-compliance with s 175 of the TIA Act or non-compliance with s 3.7 of the Minister's Guidelines. During 2022–23, ASIO and the Office reached a common understanding on the requirements of s 175 and the circumstances in which non-compliance would be considered to have occurred. ASIO assessed, and the Office

agreed, that it was non-compliant with s 175 in relation to 7 incidents and non-compliant with s 3.7 of the Minister's Guidelines in relation to 5 incidents. The Office was satisfied with ASIO's proposed remediation, which it will review during 2023-24.

Non-compliance with s 24 of the ASIO Act – authorisation of officers to exercise authority

under warrant: Section 24 of the ASIO Act sets out who may exercise the authority of a warrant obtained under Division 2 or Division 3 of the ASIO Act. ASIO notified the Office of an incident where ASIO officers were involved in executing a search warrant without a valid authorisation under s 24 being in place. ASIO concluded, on the basis of external legal advice, that this activity was likely non-compliant with s 24(1) of the ASIO Act. Relatedly, ASIO's report to the Attorney-General on this warrant (required by s 24 of the ASIO Act), including details of the incident, was not provided within 3 months as required by ASIO internal policy. The Office agreed with ASIO's assessment and proposed updates to its internal policies and procedures to address both issues.

Potential non-compliance with relevant state legislation – authorisation for continued use of listening device:

ASIO notified the Office of a potential non-compliance with the ASIO Act where collection under a listening device continued for 5 days after the relevant surveillance device authorisation had expired. ASIO immediately ceased collection and requested that data collected during this period be deleted. ASIO obtained legal advice and concluded that there was no non-compliance with the ASIO Act or relevant state legislation. Nonetheless, ASIO undertook to introduce policy and procedural changes, as well as system changes, to reduce the chance of reoccurrence. The Office agreed with ASIO's assessment, noting that while no legislative non-compliance had occurred, the incident was clearly a matter of propriety. The Office was satisfied that ASIO addressed the matter appropriately.

Non-compliance with the Telecommunications Act – notification of technical access request:

ASIO notified the Office that it had failed to provide notification to the Inspector-General within the required timeframe of the issue of a technical access request, as required by s 317HAB(1) of the Telecommunications Act. ASIO concluded it was non-compliant with s 317HAB(1). The Office agreed with ASIO's assessment and proposed updates to its internal policies and procedures.

Propriety matter – inadvertent sharing of data files with a partner agency: ASIO notified the Office of a matter relating to the inadvertent sharing of 3 data files containing personal information of ASIO staff with a partner agency during an authorised transfer of other data files. The receiving agency identified and deleted the files before they were ingested into relevant systems and then advised ASIO. ASIO concluded that the matter did not amount to the commission of an offence or non-compliance with relevant legislation. ASIO also considered that there was no clear non-compliance with the Minister's Guidelines. ASIO and the Office had differing views on whether s 4.1 and 4.2 of the Minister's Guidelines were relevant to the incident. The Office considered the incident could constitute non-compliance with the Minister's Guidelines; however, it was satisfied with ASIO's proposed remediation.

Non-compliance with the Crimes Act – assumed identities: ASIO notified the Office of an incident involving 2 instances where approvals were provided in circumstances in which the approving officer did not have the authorisation to do so. Both cases related to circumstances where ASIO's IT system for managing assumed identities had not been updated following staffing changes. ASIO concluded that the first instance was non-compliant with s 15KE of the Crimes Act and that the second instance was non-compliant with s 15KF(5) of the Crimes Act. The Office agreed with this assessment and considered ASIO's remediation to be appropriate.

Australian Secret Intelligence Service

In 2022–23, the Office has undertaken inspections of ASIS's activities and reviewed compliance incidents reported by ASIS. The Office did not commence any inquiries under s 8 of the IGIS Act in relation to ASIS.

The Office implemented a risk-based approach to its inspections of ASIS, given the breadth of ASIS's functions under s 8 of the *Intelligence Services Act 2001* (IS Act).

The Office continued to independently review all compliance incident reports from ASIS.

Three triannual meetings were held between the Inspector-General, the Office's senior leadership team and ASIS senior executives in July 2022, December 2022 and March 2023. These meetings were a valuable opportunity to discuss organisational priorities as well as constraints and challenges. The Inspector-General and the Office's senior leadership team also met with the newly appointed Director-General of ASIS shortly after she commenced in the role in February 2023.

Access to systems, personnel and information

In 2022–23, ASIS provided the Office with facility access and some direct access to ASIS systems to enable oversight work. The Office experienced some delays in accessing relevant ASIS records, which hampered the Office's ability to finalise inspections in a timely manner. ASIS and the Office worked collaboratively to identify solutions to improve direct system and information access, and ASIS has a project underway to implement those improvements in early 2023–24.

Inspections

The Office undertook 16 inspections of ASIS activities in 2022–23. Thirteen were completed and 3 remain in progress at the end of 2022–23. The outcomes of the 3 inspections underway will be reported in 2023–24. In addition, the Office completed 5 inspections that commenced in 2021–22.³

Of the 18 inspections completed in the reporting period, the Office did not identify any legality or propriety concerns in the following 10 inspections:

- ministerial submissions (6 inspections)
- operational files related to priority thematic areas (2 inspections)
- cooperation with ASIO under s 13B of the IS Act
- management of assumed identities.

In the remaining 8 of the 18 inspections completed, a high level description of the findings and recommendations are outlined in the following summaries.

³ The 2021–22 IGIS Annual Report stated that 4 inspections that commenced in the 2021–22 reporting period were carried over to the 2022–23 reporting period. This difference is due to a change in the way inspection commencement dates are calculated.

Use of assumed identities

The Office undertook 2 inspections of ASIS's use and management of assumed identities under the Crimes Act. The first inspection identified several propriety concerns with ASIS's management of its assumed identities regime, particularly related to the interpretation and implementation of relevant sections of the Crimes Act. The Office identified 7 instances of non-compliance with policy and made 10 recommendations for ASIS to improve its assumed identities regime.

The Office conducted a second inspection on ASIS's use and management of assumed identities, to review ASIS's implementation of the first inspection's recommendations. As ASIS was still in the process of implementing the recommendations from the first inspection, the Office finalised this second inspection without any findings. An inspection into ASIS's implementation of recommendations from the first inspection on use and management of assumed identities is scheduled for 2023-24.

Cooperation with ASIO under s 13B of the *Intelligence Services Act 2001*

The Office completed 2 inspections of arrangements in place for ASIS to undertake activities to support ASIO in the performance of its functions, as outlined in s 13B(1) of the IS Act. One inspection did not identify any instances of non-compliance with legislation or policy.

In the follow-up inspection, the Office found 2 instances of non-compliance with human rights procedures related to ASIS's engagement with foreign liaison partners during a series of overseas deployments. The Office found that these 2 incidents were procedural in nature and did not adversely affect any individual's human rights. The Office provided 4 recommendations aimed at strengthening ASIS's compliance with, and application of, ASIS's *Rules to Protect the Privacy of Australians*.

Human rights procedures

The Office conducted an inspection of ASIS procedures to manage the risk to human rights when undertaking cooperation with foreign authorities under s 13(1)(c) of the IS Act. This inspection used a sample of 10 foreign partners to check that ASIS had proper human rights risk management procedures in place for each foreign partner.

The Office noted the improvement in ASIS's compliance with its human rights procedures since a prior inspection, but recommended further improvements should be implemented to the existing procedures. Additionally, the Office identified one instance of non-compliance with ASIS's existing human rights procedures when ASIS engaged with a liaison partner without an extant assessment of the human rights risks. The Office did not consider that this instance of non-compliance adversely affected any individual's human rights.

Operational files related to priority thematic areas

The Office completed 3 inspections regarding operational functions undertaken in relation to priority thematic areas, including 2 inspections that commenced in the 2021-22 reporting period and were concluded in July 2022. The Office identified legality and propriety issues in one of the 3 inspections.

Specifically, the Office identified 6 instances of non-compliance with ASIS Privacy Rule 6.1 and one instance of non-compliance with ASIS's human rights procedures in an operational file inspection of a nominated section at ASIS headquarters. All non-compliance was related to incorrect approvals for sharing sensitive intelligence information with a foreign partner. ASIS submitted a compliance report related to the instance of non-compliance with ASIS human rights procedures.

Operational files related to ASIS activities overseas

The Office undertook inspections of ASIS's operational files at 2 overseas locations over specified time periods. The Office did not identify any instances of non-compliance with legislation or policy in either inspection; however, both inspections identified issues of propriety relating to record keeping and human rights risk management procedures.

One inspection provided 3 recommendations designed to strengthen ASIS's record keeping practices to ensure evidence of compliance with the law and ASIS policies can be better demonstrated.

The second inspection identified weaknesses in ASIS's compliance with human rights risk management procedures in a particular location and provided recommendations to strengthen ASIS's approach.

Ministerial directions under s 6(1)(e) of the *Intelligence Services Act 2001*

The Office reviewed arrangements in place for ASIS to undertake activities under the Foreign Minister's direction related to the capabilities, intentions or activities of people or organisations outside Australia under s 6(1)(e) of the IS Act. The inspection was reported in 2 parts.

The first report was provided to the Foreign Minister and the Director-General of ASIS and addressed the legality of the current arrangements in place for the Foreign Minister to direct such activities. The Office found that, in a number of important respects, the protocol developed by ASIS for operational activities under the Minister's direction amounted to an impermissible attempt to delegate the function entrusted to the Minister.

The second report was provided to ASIS only and addressed the legality and propriety of the specific activities undertaken under these directions during the inspection period. The Office did not identify any non-compliance with the implementation of the extant directions, but provided recommendations intended to strengthen propriety considerations and practices.

Use of weapons

The Office reviewed ASIS's management of weapons and associated qualifications, with a focus on Schedule 2 of the IS Act. Schedule 2 provides the legislative framework for ASIS officers to use weapons in certain circumstances.

In this inspection, the Office did not identify any non-compliance with legislative requirements, but did identify propriety concerns. Specifically, the Office identified one instance of unclear information being provided to the Foreign Minister regarding the weapons qualifications of an ASIS officer being posted overseas.

Compliance incidents

In 2022–23, ASIS provided 10 compliance reports to the Office. Some reports covered multiple compliance incidents related to a particular theme or target. The Office reviewed each reported incident and, where appropriate, provided ASIS with recommendations for remediation and actions to minimise recurrence. Of the 10 reports, 2 remain under investigation, 2 were closely linked to inspections and are dealt with in the inspections section above (refer to sections entitled 'Use of assumed identities' and 'Operational files related to priority thematic areas'), and 2 had no findings of non-compliance.

Themes, findings and recommendations for the remaining 4 reports are detailed on the following page.

Non-application of the Privacy Rules

The Office found that in 7 instances, ASIS did not apply the *Rules to Protect the Privacy of Australians* before communicating information concerning Australian persons. These communications were in contravention of s 15 of the IS Act. The Office recommended ASIS improve mandatory training to ensure all ASIS staff understand their obligations under the *Rules to Protect the Privacy of Australians*.

Non-recording of the Privacy Rules

The Office found that in one instance, ASIS did not properly record application of the *Rules to Protect the Privacy of Australians*, in contravention of ASIS internal policy.

Section 8 of the *Intelligence Services Act 2001*

The Office found one instance in which ASIS was non-compliant with s 8 of the IS Act, when ASIS failed to obtain written authorisation from the Foreign Minister before undertaking an activity or series of activities related to collecting intelligence on an Australian person. ASIS has undertaken to improve internal processes to address this issue. The Office is satisfied that this specific incident was a standalone incident, and the Office will continue to regularly review the compliance of ASIS's operational activities with s 8 of the IS Act for evidence of systemic weakness.

Other reviews

During 2022–23, the Acting Director-General of ASIS authorised one emergency authorisation in accordance with s 9D of the IS Act. Paragraph 9D(8)(b) of the IS Act requires the Inspector-General to provide the responsible minister with a report on the Inspector-General's views of the extent of the compliance by the agency head with the requirements of s 9D. The Inspector-General must also provide a copy of the conclusions in the report to the PJCIS.

The Inspector-General concluded that the Acting Director-General complied with the requirements of s 9D of the IS Act when exercising this power, and informed the responsible minister and the PJCIS as required.

Australian Signals Directorate

In 2022–23, the Office has undertaken both inquiries and inspections of ASD's activities, and reviewed compliance incidents reported by ASD.

Inquiries were undertaken into specific issues or matters identified through the Office's oversight activities. During the reporting period, one inquiry and one preliminary inquiry were commenced under s 8 and s 14 of the IGIS Act.

The Office implemented a risk-based approach to its inspections of ASD, given the breadth of ASD's activities under its functions under s 7 of the IS Act. In 2022–23, the Office focused on targeted inspections in areas of growth under ASD's Project REDSPICE (Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers).

The Office continued to independently review all compliance incidents reported by ASD relating to non-compliance with legislation or with ASD's internal policies and procedures.

The Inspector-General and the Office's senior leadership team met the Director-General of ASD and ASD senior executives 3 times throughout the year to discuss organisational priorities, as well as constraints and challenges.

Access to systems, personnel and information

In 2022–23, ASD provided the Office with appropriate direct access to ASD systems and facilities to support its oversight work. Overall, for individual inspections and inquiries ASD provided access to appropriate personnel and information in a timely manner to enable the Office's oversight activities.

Inquiries

Ministerial Authorisation

In the previous reporting period, in May 2022, the Inspector-General commenced a preliminary inquiry into ASD's submission for a Ministerial Authorisation and the activities approved and undertaken under that authorisation. This preliminary inquiry examined:

- whether the activities authorised were within the scope of the functions specified in the accompanying ministerial submission, the authorisation itself and other relevant material; and
- whether the submission that accompanied the application for the authorisation addressed all relevant statutory criteria.

In October 2022, the Inspector-General decided that limited further investigation, in the form of an inquiry, was required into the Ministerial Authorisation, and other relevant material. The inquiry focused on:

- the completeness of the ministerial submission that sought the authorisation and whether the Minister for Defence was properly advised of the relevant legal and operational risks associated with the authorisation; and
- the circumstances facing ASD at the time and the reasons for the urgency of the request.

The inquiry concluded in May 2023 and found the submission and accompanying attachments failed to address the statutory requirements for the authorisation which was being sought. However, ultimately ASD undertook no operational activities under the authorisation before it was

cancelled on 26 September 2022. Further, the Office also found no reason to doubt the urgency under which the authorisation was sought.

In response, ASD advised it had implemented new practices to address matters raised in this inquiry for future ministerial submissions. The Office will review the new practices in 2023–24.

Preliminary Inquiries

The Inspector-General commenced an own motion preliminary inquiry into matters raised through disclosures and complaints to the Office. This preliminary inquiry remains underway and is further detailed in the Complaints and Disclosures section of this report (page 127).

Inspections

The Office commenced 15 inspections of ASD activities in 2022–23. Of these, 14 were completed during the reporting period and one remained underway at the end of 2022–23. In addition, the Office completed 2 inspections that were commenced during 2021–22.

Of the 16 inspections completed in this reporting period, 15 identified no legality or propriety concerns. The inspections covered the following topics or activities:

- the legality and propriety of ASD's conduct under Ministerial Authorisations to undertake certain activities (4 inspections)
- the accuracy of information communicated in ministerial submissions, as well as the legality and propriety of any activities described in the submission (3 inspections)
- the application of ASD's *Rules to Protect the Privacy of Australians* made under the IS Act (4 inspections)
- targeted inspections in areas of growth under REDSPICE (2 inspections)
- targeted inspections of joint activities with other agencies (2 inspections).

In a number of inspections listed above, the Office made recommendations, predominately related to record keeping practices that were not aligned with internal ASD policies and processes. ASD has committed to updating the relevant policy guidance provided to its staff.

In the 2 targeted inspections in areas of growth under REDSPICE – namely cyber-focused activities – the Office found similar issues as identified in the inquiry into the Ministerial Authorisation (referenced above), regarding the sufficiency of ASD's submission to the Minister for Defence in support of its requests for Ministerial Authorisation. The Office notes that both REDSPICE inspections occurred shortly after the inquiry into the Ministerial Authorisation. As such, many of the recommended actions – including for ASD to review its internal policies and processes relevant to activities conducted under its cyber functions – had not yet occurred. The Office will continue to review these areas in the 2023–24 inspection program.

One inspection completed in this reporting period identified findings related to legality concerns. This inspection was focused on ASD's Ministerial Authorisations, and the Office identified a potential incident of legislative non-compliance with the TIA Act. This matter is under investigation by ASD and the Office will conduct a review of the issue when ASD completes its internal investigation.

Overturned presumptions of nationality

The Minister for Defence issues written rules to regulate ASD's communication and retention of intelligence information about Australian persons (the *ASD Rules to Protect the Privacy of Australians*). These rules require ASD to provide the Office with access to all of ASD's intelligence holdings and report to the Office any non-compliance with the rules. ASD must also report to the Office when it determines a person previously presumed to be foreign is an Australian person – known as 'overturning a presumption of nationality' (OPN). This usually occurs when ASD obtains further information on an individual. If the initial presumption was reasonable, and appropriate steps were taken to manage information related to that individual, such incidents do not represent non-compliance with legislation or the *Rules to Protect the Privacy of Australians*.

In 2022–23, the Office reviewed 45 reports in which the application of ASD's *Rules to Protect the Privacy of Australians* resulted in a presumption of nationality being overturned, including 6 reports received during a previous reporting period.

In each of the 45 OPN cases reviewed in this reporting period, the Office determined the initial presumption of nationality was reasonable, and that ASD took appropriate measures to protect the privacy of the Australian persons. The Office also noted that ASD had remediated its internal processes that contributed to the occurrence of some OPN instances, and the Office observed that ASD worked closely with partner agencies to remind them of their obligations regarding the reporting of new intelligence information relevant to ASD's decision on the application of the *Rules to Protect the Privacy of Australians*.

At the end of the reporting period, 3 individual OPN cases remained under review.

The Office also made some administrative findings regarding ASD's OPN processes, predominately related to data querying or record keeping practices that were inconsistent with internal ASD policies and guidelines. Each of these instances has been resolved by ASD, and ASD has undertaken to update the relevant policies and guidance it provides to staff on these matters. The Office will review these updates in similar activities in the next reporting period.

Compliance incidents

The Office independently reviews all potential compliance incidents reported by ASD. The Office often requires supplementary information or technical briefings from ASD while investigating incidents to ensure circumstances surrounding the incident can be fully understood and the Office can form an informed, independent view. The technical complexity of ASD's compliance incidents may also result in requests for additional legal advice by either ASD or the Inspector-General, which can substantially lengthen the overall time taken to finalise an incident.

In 2022–23, ASD provided the Office with 11 notifications of potential compliance incidents at the start of ASD's internal investigation process. ASD also continued its investigation of a further 8 potential compliance incidents from previous reporting periods. Of these 19 notifications, ASD provided the Office with 8 compliance incident reports and 11 remained under internal ASD investigation and will be reviewed by the Office upon receipt of the formal reports.

In 2022–23, the Office reviewed 12 compliance incident reports, including the 8 provided during the reporting period and 4 provided in previous reporting periods. Of these 12 reports, 3 potential incidents were determined by ASD, and agreed by the Office, to be compliant as they did not represent non-compliance with legislation or ASD's internal policies and procedures. Eight reported compliance incidents were confirmed by the Office as matters of legislative non-compliance, resulting in 10 instances of non-compliance with legislation, which are

discussed further below. At the end of the reporting period, one compliance incident was still under review, pending ASD receiving additional legal advice.

ASD has also undertaken to investigate one additional matter of non-compliance identified by the Office through regular inspection activities. The Office will review this matter in 2023–24.

Compliance incidents reviewed by the Office in 2022–23 are described below.

Telecommunications (Interception and Access) Act 1979

Non-compliance with s 63 of the TIA Act: In May 2022, ASD confirmed it was non-compliant with s 63 of the TIA Act following an incident in September 2021, in which a system update led to the incorrect labelling of data, making it available to analysts not authorised to have access. In reviewing this incident, the Office found that ASD acted promptly to manage the non-compliance, and the remedial actions taken following the incident were appropriate in the circumstances. However, the Office provided a number of recommendations to address potential propriety and governance concerns.

Non-compliance with s 7(1)(c) of the TIA Act: In June 2022, ASD confirmed it was non-compliant with s 7(1)(c) of the TIA Act following an incident in November 2021, in which it was erroneously enabled to intercept communications passing over a telecommunications system. Although ASD was authorised to intercept some of the communications from the target, due to this error, ASD could have intercepted communications it was not authorised to intercept. In this instance, no unauthorised communications were identified as being intercepted. In reviewing the incident, the Office recognised that the responsible team had taken steps to mitigate future incidents by updating internal processes. The Office suggested that this guidance be shared more broadly within ASD. The Office also noted ASD's intent to develop automated compliance and assurance mechanisms, which the Office will review in future inspections.

Non-compliance with s 63(1) of the TIA Act: In January 2022, ASD confirmed it was non-compliant with s 63(1) of the TIA Act following an incident in December 2021, in which a technical malfunction resulted in data inadvertently being made accessible to analysts not authorised to have access. In reviewing this incident, the Office found that ASD acted promptly to contain the incident and implemented appropriate controls to mitigate future occurrences of similar incidents.

Two non-compliances with s 63(1) of the TIA Act: In December 2022, ASD confirmed it was non-compliant with s 63(1) of the TIA Act in 2 separate incidents in July 2022, in which data collected by a partner agency was inadvertently forwarded to ASD and subsequently ingested into ASD systems, resulting in ASD making a record it was not permitted to make.

In the first incident, misconfiguration of a system controlled by the other agency resulted in unauthorised communications being passed to ASD. In the second incident, data lawfully collected under warrant by the other agency was mislabelled prior to being communicated to ASD. ASD has removed all impacted data from both incidents from its systems.

In reviewing these incidents, the Office determined that they resulted from circumstances outside ASD's control. The Office considered that ASD acted promptly and properly to remediate the situation and took appropriate steps within the scope of its responsibilities to reduce the risk of recurrence of similar incidents.

Four non-compliances with s 7(1)(a), s 7(1)(c) and s 63(1) of the TIA Act: In December 2022, ASD confirmed it was non-compliant with both s 7(1)(a) and s 63(1) of the TIA Act following an incident from July 2021 where ASD inadvertently enabled interception that fell outside the

scope of an existing authorisation and, in doing so, intercepted communications passing over a telecommunications system. It subsequently stored a record of these communications that it was not authorised to intercept.

In the course of investigating the incident, ASD identified a second incident in which ASD enabled unauthorised interception of communications in contravention of s 7(1)(c) of the TIA Act, but that did not result in any collection of communications. When the Office reviewed the incident, a third incident was identified where the interception of communications had been unlawfully enabled, but no communications were collected. ASD undertook to review the third matter and, in March 2023, confirmed it to be in contravention of s 7(1)(c) of the TIA Act.

The Office's review of these incidents determined that ASD had acted promptly and appropriately to resolve the matters, and that all unauthorised data had been appropriately removed from ASD systems. In addition, the review noted that ASD had proactively engaged relevant parties to remediate their standard operating procedures, and provided updated compliance guidance for ASD staff and partner agencies. The Office also noted ASD's intent to develop automated compliance and assurance mechanisms, which the Office will review in future inspections.

Non-compliance with s 7(1)(c) of the TIA Act: In December 2022, ASD confirmed it was non-compliant with s 7(1)(c) of the TIA Act during an historical incident from November 2016, which was identified in July 2022 when ASD undertook a proactive review of its records following the decision in *Alexander v Minister for Home Affairs* [2022] HCA19. In the conduct of its review, ASD identified one incident where it inadvertently enabled interception that fell outside the scope of an existing authorisation and, in doing so, enabled the interception of communications passing over a telecommunications system in contravention of s 7(1)(c) of the TIA Act. Due to ASD data retention processes, any communications that were potentially intercepted had already been removed from ASD systems at the time the incident was identified. As such, it could not be definitely determined whether ASD intercepted any communications through this activity; however, during the review of this incident the Office identified no record of any communications having been collected.

In reviewing this incident, the Office found that ASD had acted promptly and appropriately to resolve the matter once identified, and engaged relevant parties to remediate their standard operating procedures. The Office also noted ASD's intent to develop automated compliance and assurance mechanisms, which the Office will review in future inspections.

Other reviews

The Office also reviewed ASD's compliance with the requirements of s 9D of the IS Act, regarding ASD's use of an emergency authorisation in relation to circumstances which involved an imminent risk to the safety of an Australian person who was outside Australia. Paragraph 9D(8)(b) of the IS Act requires the Inspector-General to provide the responsible minister a report on the Inspector-General's views of the extent of the compliance by the agency head with the requirements of s 9D and also provide a copy of the conclusions in the report to the PJCIS.

The Inspector-General concluded that the Director-General of ASD complied with the requirements of s 9D of the IS Act when exercising this power, and informed the responsible minister and the PJCIS as required.

Australian Geospatial-Intelligence Organisation

In 2022–23, the Office has undertaken inspections of AGO's activities. The Office did not commence any inquiries under s 8 of the IGIS Act in relation to AGO.

The Office implemented a risk-based approach to its inspections of AGO, given the breadth of AGO's activities under its functions under s 6B of the IS Act. In 2022–23, the Office undertook proactive deep-dive inspections into areas of higher risk or sensitivity.

The Inspector-General and the Office's senior leadership team met with the Director of AGO and AGO senior executives twice in the reporting period. These meetings were a valuable opportunity for both sides to discuss organisational priorities and challenges, along with oversight and inspection activities.

Access to systems, personnel and information

In 2022–23, AGO provided the Office with appropriate direct access to AGO systems and facilities to support its oversight work. Overall, for individual inspections AGO provided access to appropriate personnel and information in a timely manner to enable the Office's oversight activities.

Inspections

The Office undertook and completed 17 inspections of AGO activities in 2022–23. There were no inspections underway but not completed at the end of 2021–22 or 2022–23.

In all 17 inspections, the Office did not identify legality or propriety concerns. The inspections covered the following topics or activities:

- COVIDSafe app data
- application of AGO's *Rules to Protect the Privacy of Australians* made under the IS Act (3 inspections)
- Ministerial Authorisations to undertake certain activities (3 inspections)
- ministerial submissions (1 inspection)
- Director's Approvals (3 inspections)
- Post Activity Compliance Reporting
- AGO's support to Defence advice to the Foreign Investment Review Board
- use of open source datasets
- provision of geospatial products to partners (3 inspections).

In a number of inspections, the Office provided findings and recommendations relating to AGO's record keeping and adherence to, or currency of, internal policies and procedures. AGO is actioning findings and recommendations. The Office will continue to review these areas in the 2023–24 inspection program.

Compliance incidents

The Office independently reviews all compliance incidents reported by AGO relating to non-compliance with legislation or AGO internal policies and procedures. In this reporting period, no compliance incidents were reported by AGO.

Other reviews

In 2022–23, the Office also reviewed AGO's compliance with the requirements of s 9D of the IS Act, regarding AGO's use of an emergency authorisation in relation to circumstances which involved an imminent risk to the safety of an Australian person who was outside Australia. Paragraph 9D(8)(b) of the IS Act requires the Inspector-General to provide the responsible minister a report on the Inspector-General's views of the extent of the compliance by the agency head with the requirements of s 9D and also provide a copy of the conclusions in the report to the PJCIS.

The Inspector-General concluded that the Director AGO complied with the requirements of s 9D of the IS Act when exercising this power, and informed the responsible minister and the PJCIS as required.

Defence Intelligence Organisation

In 2022–23, the Office has undertaken inspections of DIO's activities. The Office did not commence any inquiries under s 8 of the IGIS Act in relation to DIO.

The Office has implemented a risk-based approach to its inspections of DIO. Due to the nature of DIO's role, DIO's activities have a lower risk to the privacy of Australians and, therefore, the Office undertakes fewer oversight activities in relation to DIO's activities, compared to the activities of other intelligence agencies. In 2022–23, the Office undertook deep-dive inspections into DIO's activities in areas of higher risk or sensitivity.

The Inspector-General and the Office's senior leadership team met the Chief of Defence Intelligence and DIO senior executives twice in the reporting period. These meetings were a useful opportunity to discuss organisational priorities and challenges, along with oversight and inspection activities.

Access to systems, personnel and information

In 2022–23, DIO provided the Office with appropriate direct access to DIO systems and facilities to support its oversight work. Overall, for individual inspections DIO provided access to appropriate personnel and information in a timely manner to enable the Office's oversight activities.

Inspections

The Office commenced 4 inspections of DIO's activities and completed 4 inspections in 2022–23 reporting period. One inspection which was started in 2022–23 remains underway, and one inspection which started in 2021–22 was completed in the current reporting period.

In 3 out of the 4 finalised inspections, the Office did not identify legality or propriety concerns. These inspections were regarding:

- COVIDSafe app data
- application of DIO's *Rules to Protect the Privacy of Australians* made under the IS Act
- ministerial submissions.

The Office identified a propriety concern in one inspection, the details of which are provided below.

Analytic integrity

The Office undertook an inspection of DIO's approach to ensuring the analytic integrity of its intelligence assessment products and activities. This inspection focused primarily on areas of intelligence assessment management. The Office reviewed the tasking and scope of the products, conducted interviews of DIO staff and reviewed whether DIO could demonstrate that consultation and internal approval processes were transparent and free from bias. The purpose of the inspection was to determine DIO's ability to demonstrate analytic rigour, contestability and independence of judgements.

The Office made a number of findings and recommendations, the most substantial finding being that DIO was unable to demonstrate systemic analytical independence due to deficiencies in how analytic products are managed from initial tasking to final publication including record keeping around internal content changes. DIO accepted the findings and recommendations within the inspection report and has commenced implementing a range of measures to address areas

of concern. The Office will increase the number of inspections into the analytic independence and integrity of DIO intelligence assessments in 2023–24 to monitor implementation of the recommendations.

Compliance incidents

DIO did not report any compliance incidents to the Office in 2022–23.

Other reviews

In addition to inspection activities, the Office also reviewed DIO policies and procedures relevant to DIO's compliance with legislation or other directions. In 2022–23, DIO provided the Office with copies of its updated DIO Privacy Rules Policy. The Office provided a number of comments for DIO's consideration.

Australian Criminal Intelligence Commission and Australian Federal Police

In September 2021, the Office's jurisdiction was expanded with the enactment of the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*. The Act provides additional powers for the ACIC and AFP to identify and disrupt serious online crime. One of the new powers is a network activity warrant (NAW), which allows the ACIC and AFP to collect intelligence on criminal networks operating online. The Office has oversight responsibility for this warrant power and undertakes inspections to confirm the legality and propriety of ACIC's and AFP's activities in obtaining, managing and using a NAW.

Both agencies provided all required statutory notifications to the Inspector-General and provided appropriate access and support to enable the Office's oversight activities.

ACIC inspection

In the reporting period, the Office inspected the ACIC's use of NAWs, with a focus on the statutory requirements for documentation for the entire warrant cycle and compliance management systems. The Office did not identify any matters of legality or propriety.

AFP inspections

In the reporting period, the Office inspected the AFP's use of NAWs, examining records and policies relating to the application for, exercise of, and concluding of a NAW. The Office did not identify any matters of legality or propriety.

Cross-agency inspection and inquiry activities

Inquiries

During 2022–23, the Office conducted one inquiry and one preliminary inquiry that jointly reviewed the activities of multiple agencies.

Activities conducted under a TIA Act s 11C warrant and the s 11C(6) mandatory procedure

In September 2022, the Inspector-General informed the relevant ministers, and heads of agencies of his intention to conduct an inquiry into activities undertaken under a warrant issued by the Attorney-General under s 11C of the TIA Act. The inquiry, conducted between October 2022 and March 2023, examined the legality and propriety of the execution of the warranted activity, including the consistency of the activities with the requirements of the s 11C(6) mandatory procedure. The inquiry made a number of findings and recommendations across the agencies involved.

The findings identified one concern that the Attorney-General had not been provided with accurate information in the warrant request. Some inconsistencies were identified in the execution of the activities against the requirements of the s 11C(6) mandatory procedure. The inquiry made 3 recommendations that will enable the relevant agencies to strengthen evidence of propriety and the compliance of the activities being undertaken with the warrant and the mandatory procedure.

Although many of the findings of the inquiry were accepted by the agencies, external legal advice has been sought on some findings. Impacted agencies will also further investigate the feasibility of options to address some of the findings and recommendations provided by the Office. The Office will continue to work with these agencies to finalise these matters in 2023–24.

Preliminary Inquiries

During 2022–23, the Office commenced and completed one preliminary inquiry into the authorisations that allow communication of information obtained under a TIA Act warrant. The Inspector-General sought information from multiple agencies. Following receipt of responses from these agencies, the Inspector-General decided to commence a further limited inquiry of ASIO. The resulting inquiry commenced on 8 June 2023, and is discussed in the ASIO inquiries section on page 94.

Inspections

During 2022–23, the Office undertook 2 cross-agency inspection activities where it inspected agency activities related to:

- compliance with Part VIIIA of the *Privacy Act 1988* (Privacy Act) in relation to handling of incidentally collected COVID-19 app data; and
- compliance with the the Crimes Act requirements for annual reporting on use of assumed identities.

COVID-19 app data

In November 2022, the Office undertook an inspection of the agencies to confirm they were compliant with Part VIIIA of the Privacy Act in relation to the handling of incidentally collected COVID-19 app data. At the completion of this inspection, a report was provided to the Office of the Australian Information Commissioner and the Privacy Commissioner. In this inspection the Office found:

- there was no evidence to suggest agencies had deliberately targeted or have decrypted, accessed or used COVID-19 app data;
- agencies that have incidentally collected data had taken reasonable steps to quarantine and delete COVID-19 app data; and
- appropriate policies and procedures relating to any identified incidental collection of COVID-19 app data were in place, and were being adhered to.

The Office has received no complaints or PIDs about agencies' collection or use of COVID-19 app data.

With the decommissioning of the COVID-19 app and the repeal of the relevant parts of the Privacy Act on 14 November 2022, the Office will not undertake further inspections of the agencies in relation to this matter.

Use and management of assumed identities

The Crimes Act imposes reporting, administrative and audit regimes on those agencies using assumed identities. Section 15LG of the Crimes Act requires ASD, ASIO, ASIS and ONI to conduct 6 monthly audits of assumed identity records and s 15LE requires that each agency provide the Inspector-General with an annual report containing information on the assumed identities created and used during the year.

The Office conducted inspections of the assumed identities annual reporting provided by ASIO, ASIS, ASD and ONI for 2021–22. As agencies' reporting for 2022–23 will cover the creation and use of assumed identities up until 30 June 2023, this reporting is not available to the Office in the current reporting period, and will be reported in 2023–24.

- ASIO's annual reporting did not identify any issues, with the exception of the compliance incidents advised by ASIO and noted in the ASIO section of this report.
- ASIS did not identify any issues in its annual reporting. However, the Office did raise propriety concerns during inspections of ASIS assumed identities regime, which are detailed in the ASIS section of this report.⁴
- ASD did not authorise any assumed identities in 2021–22.⁵
- ONI and the Office did not identify any issues around ONI's use of assumed identities.

4 The ASIS Assumed Identities Annual Reporting for 2021–22 was received by the Office after 30 June 2023, but before this Annual Report content was developed. The Office is satisfied, based on the evidence provided by ASIS, that the internal audit work to inform the Assumed Identities Annual Report for 2021–22 was completed in a timely manner but due to an oversight was not provided to the Office before 30 June 2023.

5 The formal ASD Assumed Identities Annual Reporting for 2021–22 was not received by the Office before 30 June 2023. ASD had briefed the Office prior to 30 June 2023 that it had not authorised any assumed identities in 2021–22 and confirmed this in writing after 30 June 2023 but before this Annual Report content was developed.

Compliance incidents and other inspection activity relating to the use and management of assumed identities by ASIO, ASIS, ASD and ONI are detailed in the section detailing the oversight activities of each agency.

Complaints and Public Interest Disclosures

Key statistics



34

IGIS Act complaints received



6

PID Act disclosures
received and/or allocated



599

Other correspondence
handled[^]

[^]Included purported complaints that did not meet the jurisdiction of the IGIS Act or PID Act

The Office has a broad jurisdiction to receive and inquire into complaints and investigate disclosures concerning the conduct of ASIO, ASD, ASIS, and AGO, and the ACIC and AFP in relation to their intelligence functions regarding NAWs. In addition, the Office also has jurisdiction to investigate disclosures relating to the conduct of DIO and ONI.

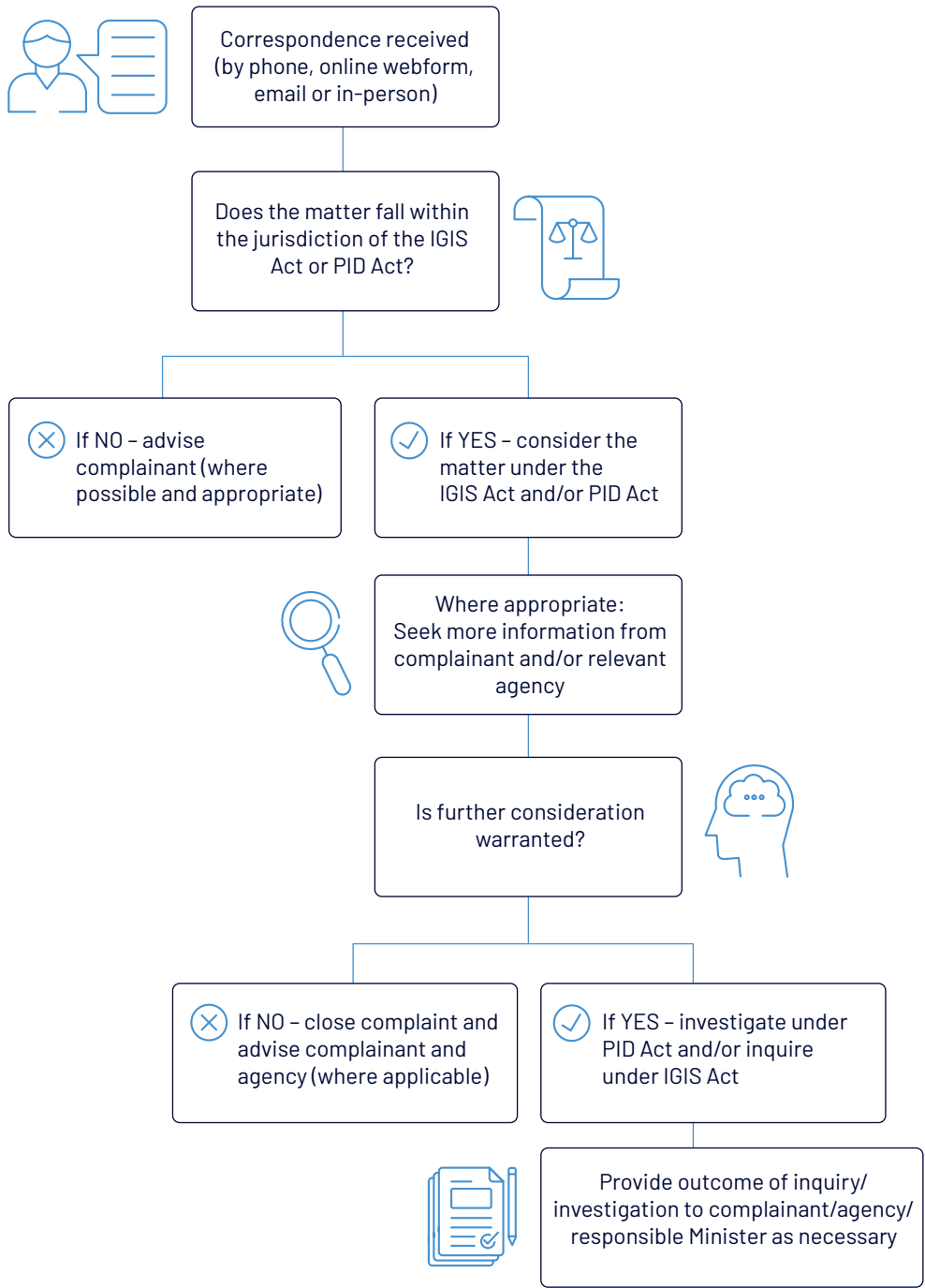
Matters that are brought to the Office may fall within the jurisdiction of the IGIS Act or the PID Act, or both. The Office also receives a large number of complaints and other correspondence that does not fall within the jurisdiction of those Acts. This can include concerns and grievances about entities other than Australian intelligence agencies, and requests for information about intelligence agencies, both of which fall outside of IGIS's jurisdiction. The Office reviews all correspondence it receives to determine whether a matter falls within the jurisdiction of the IGIS Act or the PID Act.

Table 6.1: Complaints and PID statistics

	2022–23 FY (1 July 2022 – 30 June 2023)	2021–22 FY (1 July 2021 – 30 June 2022)	2020–21 FY* (1 July 2020 – 30 June 2021)
Complaints that fell within the jurisdiction of the IGIS Act	34	80	344*
Other correspondence that did not fall within the jurisdiction of the IGIS Act or PID Act	599	431	N/A*
Visa & citizenship complaints and correspondence	70	141	124
PIDs	6	10	16

* In the 2020–21 Annual Report, the Office did not distinguish between 'complaints' (i.e. matters that fell within the jurisdiction of the IGIS Act) and 'contacts' (i.e. complaints and other correspondence that did not fall within the jurisdiction of the IGIS Act or PID Act). This approach was taken to demonstrate the high level of resources required to receive, consider and respond to all complaints and correspondence, whether or not they fell within IGIS's jurisdiction. Any comparison between the previous reporting periods and the current reporting period should take into account this difference in approach.

Figure 6.1: Complaints process



Complaints

Non-visa and citizenship related complaints

The number of non-visa and citizenship related matters raised with the Office increased during the reporting period – from 511 matters in 2021–22 to 633 matters in 2022–23. There was a decrease in the number of matters that fell within the jurisdiction of the IGIS Act, from 80 complaints in 2021–22 to 34 complaints in 2022–23.

Although there has been a decrease in the number of complaints received this year compared to 2021–22, this is commensurate with the 35 complaints received in 2019–20. The Office assessed each piece of correspondence to determine the most appropriate course of action, including to determine whether the matter fell within the jurisdiction of the IGIS Act or the PID Act. Where a matter was found not to engage either Act, the Office provided advice (where possible) to the complainant about the IGIS's jurisdiction.

IGIS officers sought complaints-related information from agencies by speaking with relevant agency staff, reviewing files and undertaking independent searches of agency databases to identify issues of legality or propriety. Most matters were able to be resolved in a timely manner having regard to the nature and complexity of each complaint.

Complaints received during the reporting period covered a wide range of matters, including allegations related to:

- employment issues, including recruitment
- conduct of investigations by other agencies, including under the PID Act
- surveillance, harassment and/or unauthorised interference with the person
- discrimination
- information gathering and sharing
- processes for conducting security assessments.

Visa and citizenship application complaints

The Office also receives complaints concerning the processing of visa and citizenship applications, particularly regarding the length of time taken to finalise applications beyond the indicative timeframes listed on the Department of Home Affairs' website. However, the Office's jurisdiction only extends to where those delays are a result of processes or practices within the intelligence agencies over which the Office has jurisdiction. Historically, the majority of visa and citizenship complaints received by the Office have concerned delays in finalising student visa applications.

The number of complaints regarding visa and citizenship applications decreased in 2022–23. An increased proportion of these complaints related to matters that did not fall within the Office's jurisdiction or had not exceeded the timeframes that the Office used as a threshold for further investigating the complaint.

The Office did not identify any systemic compliance issues in the visa and citizenship complaints investigated in 2022–23. The results of the Office's inspections into ASIO's role in visa and citizenship applications is reported in the ASIO section of this report.

Complaints inquiry

In early 2023, the Inspector-General commenced an inquiry into a complaint by Mr Daniel Duggan. The inquiry remained ongoing at the end of the reporting period.

Public interest disclosures

The Office has key responsibilities under the PID Act, including:

- receiving, and where appropriate, investigating disclosures about suspected wrongdoing within the intelligence agencies;
- assisting current or former public officials who work for, or who previously worked for, the intelligence agencies in relation to the operation of the PID Act;
- assisting the intelligence agencies in meeting their responsibilities under the PID Act, including through education and awareness activities; and
- overseeing the operation of the PID scheme in the intelligence agencies.

At the end of 2022–23, the Office had 16 authorised officers under the PID scheme in addition to its principal officer, the Inspector-General. These officers were accessible to intelligence agency staff in the course of their regular attendance at agencies for routine activities such as inspections and briefings. IGIS’s authorised officers were also contactable via secure email and phone.

The Office received 6 disclosures relating to intelligence agencies during the reporting period. Of these disclosures, IGIS allocated:

- 4 disclosures to intelligence agencies for investigation
- 2 disclosures to itself for investigation, which the Office is investigating in accordance with the PID Act.

No disclosures were allocated to the IGIS by an intelligence agency.

The kinds of disclosable conduct received by the Office during the reporting period included: allegations of maladministration; danger to health or safety; contraventions of Commonwealth, state or territory law; abuse of a position of trust; and conduct that could lead to disciplinary action. A PID may relate to one or more agencies, or types of disclosable conduct.

Table 6.2: Types of disclosable conduct

Disclosable conduct	Number of disclosures
Maladministration	3
Contravention of a law of the Commonwealth, state or territory	1
Danger to health or safety	2
Could lead to disciplinary action against a public official	3
Abuse of position of trust	3
Conduct that perverts the course of justice	3

Disclosure relating to DIO

During the reporting period, the Office finalised a disclosure investigation relating to a DIO employment matter. The disclosure raised concern about the actions taken by DIO in response to the discloser's own misconduct. The disclosure had been received and allocated to the IGIS in a previous reporting period. The Inspector-General's investigation found that no instances of disclosable conduct had occurred and made 5 recommendations to DIO that could assist it to improve some of its practices and procedures. A copy of the final report was provided to the discloser and DIO.

Preliminary inquiry into ASD

On 23 January 2023, the Inspector-General, by his own motion, commenced a preliminary inquiry into ASD's administration of PIDs under the PID Act. The preliminary inquiry followed receipt of a number of complaints made to this Office during the current and previous reporting periods, which raised concerns about ASD's handling of PIDs. The purpose of the preliminary inquiry is to determine whether the Inspector-General should inquire further into ASD's administration of the PID scheme. The preliminary inquiry remains ongoing.

Overseeing the operation of the PID scheme in the intelligence agencies

In accordance with s 44(1A)(b) of the PID Act, intelligence agencies – and the ACIC and AFP in relation to their intelligence functions regarding NAWs – are required to meet certain reporting requirements. This includes informing the IGIS when a PID is allocated to an intelligence agency (or the ACIC and AFP where relevant) for investigation.

The Office was notified of 5 PIDs received directly by the intelligence agencies or the ACIC or AFP, during the reporting period. In each of these cases, the recipient agency allocated the PID to itself for investigation.

The agencies advised the Office of the actions taken in each matter, and discussed PID-related issues with the Office as necessary.

IGIS also has statutory responsibilities for assisting agency staff in their obligations under the PID Act and for conducting training and awareness raising exercises. During the reporting period, the Office provided assistance and guidance to officials within the intelligence agencies about the operation of the scheme. This included delivering an information session about the PID scheme to members of the intelligence agencies, directed to authorised officers and other PID officials.

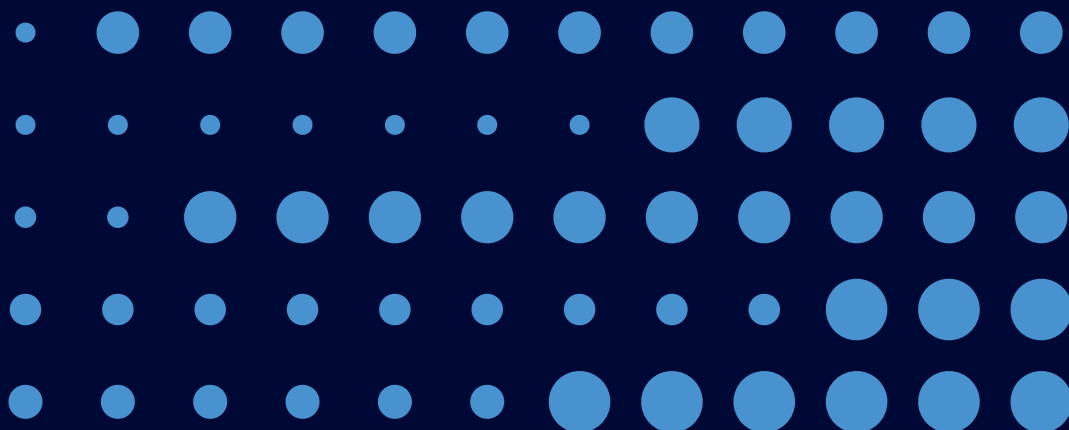
PIDs about the Office

As a Commonwealth Public Sector agency, the Office is also an agency for the purposes of the PID Act and public officials can make disclosures about suspected wrongdoing relating to it.

During 2022–23, no PIDs were made about this Office.

Section Seven

Annexures



Annexure 7.1

Other mandatory information

Subsection 17AH(2) of the PGPA Rule provides for the inclusion of other mandatory information, as required by an Act or instrument, in one or more appendices to an annual report prepared for a non-corporate Commonwealth entity.

Advertising and market research

The following information is provided in accordance with the requirements of s 311A of the *Commonwealth Electoral Act 1918*.

The Office did not incur any expenditure on advertising campaigns, market research, polling or direct mailing during the reporting period.

Ecologically sustainable development and environmental performance

The following information is provided in accordance with the requirements of s 516A of the *Environment Protection and Biodiversity Conservation Act 1999*.

The Office is committed to ensuring that its activities are environmentally responsible.

Through its co-location with AGD, the Office continues to benefit from AGD's commitments to energy saving measures. This includes a large number of energy and water saving measures, such as energy efficient lighting, heating and cooling which are incorporated into the Office premises at 3-5 National Circuit, Barton ACT.

Utilities consumption for the Office were not separately measured. For this reason, ecologically sustainable development and details of environmental performance are not able to be quantified in this report.

While the majority of the Office's infrastructure is provided and maintained by a host department, the Office considers and acts to minimise the environmental impact across a number of areas for which it is directly responsible.

These include:

- purchasing and using Australian-made recycled and/or carbon neutral paper
- configuring printers to print double-sided by default
- recycling all unclassified office paper and cardboard waste
- recycling empty toner cartridges
- continued use of a hybrid vehicle.

APS Net Zero 2030 emissions reporting

APS Net Zero 2030 is the government’s policy for the APS to reduce its greenhouse gas emissions to net zero by 2030, and transparently report on its emissions. As part of this, non-corporate and corporate Commonwealth entities are required to report on their operational greenhouse gas emissions.

The Greenhouse Gas Emissions Inventory presents greenhouse gas emissions over the 2022-23 period. Results are presented on the basis of Carbon Dioxide Equivalent (CO₂-e) emissions. Greenhouse gas emissions reporting has been developed with methodology that is consistent with the Whole-of-Australian Government approach as part of the APS Net Zero 2030 policy. Not all data sources were available at the time of the report and adjustments to baseline data may be required in future reports.

Due to the Office’s tenancy arrangement with AGD, the Office is unable to separately measure its electricity and natural gas usage from that of the other tenants at 3-5 National Circuit, Barton ACT. The Office’s electricity and natural gas emissions will be included in AGD’s emissions reporting.

Table 7.1: Greenhouse gas emissions inventory – location-based method 2022-23

Emission source	Scope 1 kg CO ₂ -e	Scope 2 kg CO ₂ -e	Scope 3 kg CO ₂ -e	Total kg CO ₂ -e
Electricity (location based approach)	N/A	-	-	-
Natural gas	-	N/A	-	-
Fleet vehicles	185	N/A	47	232
Domestic flights	N/A	N/A	13,141	13,141
Other energy	-	N/A	-	-
Total kg CO₂-e	185	-	13,188	13,372

Annexure 7.2

Requirements for annual reports

Below is the table set out in Schedule 2 of the PGPA Rule. Section 17AJ(d) requires this table be included in entities' annual reports as an aid of access.

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AD(g)	Letter of transmittal			
17AI	Preliminaries	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 section 46 of the Act and any enabling legislation that specifies additional requirements in relation to the annual report.	Mandatory	iii
17AD(h)	Aids to access			
17AJ(a)	Preliminaries	Table of contents (print only).	Mandatory	iv–v
17AJ(b)	Annexures	Alphabetical index (print only).	Mandatory	143
17AJ(c)	Preliminaries	Glossary of abbreviations and acronyms.	Mandatory	vii–viii
17AJ(d)	Annexures	List of requirements.	Mandatory	132–142
17AJ(e)	Preliminaries	Details of contact officer.	Mandatory	ii
17AJ(f)	Preliminaries	Entity's website address.	Mandatory	ii
17AJ(g)	Preliminaries	Electronic address of report.	Mandatory	ii
17AD(a)	Review by accountable authority			
17AD(a)	Section 1	A review by the accountable authority of the entity.	Mandatory	2–3
17AD(b)	Overview of the entity			
17AE(1)(a)(i)	Section 2	A description of the role and functions of the entity.	Mandatory	8

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AE(1)(a)(ii)	Section 2	A description of the organisational structure of the entity.	Mandatory	10
17AE(1)(a)(iii)	Section 3	A description of the outcomes and programmes administered by the entity.	Mandatory	17
17AE(1)(a)(iv)	Section 2	A description of the purposes of the entity as included in corporate plan.	Mandatory	6
17AE(1)(aa)(i)	Section 3	Name of the accountable authority or each member of the accountable authority.	Mandatory	16
17AE(1)(aa)(ii)	Section 3	Position title of the accountable authority or each member of the accountable authority.	Mandatory	16
17AE(1)(aa)(iii)	Section 4	Period as the accountable authority or member of the accountable authority within the reporting period.	Mandatory	39
17AE(1)(b)	n/a	An outline of the structure of the portfolio of the entity.	Portfolio departments mandatory	n/a
17AE(2)	n/a	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	Section 3	Annual performance statement in accordance with paragraph 39(1)(b) of the Act and section 16F of the Rule.	Mandatory	16–29

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AD(c)(ii)	Report on Financial Performance			
17AF(1)(a)	Section 5	A discussion and analysis of the entity's financial performance.	Mandatory	53–81
17AF(1)(b)	Section 5	A table summarising the total resources and total payments of the entity.	Mandatory	80–81
17AF(2)	n/a	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	n/a
17AD(d)	Management and Accountability			
	Corporate Governance			
17AG(2)(a)	Section 4	Information on compliance with section 10 (fraud systems).	Mandatory	48
17AG(2)(b)(i)	Preliminaries	A certification by accountable authority that fraud risk assessments and fraud control plans have been prepared.	Mandatory	iii
17AG(2)(b)(ii)	Preliminaries	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	iii

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(2)(b) (iii)	Preliminaries	A certification by accountable authority that all reasonable measures have been taken to deal appropriately with fraud relating to the entity.	Mandatory	iii
17AG(2)(c)	Section 4	An outline of structures and processes in place for the entity to implement principles and objectives of corporate governance.	Mandatory	41-48
17AG(2)(d) –(e)	n/a	A statement of significant issues reported to Minister under paragraph 19(1)(e) of the Act that relates to non-compliance with Finance law and action taken to remedy non-compliance.	If applicable, mandatory	n/a
Audit Committee				
17AG(2A)(a)	Section 4	A direct electronic address of the charter determining the functions of the entity's audit committee.	Mandatory	42
17AG(2A)(b)	Section 4	The name of each member of the entity's audit committee.	Mandatory	42-43
17AG(2A)(c)	Section 4	The qualifications, knowledge, skills or experience of each member of the entity's audit committee.	Mandatory	42-43
17AG(2A)(d)	Section 4	Information about the attendance of each member of the entity's audit committee at committee meetings.	Mandatory	42-43
17AG(2A)(e)	Section 4	The remuneration of each member of the entity's audit committee.	Mandatory	42-43
External Scrutiny				
17AG(3)	Section 4	Information on the most significant developments in external scrutiny and the entity's response to the scrutiny.	Mandatory	49

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(3)(a)	n/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)	Section 4	Information on any reports on operations of the entity by the Auditor-General (other than report under section 43 of the Act), a Parliamentary Committee, or the Commonwealth Ombudsman.	If applicable, mandatory	49
17AG(3)(c)	n/a	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)	Section 4	An assessment of the entity's effectiveness in managing and developing employees to achieve entity objectives.	Mandatory	32
17AG(4)(aa)	Section 4	Statistics on the entity's employees on an ongoing and nonongoing basis, including the following: (a) statistics on fulltime employees; (b) statistics on parttime employees; (c) statistics on gender (d) statistics on staff location	Mandatory	36

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(4)(b)	Section 4	<p>Statistics on the entity's APS employees on an ongoing and nonongoing basis; including the following:</p> <ul style="list-style-type: none"> • Statistics on staffing classification level; • Statistics on fulltime employees; • Statistics on part-time employees; • Statistics on gender; • Statistics on staff location; • Statistics on employees who identify as Indigenous. 	Mandatory	36–37
17AG(4)(c)	Section 4	Information on any enterprise agreements, individual flexibility arrangements, Australian workplace agreements, common law contracts and determinations under subsection 24(1) of the <i>Public Service Act 1999</i> .	Mandatory	38
17AG(4)(c)(i)	Section 4	Information on the number of SES and nonSES employees covered by agreements etc identified in paragraph 17AG(4)(c).	Mandatory	38
17AG(4)(c)(ii)	Section 4	The salary ranges available for APS employees by classification level.	Mandatory	37
17AG(4)(c)(iii)	Section 4	A description of nonsalary benefits provided to employees.	Mandatory	38
17AG(4)(d)(i)	n/a	Information on the number of employees at each classification level who received performance pay.	If applicable, mandatory	n/a
17AG(4)(d)(ii)	n/a	Information on aggregate amounts of performance pay at each classification level.	If applicable, mandatory	n/a
17AG(4)(d)(iii)	n/a	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	Part of Report	Description	Requirement	Page
17AG(4)(d)(iv)	n/a	Information on aggregate amount of performance payments.	If applicable, mandatory	n/a
Assets Management				
17AG(5)	Section 4	An assessment of effectiveness of assets management where asset management is a significant part of the entity's activities.	If applicable, mandatory	49
Purchasing				
17AG(6)	Section 4	An assessment of entity performance against the <i>Commonwealth Procurement Rules</i> .	Mandatory	49-50
Reportable consultancy contracts				
17AG(7)(a)	Section 4	A summary statement detailing the number of new reportable consultancy contracts entered into during the period; the total actual expenditure on all such contracts (inclusive of GST); the number of ongoing reportable consultancy contracts that were entered into during a previous reporting period; and the total actual expenditure in the reporting period on those ongoing contracts (inclusive of GST).	Mandatory	50
17AG(7)(b)	Section 4	A statement that “During [reporting period], [specified number] new reportable consultancy contracts were entered into involving total actual expenditure of \$[specified million]. In addition, [specified number] ongoing reportable consultancy contracts were active during the period, involving total actual expenditure of \$[specified million]”.	Mandatory	51

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(7)(c)	Section 4	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	50
17AG(7)(d)	Section 4	A statement that <i>"Annual reports contain information about actual expenditure on reportable consultancy contracts. Information on the value of reportable consultancy contracts is available on the AusTender website."</i>	Mandatory	50
Reportable non-consultancy contracts				
17AG(7A)(a)	Section 4	A summary statement detailing the number of new reportable non-consultancy contracts entered into during the period; the total actual expenditure on such contracts (inclusive of GST); the number of ongoing reportable non-consultancy contracts that were entered into during a previous reporting period; and the total actual expenditure in the reporting period on those ongoing contracts (inclusive of GST).	Mandatory	50
17AG(7A)(b)	Section 4	A statement that <i>"Annual reports contain information about actual expenditure on reportable non-consultancy contracts. Information on the value of reportable non-consultancy contracts is available on the AusTender website."</i>	Mandatory	50
17AD(daa)	Additional information about organisations receiving amounts under reportable consultancy contracts or reportable non-consultancy contracts			
17AGA	Section 4	Additional information, in accordance with section 17AGA, about organisations receiving amounts under reportable consultancy contracts or reportable non-consultancy contracts.	Mandatory	51-52

PGPA Rule Reference	Part of Report	Description	Requirement	Page
Australian National Audit Office Access Clauses				
17AG(8)	Section 4	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 Auditor-General 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	52
Exempt contracts				
17AG(9)	Section 4	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	52
Small business				
17AG(10)(a)	Section 4	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	50
17AG(10)(b)	Section 4	An outline of the ways in which the procurement practices of the entity support small and medium enterprises.	Mandatory	50

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(10)(c)	n/a	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	n/a
Financial Statements				
17AD(e)	Section 5	Inclusion of the annual financial statements in accordance with subsection 43(4) of the Act.	Mandatory	53–81
Executive Remuneration				
17AD(da)	Section 4	Information about executive remuneration in accordance with Subdivision C of Division 3A of Part 23 of the Rule.	Mandatory	39
17AD(f)	Other Mandatory Information			
17AH(1)(a)(i)	n/a	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	n/a
17AH(1)(a)(ii)	Annexures	If the entity did not conduct advertising campaigns, a statement to that effect.	If applicable, mandatory	130
17AH(1)(b)	n/a	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	n/a

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AH(1)(c)	Section 4	Outline of mechanisms of disability reporting, including reference to website for further information.	Mandatory	40
17AH(1)(d)	Section 4	Website reference to where the entity's Information Publication Scheme statement pursuant to Part II of FOI Act can be found.	Mandatory	52
17AH(1)(e)	n/a	Correction of material errors in previous annual report	If applicable, mandatory	n/a
17AH(2)	Section 4 Section 6 Annexures	Information required by other legislation	Mandatory	40, 83-127, 130-131

Index

A

- abbreviations, vii–viii
- accountability and management, 32–52
- accountable authority, 16, 41
- Accountable Authority Instructions, 49, 50
- address and contact information (IGIS), ii
- Administrative Appeals Tribunal (AAT), 12
- advertising and market research, 130
- AGO *see* Australian Geospatial-Intelligence Organisation (AGO)
- Alexander v Minister for Home Affairs* [2022] HCA19, 114
- ANAO *see* Australian National Audit Office
- annual performance statement
 - accountable authority statement, 16
 - reporting framework, 17
 - results:
 - Objective 1: Inquiries, 18–19
 - Objective 2, Inspections, 20–21
 - Objective 3, Complaints, 22–23
 - Objective 4, Public interest disclosures, 24–25
 - Objective 5, Assurance, 26–27
 - Objective 6, Organisational capabilities, 28–29
- anti-corruption commission *see* National Anti-Corruption Commission
- Anti-Discrimination and Human Rights Legislation Amendment (Respect at Work) Act 2022*, 2
- Anti-Discrimination and Human Rights Legislation Amendment (Respect at Work) Bill 2022*, 12
- APS *see* Australian Public Service
- Archives Act 1983*, 8, 12
- ASD *see* Australian Signals Directorate (ASD)
- ASIO *see* Australian Security Intelligence Organisation (ASIO)
- ASIS *see* Australian Secret Intelligence Service (ASIS)
- asset management, 49
- Assistant Inspectors-General, 10, 39
- assumed identities, 93, 104, 105, 107, 120, 121–122
- assurance
 - assisting ministers, 11
 - assuring parliament, 11–12
 - expert evidence to AAT or OAIC, 12
 - informing the public, 13
 - performance results and analysis, 26–27
 - see also* ministers; parliamentary committees; public information
- Attorney-General, 9, 44, 93, 112, 120
 - ASIO reporting obligations, 97, 98, 101–102, 105
 - authorisations, 98
 - IGIS updates for, 11
 - powers, 85
 - warrants, 85, 98, 101–102, 105, 120
- Attorney-General's Department, 3, 32, 43, 44
 - Office co-location with, 44, 130, 131
- Audit Committee, 40, 42–43, 47
- Auditor-General *see* Australian National Audit Office
- audits
 - financial statements audit report, 49, 54–55
 - internal, 43, 47
- AUSTRAC information, 92, 99
- Australian Commission for Law Enforcement Integrity (ACLEI), 44
- Australian Criminal Intelligence Commission (ACIC)
 - complaints against *see* complaints
 - IGIS role in respect of, 8, 119
- Australian Cyber Security Centre (ACSC), 87
- Australian Federal Police (AFP)
 - complaints against *see* complaints
 - IGIS role in respect of, 8, 119
- Australian Geospatial-Intelligence Organisation (AGO), 88, 115–116
 - complaints against *see* complaints
 - compliance incidents, 116
 - inspections, 88, 115
 - key statistics, 88
 - Ministerial Authorisations, 115
 - responsible minister, 88
 - role and functions, 88
- Australian Human Rights Commission, 44
- Australian Human Rights Commission Act 1986*, 44
- Australian Information Commissioner, 12, 45, 121
- Australian National Audit Office, 49
 - access clauses in contracts, 52
 - financial statements audit report, 49, 54–55
- Australian National University National Security College, 29, 33
- Australian persons' privacy protections *see* Privacy Rules

Australian Public Service (APS)
 APS Academy, 33
 APS Values and Code of Conduct, 48
 Census, 33
 Net Zero 2030 emissions reporting, 131
 Australian Public Service Commissioner, 3
 Australian Secret Intelligence Service (ASIS), 86, 106–109
 assumed identities, 107, 121
 complaints against *see* complaints
 compliance incidents, 86, 108–109
 cooperation with ASIO, 107
 emergency authorisations, 109
 human rights procedures, 107, 108
 inspections, 86, 106–108
 key statistics, 86
 ministerial directions, 108
 operational files, 107–108
 Privacy Rules non-compliance, 109
 responsible minister, 86
 role and functions, 86
 weapons management and use, 108
 Australian Security Intelligence Organisation (ASIO), 85, 94–105
 analytic integrity, 96
 assumed identities, 104, 105
 complaints against *see* complaints
 compliance incidents, 85, 99–105
 cooperation with ASIS, 107
 data collection and retention, 96
 device access orders, 98
 human source management, 97
 IGIS role in respect of ASIO, 6
 inquiries, 85, 94
 inspections, 85, 95–98
 interaction with minors, 97
 key statistics, 85
 non-warranted surveillance operations, 96
 questioning sessions, 98
 responsible minister, 85
see also Minister's Guidelines to ASIO
 role and functions, 85
 special intelligence operations, 97, 98
 use of force, 98
 warrants, 98
 Australian Security Intelligence Organisation Act 1979 (ASIO Act), 85, 94–96, 98–99
 non-compliance, 101–102, 105

Australian Security Intelligence Organisation
 Amendment Bill 2023, 12
 Australian Signals Directorate (ASD), 87, 110–114
 assumed identities, 121
 complaints against *see* complaints
 compliance incidents, 87, 112–114
 emergency authorisations, 114
 inquiries, 87, 110–111
 inspections, 87, 111–112
 key statistics, 87
 Ministerial Authorisations, 110–111
 preliminary inquiry, 127
 Project REDSPICE, 110, 111
 public interest disclosures, 127
 responsible minister, 87
 role and functions, 87
 Australian Taxation Office, 104
 Australian Transaction Reports and Analysis Centre (AUSTRAC) information, 92, 99

B

Brookes, Chris, 10, 39
 Business Continuity Plan, 47

C

Census Action Plan, 33–34
 Chief of Defence Force, 89
 Chief of Defence Intelligence, 117
 citizenship application-related complaints, 4, 125
 committees, 41–43
 Commonwealth Contracting Suite, 50, 52
 Commonwealth Fraud Control Framework 2017, 48
 Commonwealth Indigenous Procurement Policy, 50
 Commonwealth Ombudsman, 45, 49
 Commonwealth Procurement Rules, 49, 50
 communications interception *see*
Telecommunications (Interception and Access) Act 1979 (TIA Act)
 complaints, 2, 4, 8, 9
 IGIS function and powers, 123
 inquiry, 126
 non-visa related, 125
 performance results and analysis, 22–23
 process, 124
 statistics, 123
 visa or citizenship related, 125
 compliance discipline, 2, 91
 compliance incidents, 2, 4

- AGO, 116
- ASD, 112–114
- ASIO, 99–105
- ASIS, 108–109
- DIO, 118
- ONI, 93
- Comprehensive Review of the Legal Framework of the National Intelligence Community (Richardson Review), 35
- consultants, 50–51
- contact information (Office), ii
- contracts, 50–52
- conversation series *see* Margaret Stone Conversation Series
- Cook, Katherine, 10, 39
- corporate governance, 3, 41–43
- Corporate Plan, 16–17, 35
- corporate support, 44
- corruption *see* ethical standards; fraud control
- Counter-Terrorism (Temporary Exclusion Orders) Act 2019*, review of, 11
- COVID-19 pandemic
 - COVIDSafe app data, 45, 120, 121
 - return to ‘business as usual’, 2
- Crimes Act 1914*, 93, 104, 105, 107, 120, 121
- Criminal Code compliance, 103
- cross-agency inspection and inquiry activities, 90, 120–122
- cyber security, 87

D

- data collection and retention, 96 *see also* *Telecommunications (Interception and Access) Act 1979* (TIA Act)
- data sharing, 105
- Defence Intelligence Organisation (DIO), 89, 117–118
 - analytic integrity, 117–118
 - compliance incidents, 118
 - disclosure investigation, 127
 - inspections, 89, 117–118
 - key statistics, 89
 - responsible minister, 89
 - role and functions, 89
- definitions, vii–viii
- Department of Defence, 87, 88, 89
- Department of Home Affairs, 85
- Deputy Inspector-General, 10, 37, 39
- device access orders, 98
- DIO *see* Defence Intelligence Organisation (DIO)

- Director of AGO, 115
- Director-General of National Intelligence, 93
- Director-General of Security, 94, 96
 - authorisations, 94, 104
 - warrant requests, 100
- disability reporting, 40
- disclosures, public interest *see* public interest disclosures
- diversity and inclusion initiatives, 28, 29, 32
- Duggan, Daniel, 126

E

- ecologically sustainable development and environmental performance, 130–131
- emergency authorisations, 109, 114, 116
- emissions reporting, 131
- employees *see* staff
- engagement program *see* international engagement; public information
- enterprise agreement, 38
- entity resource statement, 80–81
- ethical standards, 48 *see also* fraud control
- Executive Board, 34, 40, 41, 47
- Executive Director, Enterprise Management Unit, 10, 39
- executives *see* Key Management Personnel; Senior Executive Service officers
- exempt contracts, 52
- expenses for outcome, 81
- expert evidence to AAT or OAIC, 12
- external scrutiny of IGIS, 49–52

F

- Fallen, Brad, 39
- financial services, 44
- financial statements, 54–79
 - audit report, 49, 54–55
 - entity resource statement, 80–81
- firearms *see* weapons management and use
- Five-Eyes Intelligence Oversight and Review Council, 3, 27, 45–46
- force, use of, 99
- fraud control, iii, 3, 47, 48
- Freedom of Information Act 1982*, 8, 12, 52
- functions *see* roles and functions

G

geospatial intelligence agency *see* Australian Geospatial-Intelligence Organisation (AGO)
governance *see* corporate governance;
information governance framework
Governance Directorate, 47
greenhouse gas emissions reporting, 131

H

health *see* workplace health and safety
human resources management *see* staff
human rights legislation, 2
human rights matters, 44, 107
human source management, 97

I

identities, assumed, 93, 104, 105, 107, 120, 121–122
Indigenous businesses, commitment to, 50
information and communications technology (ICT), 3, 28, 29, 44
information governance framework, 3, 28, 29
Information Publication Scheme, 52
information security authority *see* Australian Signals Directorate (ASD)
Innovation Trial, 34
inquiries, 4, 8, 9
ASD, 110–111
commenced, 2, 90, 110
completed, 2, 90
cross-agency, 90, 120
notification and reporting requirements, 11
performance results and analysis, 18–19
preliminary inquiries, 90, 110, 111, 120
inquiries by parliamentary committees *see* parliamentary committees
inspections, 2, 4, 8, 9, 91
ACIC, 119
AFP, 119
AGO, 88, 115
ASD, 87, 111–112
ASIO, 85, 95–99
ASIS, 86, 106–108
cross-agency, 90, 120–122
DIO, 89, 117–118
ONI, 84, 92–93
performance results and analysis, 20–21
see also compliance incidents
Inspector-General of Intelligence and Security approach, 7

investigative powers, 8
key activities, 9
letter of transmittal, iii
Office organisation chart, 10
PIDs about Office, 127
purpose of Office, 6, 12, 17
remuneration, 38, 39
review of year, 2–4
role and functions, 2, 6, 8, 11–13, 93, 123–127
statutory office holder, 36, 38
Inspector-General of Intelligence and Security Act 1986, 2, 6, 8, 9, 11, 13, 16, 17, 19–25
complaints handling *see* complaints
inquiries under *see* inquiries
Inspector-General of Intelligence and Security and Other Legislation Amendment (Modernisation) Bill 2022, 11, 12
Inspector-General's Award for Innovation, 34
Integrity Agencies Group meetings, 3, 44
intelligence agencies
engagement with, 2, 26, 27
IGIS role, 6, 8 *see also* Inspector-General of Intelligence and Security
role and powers of agencies, 2, 84–90
see also Australian Geospatial-Intelligence Organisation (AGO); Australian Secret Intelligence Service (ASIS); Australian Security Intelligence Organisation (ASIO); Australian Signals Directorate (ASD); Defence Intelligence Organisation (DIO); Office of National Intelligence (ONI)
Intelligence Services Act 2001, 86–89, 106, 110, 114, 115, 116
ASIS–ASIO cooperation, 107
emergency authorisations, 109, 114, 116
ministerial directions, 108
non-compliance, 109
privacy rules *see* Privacy Rules
internal audit, 43, 47
international engagement, 3, 27, 45–46
intranet, 28, 29

J

Jessup, Christopher, 10, 39 *see also* Inspector-General of Intelligence and Security

K

Key Management Personnel, 10, 38–39, 74

L

leadership development, 3, 33
Leadership Group, 40
learning and development, 28–29, 33
legislative changes and drafts, 2–3, 11–12, 27
letter of transmittal, iii

M

management and accountability, 32–52
Margaret Stone Conversation Series, 3, 34
market research, 130
Minister for Defence, 87, 88, 89, 110, 111, 112
Minister for Foreign Affairs, 86, 108
Minister for Home Affairs, 85, 114
Ministerial Authorisations, 86, 87, 88, 110–111, 115
ministerial directions, 86, 87, 88, 108
ministerial letters, 4, 23, 84–89
ministers
 reporting to, 11, 17, 20, 21, 26–27
 requests from, 9, 11
 responsible for intelligence agencies, 84–89
Minister's Guidelines to ASIO, 85, 94
 non-compliance, 96, 98, 99–100, 102–103, 104–105
minors, ASIO interaction with, 97
Moore, Stephen, 43

N

National Anti-Corruption Commission, 44
National Anti-Corruption Commission Act 2022, 2
National Intelligence Academy, 33
National Intelligence Community (NIC)
 enterprise management, 84, 92
 see also intelligence agencies
National Museum of Australia, Cultural and Corporate Shared Services Centre, 44
National Security and Intelligence Review Agency (Canada), visit from, 46
National Security College
 Office's Participating Agency status, 29, 33
National Security Legislation Amendment (Comprehensive Review and Other Measures No. 2) Bill 2023, 11, 12
nationality, overturned presumptions of, 112
Net Zero 2030 emissions reporting, 131
network activity warrants (NAWs), 8, 119
non-compliance with law, standards or procedures, 2
ASD, 111, 112–114

ASIO, 96, 97, 98, 99–105

ASIS, 107

ONI, 93

see also compliance incidents; inquiries;
 inspections; public interest disclosures

non-salary benefits, 38 *see also* remuneration
Notzon-Glenn, Bronwyn, 10, 39

O

Office of National Intelligence (ONI), 84, 92–93
Office of National Intelligence Act 2018, 84, 92, 93
 assumed identities, 93, 121
 compliance incidents, 93
 inspections, 84, 92–93
 key statistics, 84
 privacy rules compliance, 92
 privacy rules update, 93
 responsible minister, 84
 role and functions, 84
Office of the Australian Information Commissioner, 12, 45, 121
Office of the Commonwealth Ombudsman, 45, 49
Office of the Inspector-General of Intelligence and Security *see* Inspector-General of Intelligence and Security
ONI *see* Office of National Intelligence (ONI)
open source intelligence, 93
organisation chart, 10
organisational capabilities, 28–29
 Oversight Capability Review, 34
 see also staff
organisational profile, 36–40
outcome (IGIS), 17
 Portfolio Budget Statement, 17
 resources for outcome, 80–81
 see also annual performance statement
overturned presumptions of nationality, 112

P

parliamentary committees
 IGIS submissions and appearances, 3, 11–12, 26, 27, 49
Parliamentary Joint Committee on Intelligence and Security (PJCIS), 109, 114, 116
 IGIS submissions and appearances, 3, 11–12, 49
People Capability Framework, 33
performance pay, 40
performance results and discussion *see* annual performance statement

personal information protection see Privacy Rules
 Portfolio Budget Statements, 16–17
 portfolio, Attorney-General's, 44
 Prime Minister, 8, 9, 11, 17, 84, 92, 93
Privacy Act 1988, 45, 120, 121
 Privacy Commissioner, 93, 121
 Privacy Rules, 86, 87, 88, 92, 93, 111, 112, 115, 117, 118
 non-compliance, 107, 109
 procurement see purchasing and procurement
 professional development see learning and development
 Project REDSPICE, 110, 111
Public Governance, Performance and Accountability Act 2013, 16, 41, 42, 48, 49, 50
 Public Governance, Performance and Accountability Rule 2014, 39, 49, 50, 130
 compliance statement, 132–142
 public information, 8, 13, 26–27, 49, 52
Public Interest Disclosure Act 2013, 8, 9, 24, 25, 125, 126
Public Interest Disclosure Amendment (Review) Act 2023, 2
 Public Interest Disclosure Amendment (Review) Bill 2022, 12
 public interest disclosures, 2, 9, 126–127
 about the Office, 127
 IGIS function and powers, 123–127
 intelligence agency obligations, 127
 performance results and analysis, 24–25
 process, 124
 statistics, 4, 123
 types of disclosable conduct, 126
Public Service Act 1999, 38
 purchasing and procurement, 49–51
 purpose, 6, 12, 17

Q

Quiggin, Peter, 43

R

Reconciliation Action Plan, 28, 29, 32
 record keeping, 91
 AGO, 115
 ASD, 111, 112
 ASIO, 95, 97
 ASIS, 108
 DIO, 117
 Office, 16, 28
 ONI, 93

recruitment, 3, 28, 29, 36
 REDSPICE, 110, 111
 regulation see Ministerial Authorisations;
 ministerial directions; Privacy Rules
 remuneration, 37, 38–40, 74
 resources for outcome, 80–81
 review of year, 2–4
 Richardson Review, 35
 risk management, 47–48
 roles and functions
 IGIS, 2, 6, 8, 12, 93, 119, 123–127
 intelligence agencies, 84–89
Rules to Protect the Privacy of Australians see Privacy Rules

S

Secretary of Defence, 16, 19, 89
 security clearance processes, 36, 38
 Security Plan, 47
 Senate Legal and Constitutional Affairs Legislation Committee, 12, 49
 Senior Executive Service officers, 37, 38–39 see also Key Management Personnel
 senior management committees, 41–43
 signals intelligence see Australian Signals Directorate (ASD)
 small business participation in procurement, 50
 special intelligence operations, 85, 97
 staff
 APS Census feedback, 33–34
 average staffing level, 36, 81
 diversity and inclusion, 28, 29, 32
 employment arrangements, 38
 Key Management Personnel, 10, 38–39, 74
 learning and development, 28, 29, 33
 non-salary benefits, 36
 performance agreements, 33, 48
 profile, 4, 36–37
 recruitment and retention, 3, 28, 29, 33, 36
 remuneration, 37, 38–40
 SES officers, 37, 38–39
 workplace health and safety, 40
 see also organisational capabilities
 Staff Consultative Committee, 33
 staff presentations at public forums, 13
 stakeholder engagement, 44–45
 Stanbridge, Sarah, 10, 39
 state legislation, potential non-compliance with, 105

Stone, Margaret, 3, 34
Surveillance Legislation Amendment (Identify and Disrupt) Act 2021, 8, 119
surveillance operations, non-warranted, 96

T

Technical Advisor role, 35
Telecommunications (Interception and Access) Act 1979 (TIA Act)
ASD non-compliance, 113–114
ASIO non-compliance, 99–102, 104–105
cross-agency inquiry, 120
Telecommunications Act 1997, 98, 105
training and development, 28, 29, 33
transparency, 8, 13, 26–27, 49, 52

U

use of force, 99
use of weapons, 108

V

values, 7, 48 *see* ethical standards
Vandenbroek, Sarah, 42
visa-related complaints, 4, 125

W

warrants
Attorney-General role, 85, 98, 101–102, 105, 120
cross-agency inquiry, 120
network activity warrants, 8, 119
weapons management and use, 108
website, ii, 12
whistleblower protection scheme *see* public interest disclosures
Women's Network, 32
Work Health and Safety Act 2011, 40
workforce planning, 33, 36 *see also* organisational capabilities; staff
workplace health and safety, 40

Y

year at a glance, 4

