



IGIS

OFFICE OF THE
INSPECTOR-GENERAL
OF INTELLIGENCE
AND SECURITY

ANNUAL REPORT

2023-24

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-and-pids

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 2024



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 2023–2024

I am pleased to present the Office of the Inspector-General of Intelligence and Security annual report for the period 1 July 2023 to 30 June 2024.

This report has been prepared for the purposes of section 46 of the *Public Governance, Performance and Accountability Act 2013* and section 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 section 10 of the *Public Governance, Performance and Accountability Rule 2014*, I certify that the Office of the Inspector-General of Intelligence and Security has a Fraud and Corruption Control Plan and Guidance 2024–2026 in place in line with the Commonwealth Fraud and Corruption Control Framework 2024 and will review the fraud and corruption risk assessment in the next reporting period. I further certify that appropriate fraud and corruption 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 and corruption relating to the agency.

Yours sincerely

The Hon Christopher Jessup KC
Inspector-General of Intelligence and Security
23 September 2024

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 2023-24	4
Section Two: Overview	5
About us	6
Purpose	7
Our key activities	8
Our approach	10
Organisation chart	11
Providing assurance	12
Section Three: Annual Performance Statement	15
2023-24 Annual Performance Statement	16
Reporting framework	17
Performance review 2023-24	18
Section Four: Management and accountability	29
Our staff and culture	30
Corporate governance	38
Stakeholders	42
Risk oversight and management	45
External scrutiny	47

Section Five: Financial statements	51
Financial Statements	52
Appendix A: Entity resource statements and resource for outcomes	77
Section Six: Review of intelligence agencies	79
Overview	80
The intelligence agencies	81
Office of National Intelligence	81
Australian Security Intelligence Organisation	84
Australian Secret Intelligence Service	95
Australian Signals Directorate	100
Australian Geospatial-Intelligence Organisation	106
Defence Intelligence Organisation	109
Australian Criminal Intelligence Commission and Australian Federal Police	112
Cross-agency activities	114
Complaints and public interest disclosures	118
Section Seven: Annexures	123
Annexure 7.1	124
Annexure 7.2	127
Index	136

About this report

This report provides information on the activities, achievements and performance of the Office of the Inspector-General of Intelligence and Security for the 2023–24 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*, section 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 2024–25.

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 2023–24.

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
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
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>
NACC	National Anti-Corruption Commission

Glossary

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 section 35 of the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act), this report provides details of my inquiry and inspection activities during the year; complaints and public interest disclosures received; and agency compliance with certain privacy rules.

This year, while anticipating and preparing for legislative change affecting the Inspector-General's functions and the agencies for which we have oversight responsibility, the IGIS has focused on the core activities of conducting inquiries, making regular inspections and receiving and addressing complaints and public interest disclosures.

Regular inspection work is a daily, fundamental activity for the IGIS. Oversight teams completed and issued findings for 77 inspections - fewer than planned because inspection activities had to be prioritised due to reduced staff numbers over the year. During the year under review, one preliminary inquiry was completed into the use of artificial intelligence (AI) by agencies within the national intelligence community. One inquiry not resulting from a disclosure or complaint that had commenced in 2022-23 was completed.

Our inspection teams have the benefit of a high degree of cooperation and support from agencies in our jurisdiction. Where noncompliance, either with the law or with appropriate standards of propriety, is encountered, 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. My staff inspect the implementation of findings to ensure identified compliance issues have been addressed and practices and policies are in place to reduce the likelihood of recurrence.

Receiving and managing complaints and disclosures about intelligence agencies is a key aspect of my oversight role. In 2023-24, the number of complaints received was 64. This is greater than the number of complaints in 2022-23 (34) and fewer than the number of complaints received in 2021-22 (80). I completed one inquiry into a complaint. I also allocated one public interest disclosure about an intelligence agency for investigation to my office. Consistent with section 49(1) of the *Public Interest Disclosure Act 2013*, I decided to investigate the disclosure under the IGIS Act and this is currently the subject of an ongoing inquiry under the IGIS Act.

Further particulars of this year's completed inquiries, inspections, and complaint and disclosure matters are set out in Section 6 of this report.

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*, the *Public Interest Disclosure Amendment (Review) Act 2023* and the *Inspector-General of Intelligence and Security and Other Legislation Amendment (Modernisation) Act 2023* - will expand the powers and role of the national intelligence community and increase my oversight responsibilities.

I was consulted on the proposed legislative changes, and my staff continue to engage in consultation regarding further proposed changes. 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 the structures supporting effective oversight are recognised and included in legislation.

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

Together with senior officers, I held at least biannual meetings with the leadership and senior executives of ASIO, ASIS, ASD, ONI, DIO and AGO and kept relevant ministers informed of findings in relation to the agencies in their respective portfolios.

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 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. Meetings were also held with integrity agency partners at the officer and executive levels on a number of different issues.

The IGIS continued its international engagement with other Five Eyes Intelligence Oversight and Review Council (FIORC) members throughout the year - for example, by attending its annual meeting held in September 2023 in Ottawa. The Inspector-General will host the 2024 FIORC meeting in Canberra and Sydney in November 2024. These meetings, and the ongoing international engagement that follows, provide an important opportunity to exchange views and compare best practice and areas of cooperation.

The IGIS continues to invest in continuous review and improvement. Significant progress has been made on implementing the recommendations from the IGIS Oversight Capability Review, in establishing its Technical Advisor function and in implementing the actions identified in our 2023 APS Census Action Plan. This year saw the development of a new enterprise agreement under the APS-wide bargaining arrangements. This agreement established new conditions and arrangements for IGIS staff and brought the IGIS into line with APS-wide standards where appropriate.

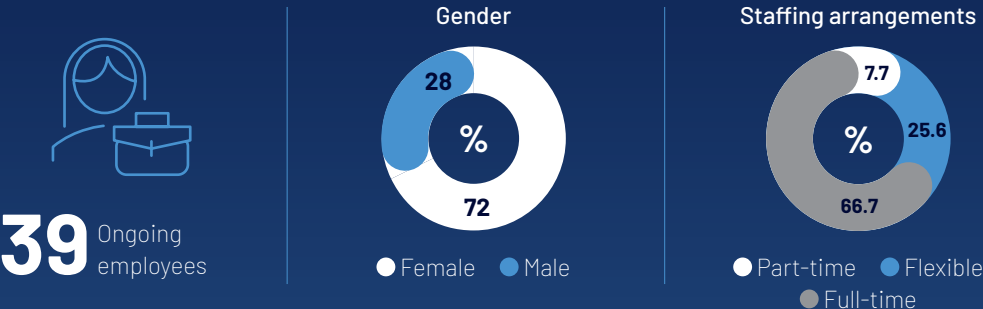
Our corporate governance framework continues to be strengthened with updating of the Fraud and Corruption Control Plan and Guidance. The work to develop and embed corporate and information governance systems and processes will continue into the next reporting period as the IGIS continues to grow.

As identified earlier, staffing levels across the Office continue to be a challenge. The planned expansion to IGIS's full complement of staff has not been achieved for several reasons, including the necessary but lengthy security clearance process and the extremely competitive external labour market. Like many public sector agencies, we continue to experience the challenges of recruiting and retaining subject matter experts across a range of skill sets. The IGIS continues to implement strategies to improve workforce retention. Over the coming year, we will continue to focus on strategic human resources initiatives to attract talent, retain high-quality staff and provide a rewarding and intellectually stimulating work environment.

I thank all staff of my office for their professionalism and dedication over the year. Our work 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 becomes more highly attuned to matters of intelligence integrity and oversight, particularly with the expansion and further development of the intelligence community.

Year at a glance 2023–24

Staffing profile as at 30 June 2024

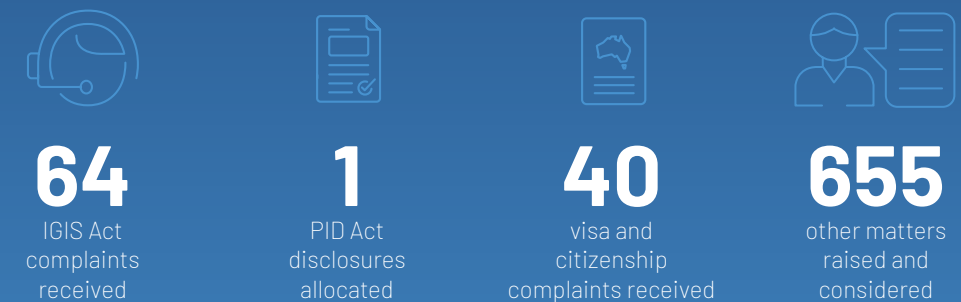


Oversight activities



*Correction to the Annual Report 2022–23 the inspections completed was 91

Complaints and public interest disclosures (PIDs)



Section Two

Overview

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 6 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 the Inspector-General 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 the 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 inspections of the intelligence agencies and we conduct in-depth inquiries. Inquiries can be undertaken in response to complaints, of the Inspector-General's own motion or at the request of a minister. When undertaking inquiries, the Inspector-General has investigative powers similar to those of a royal commission, including the power to compel persons to answer questions and produce documents and the power 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 ONI, ASIO, ASIS, ASD, AGO and DIO or the use of NAWs by the ACIC and the AFP. Complaints about the activities of an intelligence agency can be made by a member of the public or by a current or former employee of an intelligence agency. When the Inspector-General decides not to inquire into a complaint, the complainant is informed in writing. Details about individual complaints and their resolution are not made public by the Inspector-General, 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* to provide evidence on the damage that may be caused by the disclosure of certain material in disputed matters.

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.

This purpose is guided by the role of the Inspector-General of Intelligence and Security outlined in section 4 of the IGIS Act:

- 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; and
- 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 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 Inspector-General 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 the most formal activity we undertake to review the operations of intelligence agencies. An inquiry may be initiated by the Inspector-General by their own motion (which may in some cases be in response to a public interest disclosure (PID)), or at the request of the Attorney-General, the relevant responsible minister or the Prime Minister. The Inspector-General may initiate a preliminary inquiry into the action of an intelligence agency in connection with a complaint or 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 and people who have had dealings with the agencies. These contacts are mostly initiated through our website or through a telephone call. 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 IGIS officers 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 for the Inspector-General to handle the investigation.

Provide assurance to ministers, Parliament, and the public

An important part of the Inspector-General's role is to assist the Government in assuring the parliament and, to the extent possible, the public that there is effective oversight and scrutiny of intelligence agencies. Our regular program of inspections and inquiries into the activities and procedures of intelligence agencies, as well as the management of complaints and PIDs, contribute to providing this assurance.



A crucial element of assurance is communicating information about our role and the outcomes of our work to ministers, the parliament, and the public. We accomplish this through a series of complementary activities. These include submissions to parliamentary inquiries and other reviews of national security matters; and providing comments on matters relating to oversight and accountability in draft legislation. We deliver presentations and participate in engagements with the public and experts across the national security community, the legal profession, oversight bodies, and academia in Australia and internationally.

We make public as much information as possible, including through the production of an annual report that includes – with consideration for protective security requirements – details of inspection, inquiry, complaint and PID activities and findings for each agency. In 2023–24 the Inspector-General also published on its public website one preliminary inquiry report on the agencies' use and management of artificial intelligence. The Inspector-General and IGIS executive also regularly meet with each agency's senior officers and provide regular updates to the agencies' ministers on the key issues for each agency and the Inspector-General.

Our approach

We are united to achieve our mission by being:

Independent and impartial



Independence is fundamental to the Inspector-General's role and the role of officers assisting the Inspector-General. 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 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 proportion of the information 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.



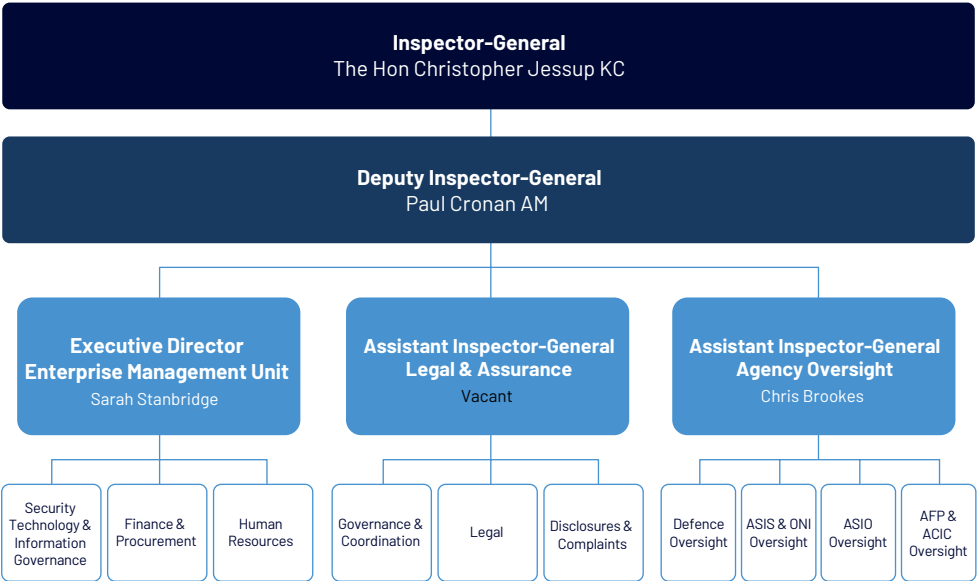
Influential



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.

Organisation chart

Figure 2.1: IGIS organisation structure at 30 June 2024



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 2023–24, no occasion arose for a report on inadequate action.

Under section 25A of the IGIS Act, the Inspector-General may report to the responsible minister on a completed inspection of an intelligence agency. In 2023–24, the Inspector-General provided one section 25A inspection report to a minister.

Under section 25B of the IGIS Act, the Inspector-General may report to the responsible minister on a completed preliminary inquiry into an intelligence agency. In 2023–24, the Inspector-General provided one section 25B preliminary inquiry report on the agencies’ use and management of artificial intelligence to multiple ministers. This preliminary inquiry is discussed further on page 114 – Section 6, Review of Intelligence Agencies.

Additionally, in the 2023–24 period, the Inspector-General wrote twice to each responsible minister to provide updates regarding inspections, disclosures and complaints, and legislative development activities relevant to the agency or agencies in their portfolio. In this same period, the Inspector-General wrote twice to the Attorney-General to provide a similar update on activities related to all agencies within our jurisdiction.

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

During 2023–24, the Inspector-General received no requests from the Prime Minister or ministers 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 their oversight and review role but do not comment on the policies underpinning the Bills.

Parliamentary Joint Committee on Intelligence and Security

During 2023–24, the Inspector-General and senior staff appeared before the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in public hearings into the review of:

- the Intelligence Services Legislation Amendment Bill 2023
- Division 3 of Part III of the *Australian Security Intelligence Organisation Act 1979* (Compulsory Questioning Powers).

Table 2.1: IGIS submissions to Parliamentary Joint Committee on Intelligence and Security 2023–24

IGIS submissions to PJCIS
Submission 7 to the Review of the Intelligence Services Legislation Amendment Bill 2023 by the Parliamentary Joint Committee on Intelligence and Security
Submission 6 to the Review of Administration and Expenditure No. 22 (2022–23) by the Parliamentary Joint Committee on Intelligence and Security
Submission 2 to the Review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023 by the Parliamentary Joint Committee on Intelligence and Security
Submission 3 to the Review of Division 3 of Part III of the <i>Australian Security Intelligence Organisation Act 1979</i> by the Parliamentary Joint Committee on Intelligence and Security

The Senate Select Committee on Adopting Artificial Intelligence

In May 2024, the IGIS provided a submission to the Senate Select Committee on Adopting Artificial Intelligence to inform the committee of its preliminary inquiry into the use and management of Artificial Intelligence by the National Intelligence Community (see the Cross Agency Activities section on page 114). In June 2024, as soon as the report was finalised, the IGIS provided a copy of its final report to the committee to inform its inquiry. The IGIS was not required to engage with the committee further as part of its inquiry.

Legal and Constitutional Affairs Legislation Committee

In 2023–24, the Office did not make any submissions to the Senate Legal and Constitutional Affairs Legislation Committee.

Evidence to the Administrative Appeals Tribunal and 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.

From 12 August 2023, the Australian Information Commissioner is not required to seek evidence from the Inspector-General unless the record or document in question relates directly or indirectly to the performance of functions or duties or to the exercise of the powers of an intelligence agency or to the performance of intelligence functions of a body as defined in the IGIS Act.

During 2023–24, the Inspector-General received 12 requests for evidence from the Australian Information Commissioner in relation to freedom of information exemptions.

Section Three

Annual Performance Statement



2023–24 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 the IGIS's annual performance statement for the financial year 2023–24, as required under paragraph 39(1)(a) of the PGPA Act and incorporating the additional requirements under section 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 IGIS's performance framework is set out in our Corporate Plan 2023–24 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 the public as to whether Australia's intelligence and security agencies act legally and with propriety by inspecting, inquiring into and reporting on their activities.

'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

Inspector-General of Intelligence and Security Act 1986 (IGIS Act)

Portfolio Budget Statements

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

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

Corporate Plan

IGIS purpose:

- 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 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.

Annual Performance Statement

Reports against the performance framework.

Performance review 2023–24

In 2023–24, the IGIS fully achieved 4 of its 5 objectives and identified room for improvement against the other one objective. We fully or substantially achieved all of the 7 performance measures identified in the Corporate Plan 2023–24. Underlying the IGIS’s assessed performance on each performance target are 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 IGIS is confident 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 it undertakes.

Objective 1: Inquiries		
<div></div> <div>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	Performance targets	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.	 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
	Implement the recommendations of the internal Oversight Capability Review relevant to inquiries.	 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	Performance targets	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 were 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

* IGIS Act section 16 has been replaced with section 32AB







Analysis

During 2023–24, the IGIS 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 assessed as achieved. The inquiry report finalised in 2023–24 was provided to the responsible minister or head of agency in 7 working days or under, following feedback on the draft report, and the report clearly articulated findings, promoting meaningful reviews of policy and procedures in the relevant agency. The draft inquiry report was also provided to the agency head in 7 working days or under. While not complete, the IGIS made significant progress against the implementation of the recommendations of the Oversight Capability Review and has implemented all recommendations relevant to the conduct of inquiries.

Measure 1.2 is assessed as achieved. Before the commencement of each inquiry initiated in 2023–24, 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 report from the inquiry completed in the reporting period was provided to the relevant agency head, the responsible minister and the Attorney-General.



Section 6 provides a detailed overview of the Inspector-General’s inquiries during the reporting period.

Objective 2: Inspections		
<div></div> <div>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.</div>		
Performance Measure	Performance targets	Result
2.1 Conduct inspections efficiently and effectively	Annual risk-based inspection plans are developed by July for each agency in jurisdiction and are updated throughout the year as additional issues are identified.	<div></div> <div>Achieved</div>
	All inspection activities in the inspection plan are commenced during the annual cycle.	<div></div> <div>Substantially Achieved</div>
	Preliminary investigations into proactively reported compliance incidents are completed in a timely manner.	<div></div> <div>Achieved</div>
	Inspection outcomes, including findings and recommendations, are clearly communicated to the agency and promote meaningful reviews of policy, process, procedure, training or technology.	<div></div> <div>Achieved</div>
	Implement the recommendations of the internal Oversight Capability Review relevant to inspections.	<div></div> <div>Achieved</div>
	Overall assessment	Achieved

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	Performance targets	Result
2.2 Conduct inspections consistent with the IGIS Act	Responsible ministers are provided with a biannual report outlining the key inspection activities each year.	 Achieved
	Annual inspection plans are reviewed in accordance with key priorities and risk before being provided to agency heads in July. [IGIS Act, s 9A(1)]	 Achieved
	Overall assessment	Achieved

Analysis

During 2023–24, the IGIS 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. ‘All inspection activities in the inspection plan are delivered during the annual cycle’ is assessed as substantially achieved. The IGIS undertook a deliberate process in January 2024 to review the progress of its inspection plans in light of resourcing constraints. At this point the IGIS decided to cancel approximately 10% of scheduled inspections for 2023–24. The IGIS ensured it prioritised the inspections it would continue to deliver to maximise assurance for parliament, ministers and the public. While implementation is not complete, significant progress has been made against the implementation of the recommendations of the Oversight Capability Review, and the IGIS has implemented all recommendations relevant to the conduct of inspections.






Measure 2.2 is assessed as achieved. Each agency head was provided with a risk-based annual inspection plan in July 2023, and responsible ministers were provided with biannual reports in September 2023 and June 2024.

Section 6 provides a detailed overview of the Inspector-General’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	Performance targets	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]	 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
	Procedures on the handling of complaints are regularly reviewed to ensure our processes are robust.	 Substantially Achieved
	Overall assessment	Achieved

Analysis

During 2023–24, the IGIS 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 IGIS received 64 complaints during the year that were within its jurisdiction. The IGIS also received 40 visa or citizenship complaints. In addition, the IGIS considered more than 655 additional matters to determine whether they fell within the Inspector-General's jurisdiction.

In 2023–24, 2 inquiries were commenced in response to complaints raised with the IGIS (one complaint received in this reporting period and one complaint received in a previous reporting period). The inquiries remain 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 where reasonably practicable to do so.







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

The IGIS continues to review and 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	Performance targets	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
	Procedures on the handling of PIDs are regularly reviewed to ensure our processes are robust.	 Substantially Achieved
	Overall assessment	Substantially achieved

* The PID Act was amended on 1 July 2023, with the effect that an authorised officer must decide to allocate a disclosure (s 43(3)(a)) or not to allocate a disclosure (s 43(3)(a) and s 43(4)).

The PID Act was amended on 1 July 2023, with the effect that an authorised officer must use best endeavours to make a decision about the allocation of a disclosure within 14 days after a requirement to make the decision arises (s 43(11)).

Analysis

During 2023–24, the IGIS substantially achieved its objective to receive and, where appropriate, investigate disclosures about suspected wrongdoing within an intelligence agency.

In the reporting period, the Inspector-General assessed 16 matters that resulted in a decision not to allocate a disclosure. Further information is provided in Section 6 of this report.

In the reporting period, the Office allocated 1 disclosure relating to an intelligence agency to itself for investigation under the PID Act. The disclosure was received in the previous reporting period. The Inspector-General then exercised their power under section 49(1) of the PID Act to choose not to investigate the matter as a PID, but to instead commence an inquiry under the IGIS Act. The discloser was notified of these decisions in a timely way. The IGIS received notification of 7 disclosures made to intelligence agencies, as required by the PID Act, but none of these were allocated to the IGIS.

Two disclosures allocated to the IGIS in the 2022–23 financial year were still under investigation as at 30 June 2024. The Inspector-General did not allocate any disclosures to the intelligence agencies for investigation in the reporting period. No disclosures were allocated to the Inspector-General by an intelligence agency.

The interplay between the IGIS Act and the PID Act is often complex, and the intricate and sensitive nature of many of the complaints made to the IGIS, 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 IGIS treats disclosure investigations, the volume of materials gathered and the logistical matters that can arise in obtaining classified information (including from disclosers), it can take an extended period for the IGIS to undertake an investigation. The IGIS makes every effort to provide disclosers with regular updates as to the progress of the relevant investigation, where applicable.

The IGIS will continue 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	Performance targets	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 matters relating to oversight and accountability in draft legislation.	 Achieved
	Produce a publicly available annual report that provides as much information as possible 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 across the national security community, the legal profession, oversight bodies, and academia in Australia and internationally.	 Achieved
	IGIS executives participate in at least biannual meetings with each agency's senior officers to understand agency priorities and share oversight of key issues and findings.	 Achieved
	Provide regular updates to the agencies' ministers on the key issues for each agency and the Office.	 Achieved
Overall assessment		Achieved

Analysis

During 2023–24, the IGIS achieved its objective to provide ministers, parliament and, to the extent possible, the public with assurance that the activities and procedures of intelligence agencies are open to scrutiny. In the reporting period, the IGIS provided multiple submissions to parliamentary inquiries, hearings and other reviews of national security matters as detailed on page 13 of Section 2.

The IGIS provided biannual letters to responsible ministers and had a number of meetings with ministers and senior advisors on topics relevant to the IGIS's role.

The IGIS *Annual report 2022–23* is publicly available on our 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 2023–24, senior IGIS officers delivered a number of presentations to the public or national security experts in Australia. On the international stage, the IGIS delivered presentations and led working groups in multilateral fora such as the FIORC and hosted short-term visits from bilateral partners.

In the reporting period, the IGIS 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 IGIS on a range of topics relevant to agency priorities. Both of these elements assist the IGIS to better target oversight activities based on a deeper understanding of the agencies' activities and operating environment.

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 the Australian Public Service (APS) Values, Employment Principles and Code of Conduct. This framework 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 IGIS.

Diversity and inclusion

The IGIS has a strong commitment to diversity and inclusion (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 IGIS Diversity and Inclusion Committee progresses initiatives 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 agency. The committee plays a key role in providing strategic advice on the IGIS inclusion and diversity strategy.

The committee works closely with the IGIS Social Club and with colleagues in the Attorney-General's Department (AGD), the National Intelligence Community and the wider APS, drawing on these larger networks to support, enable and add to our existing D&I efforts.

During 2023–24, the committee focused on finalising the IGIS Reconciliation Action Plan; embedding D&I into office culture and planning; and building the IGIS's understanding of D&I issues through events, resource packs and education. A key driver of the committee's activities in 2023–24 was the office-wide D&I Health Check the committee ran in early 2022. The D&I Health Check highlighted positives regarding the IGIS's culture but, more importantly, identified key areas for improvement. The committee has used this information to provide recommendations to the IGIS Executive Board to inform and prioritise organisational change and efforts. The committee has also 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 its initiatives are targeted to deliver maximum impact. This work will be ongoing into 2024–25.

Learning and development

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 IGIS People Capability Framework details the skills, behaviours and attributes expected of IGIS officers and informs a range of workforce planning and management activities, including learning and development, broadbanding and performance management. Internal training and professional development workshops for IGIS officers are supplemented by programs offered by the APS Academy, the National Intelligence Academy and a range of other providers. In addition, the IGIS'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 November 2023, the IGIS published on its website both its 2023 Australian Public Service Census results and its 2023 APS Census Action Plan. The plan was formulated in concert with feedback from staff gathered through the engagement of a specialist human resources consulting firm.

The plan identified 4 immediate or short-term actions, 2 medium-term actions and 1 long-term action.

Of the 4 short-term actions, 3 have been completed on schedule, with the IGIS establishing an innovation program, developing its Employee Value Proposition and formalising its Senior Executive Service (SES) leadership planning workshops. The fourth action – the establishment of an employee recognition program – is underway.

At this stage the medium- and long-term actions have not been completed; however, their current status and progress is consistent with the plan developed.

The IGIS will continue publishing its APS Census highlights report and Census Action Plan on the IGIS website annually.

Oversight Capability Review

In the second half of 2021-22, the IGIS allocated a senior member of staff to undertake an Oversight Capability Review to examine the practices, procedures and capabilities of the agency oversight area and provide practicable recommendations on how it could remain fit for purpose. The review recognised that the IGIS has been through a rapid period of expansion and that the nature of its work had evolved accordingly to be more risk based and proactive in nature. In addition, the intelligence community's size, capability and operational breadth have expanded and continue to evolve, providing 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 IGIS 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 IGIS'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 IGIS has consistent and timely access to enable its oversight activities
- enhance information sharing on oversight activities undertaken, and lessons learned, across the IGIS.

Implementation has progressed in 2023–24: 17 of the 23 recommendations are complete, with a further 6 underway. The IGIS's executive will maintain oversight of the review's implementation through regular reporting and oversight.

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 be established to provide technical expertise and assistance to the Inspector-General. In response to this recommendation, the IGIS established and filled a dedicated Technical Advisor position, on an initial 12-month basis, which was extended to 15 months. The role provided an interim Technical Advisor function to deliver advice and guidance to the IGIS's oversight activities and inform decision-making regarding the IGIS's approach to engaging with technical advice in the future, including how to best obtain technical advice independent from the agencies we oversee.

The interim Technical Advisor delivered significant value to the IGIS's work in 2023–24. This has included contributing to a number of inspections, inquiries and disclosures and complaints outlined in Section 6 of this annual report and to the development of the IGIS's 2023–24 inspection plans for each agency in our jurisdiction.

Following the valuable outcomes provided by the interim Technical Advisor, the IGIS undertook a recruitment activity to fill the position permanently. Unfortunately that recruitment activity was unsuccessful and the IGIS is currently taking action to engage a second interim Technical Advisor before undertaking another recruitment round in the first half of 2024–25.

Organisational profile



39

ongoing employees*



13%

on part-time arrangements



25%

on other flexible arrangements



97.5%

of staff are in Canberra#

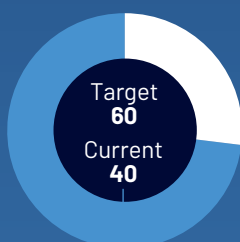
* Including 2.5% on long-term leave.

#This includes 1 employee who was working interstate on a temporary, non-ongoing basis.

No employees identified as indigenous.

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

Average staffing level (ASL)



The IGIS did not reach its target ASL of 60 in the reporting period due to a combination of:

- external labour market shortages
- challenges with the Top-Secret Positive Vetting clearance pipeline
- staff separations.

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

Recruitment environment

The IGIS 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. For the IGIS, these issues are made more challenging by the lengthy security clearance process.

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

Recruitment activities

This year, the IGIS 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 APS 4-6 and EL 1-2 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 IGIS has implemented creative recruitment strategies such as:

- a temporary employment register
- a section 26 transfer website portal
- secondments across the National Intelligence Community
- 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 2023-24)	At 30 June 2024				As at 30 June 2023			
	Male	Female	Uses a different term	Total	Male	Female	Uses a different term	Total
APS classification								
APS 4 (\$76,019-\$82,710)	0	1	0	1	0	0	0	0
APS 5 (\$84,624-\$91,796)	1	1	0	2	1	2	0	3
APS 6 (\$96,574-\$108,528)	2	7	0	9	2	7	0	9
Executive Level 1 (\$116,656-\$130,045)	4	8	0	12	7	10	0	17
Executive Level 2 (\$135,788-\$161,306)	2	11	0	13	2	7	0	9
SES Band 1 (\$205,761-\$235,926)	1	0	0	1	1	1	0	2
SES Band 2 (\$265,007-\$300,742)	1	0	0	1	0	1	0	1
Total	11	28	0	39	13	28	0	41

Note: 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 IGIS 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 14 March 2024, all non-SES officer salaries and conditions were made under the IGIS Enterprise Agreement 2024–2027. There are currently 3 SES Officer positions in the agency, 2 being filled as at June 2024. These officers are engaged in accordance with individual determinations under section 24(1) of the PS Act. Two of the SES positions are filled and recruitment activities were finalised in early 2024 for the third, with clearance processes underway.

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 \$1,317.

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 IGIS has 3 SES positions: one SES Band 2 position and 2 SES Band 1 positions. The IGIS also has one Executive Director (EL 2) position leading the Enterprise Management Unit. All of these positions are designated as key management personnel.

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

Executive remuneration

Table 4.2: Information about remuneration for key management personnel

Key management personnel							
Name and position title	Short-term employment benefits		Post-employment benefits		Other long-term benefits		Termination benefits
	Base salary ¹ (\$)	Other benefits and allowances ² (\$)	Superannuation contributions (\$)	Long service leave ³ (\$)	Other long-term benefits (\$)	Termination	Total remuneration ⁴ (\$)
The Hon Christopher Jessup KC Inspector-General (1 July 2023 to 30 June 2024)	467,300	106,704	27,399	-	-	-	601,403
Bronwyn Notzon-Glenn Deputy Inspector-General (1 July 2023 to 18 February 2024)	159,383	18,333	39,682	4,280	-	-	221,678
Paul Cronan Deputy Inspector-General (11 December 2023 to 30 June 2024)	145,493	16,391	24,838	3,528	-	-	190,249
Chris Brookes Assistant Inspector-General (1 July 2023 to 30 June 2024)	209,792	29,619	41,862	5,446	-	-	286,720
Katherine Cook Assistant Inspector-General (1 July 2023 to 8 September 2023)	42,648	5,783	7,975	1,100	-	-	57,507
Sarah Stanbridge Executive Director (1 July 2023 to 30 June 2024)	192,786	4,487	35,559	4,900	-	-	237,731

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-General's 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 IGIS does not have a performance pay scheme.

Workplace health and safety

The IGIS is committed to promoting and sustaining a safe and healthy workplace – one that values inclusion and ensures a healthy, resilient and capable workforce. The IGIS 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 2023–24, the IGIS continued to provide a range of health and wellbeing initiatives to staff, including:

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

No notifiable incidents resulting from undertakings carried out by the IGIS 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 IGIS and no notices were given to the IGIS 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 IGIS 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 IGIS is committed to good governance and the highest standards of accountability, transparency and integrity.

The IGIS's corporate governance framework guides good governance and sound business practices across the agency.

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, several committees support the Inspector-General and senior executives to fulfil their corporate and governance responsibilities. The committees provide a range of advice and support IGIS operations in key decision-making.

The Executive Board is the primary decision-making body of the IGIS. It is composed of the IGIS'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
- coordination of people and projects for the IGIS.

The Executive Board also provides an opportunity for members to discuss the ongoing oversight activities carried out by the IGIS. In doing so, the Executive Board supports the Inspector-General in discharging their responsibilities as the accountable authority under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

In addition to the Executive Board, several 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 IGIS 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 IGIS’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/2024-05/IGIS%20Audit%20Committee%20Charter%20-%202024.pdf>

The Inspector-General, the 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 4.3 IGIS Audit Committee membership

Audit Committee member	Qualifications, knowledge, skills and experience	Meetings attended	Total annual remuneration
Current members			
Ms Karla Bogaart Chair (External member)	<p>Ms Bogaart holds a Bachelor of Commerce majoring in Accounting and is a Fellow Member of the Institute of Chartered Accountants.</p> <p>Ms Bogaart has over 30 years’ experience in chartered accounting in the private sector.</p> <p>Ms Bogaart was previously Chair for the Audit Committee at CIT Solutions from 2020 to 2024.</p>	10 April 2024	\$20,000

Audit Committee member	Qualifications, knowledge, skills and experience	Meetings attended	Total annual remuneration
Ms Sarah Vandenbroek Former Chair (External member)	<p>Ms Vandenbroek holds a Bachelor of Information Management and a Graduate Diploma in Accounting and is a Fellow of CPA Australia. Ms Vandenbroek has held a range of senior roles in the Australian Public Service, including as a Chief Financial Officer and a Chief Operating Officer. Ms Vandenbroek is the First Assistant Secretary of the Territories Division in the Department of Infrastructure, Transport, Regional Development, Communications and the Arts.</p>	3 August 2023 16 November 2023 29 February 2024	Nil
Mr Stephen Moore (External member)	<p>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.</p> <p>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.</p>	3 August 2023 16 November 2023 29 February 2024 10 April 2024	\$3,630

Audit Committee member	Qualifications, knowledge, skills and experience	Meetings attended	Total annual remuneration
Mr Peter Quiggin KC (External member)	Mr Quiggin holds a Bachelor of Laws, a Graduate Diploma in Professional Accounting and 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.	3 August 2023 16 November 2023 29 February 2024 10 April 2024	\$18,750

Internal audit

Internal audit provides independent and objective assurance and advice to the Inspector-General – through the Audit Committee – that the IGIS'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. The IGIS engaged with AGD in a joint procurement process to contract an external provider of internal audit services to conduct an internal audit program. In the reporting year, the IGIS completed 2 internal audit activities: on-call arrangement review and asset management.

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 IGIS 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 information and communications technology (ICT) systems and capabilities. IGIS officers also participate in a number of portfolio-wide working groups chaired by the department.

Corporate support

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

Accountability and integrity agencies

The IGIS 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 meetings of the Integrity Agencies Group, whose members include the heads of integrity agencies and other relevant Commonwealth agencies. The purpose of the Integrity Agencies Group is to lead coordination and enhancement of institutional integrity across the Commonwealth.

National Anti-Corruption Commission

Since the establishment of the National Anti-Corruption Commission (NACC) the IGIS has continued to engage with the NACC to ensure that the IGIS can enable effective engagement between the NACC and the intelligence agencies where it is necessary to address concerns about serious and systemic corruption. The IGIS has partnered with the NACC to deliver briefings at the National Security College to national security and intelligence professionals on oversight and anti-corruption.

Australian Human Rights Commission

The Australian Human Rights Commission is required by section 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 the intelligence agencies. During 2023–24, the Australian Human Rights Commission did not refer any such matters to the Inspector-General.

Office of the Australian Information Commissioner

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

Office of the Commonwealth Ombudsman

IGIS officers continued to engage and meet regularly with staff from the Office of the Commonwealth Ombudsman on a wide range of issues, including current and potential future jurisdiction and areas of related oversight. The responsibilities of the 2 offices are considered complementary and a memorandum of understanding exists between them.

International engagement

The IGIS engages with international accountability and integrity agencies to discuss emerging issues and new developments in other jurisdictions.

Five Eyes Intelligence Oversight and Review Council

In 2023–24, the Inspector-General and IGIS officers deepened engagement with the FIORC. The FIORC comprises the following intelligence oversight, review and security entities of the Five Eyes countries:

- the Inspector-General of Intelligence and Security of Australia
- the Office of the Intelligence Commissioner of Canada
- the National Security and Intelligence Review Agency (NSIRA) of Canada
- the Commissioner of Intelligence Warrants of New Zealand
- 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 FIORC 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 FIORC aims to meet in person at least once each year. In September 2023, members met in Ottawa, Canada. Topics discussed included:

- setting the foundation for effective oversight
- ministerial and executive-level control
- review topic triaging and protective oversight risk assessment
- data protection and civil liberties boards
- cooperation with legislative oversight committees
- communication with courts and judicial commissioners
- learning from non-National Security accountability bodies
- reporting
- recommendations
- strengthening accountability for the future.

Council members continue to meet quarterly via teleconference and progress opportunities for collaboration and knowledge sharing through working groups. The next annual conference is planned to be held in Australia in November 2024.

Bilateral engagement

During the reporting period, IGIS officers engaged bilaterally with international counterparts in a variety of ways and on a range of issues affecting the IGIS. The IGIS hosted a member of Canada's NSIRA for a short-term visit in August 2023, and a small working-level delegation from the IGIS undertook a short-term visit to NSIRA in Ottawa in April 2024. These visits were valuable in building institutional links between the IGIS and NSIRA and identifying similarities, differences and opportunities in Australia's and Canada's operating environments and oversight approach. Key areas for cooperation and collaboration included:

- technical advice to oversight activities
- inspection, inquiry and disclosures and complaints methodologies
- reporting
- the sharing of experiences and lessons learned on recruitment and retention initiatives
- opportunities for longer term visits and joint work for working-level officers.

Risk oversight and management

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

The IGIS 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 IGIS needs to have in place to reduce them to an acceptable level are vitally important in developing fraud and corruption control measures, business continuity arrangements and strategic plans for the IGIS.

The IGIS’s risk oversight and management tools include its Risk Management Framework, risk appetite and risk tolerance statements, Risk Register, Audit Committee reviews, Fraud and 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, including related controls and mitigation strategies. The Governance Directorate coordinates biannual reviews with risk owners which are considered by the Executive Board. The Audit Committee provides advice to the Inspector-General about the IGIS’s risk framework, governance, compliance and financial accountability. The Audit Committee will be informed by an internal audit plan tailored to the size and functions of a small agency. The audit plan will be supplied through externally contracted arrangements.

The IGIS monitors and reviews risk against the following categories.



The IGIS 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 an expanding workforce, evolving jurisdiction and changes in the national security environment. The IGIS will manage these risks through strong planning, building effective stakeholder relationships, strengthening the control framework, and reviewing and updating the Risk Register.

Ethical standards

During 2023–24, the IGIS continued its commitment to high ethical standards. High ethical standards across the IGIS are maintained through:

- APS integrity and values training
- mandatory online fraud and corruption training
- modelling of appropriate behaviors by 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 IGIS performance agreement process.

The IGIS 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 IGIS’s fraud control strategies comply with the Commonwealth Fraud Control Framework 2024 and the legislative requirements as defined in the PGPA Act.

The IGIS Fraud and Corruption Control Plan and Guidance 2024–26 provides the foundations of the IGIS’s fraud control framework.

The Fraud and Corruption Control Plan and Guidance outlines the IGIS’s approach to managing fraud and corruption risks and ensures that the 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 IGIS are examined promptly, confidentially and diligently and, where necessary, they are referred for investigation by an appropriate authority.

The IGIS had no reports of fraud in 2023–24.

External scrutiny

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

The ANAO completed an audit of the IGIS's financial statements for 2023–24. The independent auditor's report is presented in the financial statements section of this annual report.

The Inspector-General and IGIS officers appeared before the Senate Legal and Constitutional Affairs Legislation Committee at its estimates hearings in February 2024 and May 2024. The IGIS also attended public and private hearings of the PJCIS and provided submissions on a range of inquiries. Where security classifications permit, the IGIS'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 IGIS worked collaboratively with the ANAO and the Commonwealth Ombudsman.

Asset management

The management of IGIS assets is governed by internal policies and procedures on asset management that are based on government best practice. The IGIS 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 IGIS's fixed assets include office plant and equipment, purchased software and leasehold improvements.

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 section 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 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 the IGIS's website in the reporting period in accordance with the Senate Continuing Order for Indexed File Lists (Harradine Order).

Purchasing and procurement

Purchasing

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

The IGIS's purchasing framework seeks to ensure:

- procurement methods are efficient and cost-effective and take account of the IGIS'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 (SME) 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 IGIS is committed to the continued development and support of Indigenous businesses, under the Commonwealth Indigenous Procurement Policy.

The IGIS supports small business participation in the Commonwealth Government procurement market. 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 IGIS's decision-making. When deciding to engage a consultant, the IGIS requires decision-makers to consider the skills 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 2023–24 are shown in the following tables.

Table 4.4: Reportable consultancy contracts 2023–24

Reportable consultancy contracts 2023–24	Number	Expenditure (\$, GST inc.)
New contracts entered into during the reporting period	7	135,881.77
Ongoing contracts entered into during a previous reporting period	3	139,643.00
Total	10	275,524.77

Table 4.5: Reportable consultancy contract expenditure 2023–24

Name of organisation	Expenditure (\$, GST inc.)
Yardstick Advisory Pty Ltd (ABN 38 158 309 150)	125,037.00
1 and One Pty Ltd (ABN 13 637 567 947)	65,560.00
Tailored HR Solutions (ABN 55 625 831 706)	30,749.77
Humanify HR Consulting Pty Ltd (ABN 80 651 424 869)	29,106.00
PQOC Consulting (ABN 94 484 818 597)	15,000.00
Work Science Pty Ltd (ABN 49 118 332 880)	4,620.00
Optimum Business Consulting Pty Ltd (ABN 48 091 681 462)	4,000.00
The ITSM Hub Pty Ltd (ABN 89 165 912 087)	1,452.00

During 2023–24, 7 new reportable consultancy contracts were entered into involving total actual expenditure of \$135,881.77. In addition, 3 ongoing reportable consultancy contracts were active during the period, involving total actual expenditure of \$139,643.00.

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 2023–24 are shown in the following tables.

Table 4.6: Reportable non-consultancy contracts 2023–24

Contract types	Number	Expenditure (\$, GST inc.)
New contracts entered into during the reporting period	9	235,473.52
Ongoing contracts entered into during a previous reporting period	1	266,545.22
Total	10	502,018.74

Table 4.7: Reportable non-consultancy contract expenditure 2023–24

Name of organisation	Expenditure (\$, GST inc.)
Remote Pty Ltd (ABN 21 086 319 146)	266,545.22
Compas Pty Ltd (ABN 90 008 615 745)	87,243.75
OPC IT Pty Ltd (ABN 29 008 657 618)	30,000.00
Face 2 Face Recruitment Pty Ltd (ABN 47 112 122 504)	28,799.77
Gillian Beaumont Recruitment Pty Ltd (ABN 58 107 780 683)	27,500.00
Horizon One Recruitment Pty Ltd (ABN 98 129 885 838)	11,440.00
Agora Consulting Pty Ltd (ABN 28 604 109 604)	50,490.00

Australian National Audit Office access clauses

The IGIS'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

The IGIS publishes information on the value of contracts and consultancies on the AusTender website, but it 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 2023–24, the IGIS exempted from publication 2 contracts with the total value of \$302,316.

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 2024:

- (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 2024 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 2024 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 material accounting policy information 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 their 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

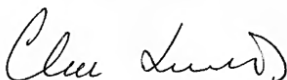
My objective is to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes my opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that 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

9 August 2024

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
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


Office of the Inspector-General of Intelligence and Security

STATEMENT BY THE ACCOUNTABLE AUTHORITY AND CHIEF FINANCIAL OFFICER

In our opinion, the attached financial statements for the year ended 30 June 2024 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
9 August 2024

Signed.....

Ms Gerlinde Nicolson
Chief Financial Officer
9 August 2024

Statement of Comprehensive Income

for the period ended 30 June 2024

		2024	2023	Original
	Notes	\$	\$	Budget
				\$
NET COST OF SERVICES				
Expenses				
Employee benefits	1.1A	7,732,668	7,118,860	9,227,000
Suppliers	1.1B	3,663,159	2,984,748	4,436,000
Depreciation and amortisation	2.2A	1,642,618	920,252	714,000
Finance costs		-	6	-
Write-down and impairment of assets	2.2A	21,641	34,720	-
Total expenses		13,060,086	11,058,586	14,377,000
Own-source revenue				
Revenue from contracts with customers	1.2A	33,842	33,665	-
Other revenue	1.2B	50,000	40,000	67,000
Total own-source revenue		83,842	73,665	67,000
Net (cost of) services		(12,976,244)	(10,984,921)	(14,310,000)
Revenue from Government	1.2C	13,417,000	12,561,000	13,596,000
Surplus/(Deficit) attributable to the Australian Government		440,756	1,576,079	(714,000)
OTHER COMPREHENSIVE INCOME				
Items not subject to subsequent reclassification to net cost of services				
Changes in asset revaluation reserve		-	229,135	-
Total comprehensive income/(loss)		440,756	1,805,214	(714,000)

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

Budget Variances Commentary

Statement of Comprehensive Income

Employee benefits

Employee expenses were \$1.49m (16%) lower than the original budget. OIGIS achieved an actual ASL of 40 for the year against a funded ASL of 60. 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 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.

Suppliers

Suppliers are \$0.77m (17%) lower than the original budget. With lower than anticipated ASL less expenditure was incurred for travel and training.

Depreciation and amortisation

Depreciation and amortisation expenses were \$0.93m higher than the original budget. This is a result of the change in useful life for Leasehold Improvements from the asset revaluation undertaken in 2022-23.

Statement of Financial Position

as at 30 June 2024

		2024	2023	Original Budget
	Notes	\$	\$	\$
ASSETS				
Financial assets				
Cash and cash equivalents	2.1A	805,045	521,658	522,000
Trade and other receivables	2.1B	31,089,788	31,829,176	29,926,000
Total financial assets		31,894,833	32,350,834	30,448,000
Non-financial assets				
Leasehold improvements	2.2A	11,429	1,342,000	-
Property, plant and equipment	2.2A	673,896	929,342	1,478,000
Intangibles	2.2A	265	56,609	228,000
Prepayments		247,701	238,212	170,000
Total non-financial assets		933,291	2,566,163	1,876,000
Total assets		32,828,124	34,916,997	32,324,000
LIABILITIES				
Payables				
Suppliers	2.3A	270,041	300,008	524,000
Other payables	2.3B	478,699	449,525	-
Total payables		748,740	749,533	524,000
Provisions				
Employee provisions	4.1A	1,615,440	1,722,283	2,396,000
Total provisions		1,615,440	1,722,283	2,396,000
Total liabilities		2,364,180	2,471,816	2,920,000
Net assets		30,463,944	32,445,181	29,404,000
EQUITY				
Contributed equity		8,325,196	10,747,189	9,031,000
Reserves		243,400	243,400	15,000
Retained surplus/(Accumulated deficit)		21,895,348	21,454,592	20,358,000
Total equity		30,463,944	32,445,181	29,404,000

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 \$1.16m (4%) higher than the original budget. Unspent appropriations have materialised due to the surplus generated in 2023-24 as outlined in the Statement of Comprehensive Income budget variances commentary.

Non-financial assets

Aggregate non-financial assets recognised are \$0.94m (50%) lower than the original budget. Prior and current year capital acquisitions did not materialise to the extent of that budgeted partly due to lower than anticipated staffing levels.

Employee provisions

Employee provisions are \$0.78m (33%) lower than the original budget. This is reflective of the increase in the 10 year Government Bond rate and the difference in the provision for a funded ASL of 60 compared to an actual ASL of 40 at 30 June 2024.

Statement of Changes in Equity

for the period ended 30 June 2024

		2024	2023	Original Budget
	Notes	\$	\$	\$
CONTRIBUTED EQUITY				
Opening balance		10,747,189	10,554,949	10,747,000
Transactions with owners				
Distributions to owners				
Returns of capital	3.1B	(2,705,993)	(3,565,760)	(2,000,000)
Contributions by owners				
Departmental capital budget		284,000	3,758,000	284,000
Closing balance as at 30 June		8,325,196	10,747,189	9,031,000
RETAINED EARNINGS				
Opening balance		21,454,592	19,878,513	21,072,000
Comprehensive income				
Surplus/(Deficit) for the period		440,756	1,576,079	(714,000)
Closing balance as at 30 June		21,895,348	21,454,592	20,358,000
ASSET REVALUATION RESERVE				
Opening balance		243,400	14,265	15,000
Comprehensive income				
Other comprehensive income		-	229,135	-
Closing balance as at 30 June		243,400	243,400	15,000
TOTAL EQUITY				
Opening balance		32,445,181	30,447,726	31,834,000
Surplus/(Deficit) for the period		440,756	1,576,079	(714,000)
Other comprehensive income		-	229,135	-
Transactions with owners		(2,421,993)	192,240	(1,716,000)
Closing balance as at 30 June		30,463,944	32,445,181	29,404,000

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

Returns of capital

Unspent prior year appropriations totalling \$2,705,993 were quarantined under three year sunset clauses and returned to the Official Public Account on 1 July 2023 and 1 July 2024.

Comprehensive Income and Other Comprehensive Income

Variance is reflective of the surplus generated in 2023-24 as outlined in the Statement of Comprehensive Income.

Cash Flow Statement

for the period ended 30 June 2024

		2024	2023	Original Budget
	Notes	\$	\$	\$
OPERATING ACTIVITIES				
Cash received				
Appropriations		12,175,777	11,137,875	15,047,000
Net GST received		191,196	133,388	100,000
Other		477,418	33,665	27,000
Total cash received		12,844,391	11,304,928	15,174,000
Cash used				
Employees		8,279,585	7,398,458	8,678,000
Suppliers		3,837,843	3,356,586	4,496,000
Interest payments on lease liabilities		-	6	-
Section 74 receipts transferred to OPA		443,576	547,561	-
Total cash used		12,561,004	11,302,610	13,174,000
Net cash from operating activities		283,387	2,317	2,000,000
INVESTING ACTIVITIES				
Cash used				
Purchase of property, plant and equipment		21,898	129,668	284,000
Total cash used		21,898	129,668	284,000
Net cash (used by) investing activities		(21,898)	(129,668)	(284,000)
FINANCING ACTIVITIES				
Cash received				
Contributed equity		21,898	129,668	284,000
Total cash received		21,898	129,668	284,000
Cash used				
Principal payments of lease liabilities		-	2,523	-
Return of contributed equity		-	-	2,000,000
Total cash used		-	2,523	2,000,000
Net cash from/(used by) financing activities		21,898	127,145	(1,716,000)
Net increase/(decrease) in cash held		283,387	(206)	-
Cash and cash equivalents at the beginning of the reporting period		521,658	521,864	522,000
Cash and cash equivalents at the end of the reporting period	2.1A	805,045	521,658	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

All new, revised, amending standards and/or interpretations that were issued prior to the sign-off date and are applicable to the current reporting period did not have a material effect on OIGIS's financial statements.

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 2024

1.1 Expenses

	2024	2023
	\$	\$
1.1A: Employee benefits		
Wages and salaries	5,162,222	5,317,874
Superannuation		
Defined contribution plans	548,431	595,420
Defined benefit plans	889,172	367,828
Leave and other entitlements	1,132,843	723,261
Separation and redundancies	-	114,477
Total employee benefits	7,732,668	7,118,860

Accounting Policy

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

	2024	2023
	\$	\$
1.1B: Suppliers		
Goods and services supplied or rendered		
Audit Fees	50,000	35,000
Consultants	347,884	383,783
Contractors	321,627	472,215
ICT and communication	1,023,314	576,539
Insurance	24,387	19,069
Legal	30,312	56,889
Property	671,724	634,433
Recruitment and HR	216,525	89,001
Security vetting	464,535	92,255
Training	149,379	301,690
Travel	229,396	225,085
Other	126,902	87,646
Total goods and services supplied or rendered	3,655,985	2,973,605
Other suppliers		
Workers compensation expenses	7,174	11,143
Total other suppliers	7,174	11,143
Total suppliers	3,663,159	2,984,748

1.2 Own-Source Revenue and Gains

	2024	2023
	\$	\$

Own-Source Revenue

1.2A: Revenue from contracts with customers

Rendering of services	33,842	33,665
Total revenue from contracts with customers	33,842	33,665

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.

	2024	2023
	\$	\$

1.2B: Other revenue

Resources received free of charge		
Remuneration of auditors	50,000	35,000
Australian Signals Directorate	-	5,000
Total other revenue	50,000	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.

	2024	2023
	\$	\$

1.2C: Revenue from Government

Appropriations		
Departmental appropriations	13,417,000	12,561,000
Total revenue from Government	13,417,000	12,561,000

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

	2024	2023
	\$	\$
2.1A: Cash and cash equivalents		
Cash on hand or on deposit	805,045	521,658
Total cash and cash equivalents	805,045	521,658

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.

	2024	2023
	\$	\$
2.1B: Trade and other receivables		
Appropriation receivables		
Appropriation receivable	31,011,136	31,770,229
Total appropriation receivables	31,011,136	31,770,229
Other receivables		
GST receivable from the Australian Taxation Office	15,481	36,773
Inter-agency staff leave transfers	61,647	22,174
Other	1,524	-
Total other receivables	78,652	58,947
Total trade and other receivables	31,089,788	31,829,176

Credit terms for goods and services were within 30 days (2023: 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 2024 (2023: 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 2023					
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 1 July 2023	1,342,000	929,342	-	56,609	2,327,951
Additions					
Purchase or internally developed	-	21,898	-	-	21,898
Write-downs recognised in net cost of services	-	(21,641)	-	-	(21,641)
Depreciation and amortisation	(1,330,571)	(255,703)	-	(56,344)	(1,642,618)
Total as at 30 June 2024	11,429	673,896	-	265	685,590
Total as at 30 June 2024 represented by					
Gross book value	1,342,000	924,682	21,837	937,893	3,226,412
Accumulated depreciation, amortisation and impairment	(1,330,571)	(250,786)	(21,837)	(937,628)	(2,540,822)
Total as at 30 June 2024	11,429	673,896	-	265	685,590

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. The carrying amounts in 2023-24 do not differ materially from those which would be determined using fair value at the end of the reporting period.

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. Comprehensive valuations are carried out at least once every 3 years.

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 last 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:

	2024	2023
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 2024. 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 (2023: 3 years).

All software assets were assessed for indications of impairment as at 30 June 2024.

2.3 Payables

	2024	2023
	\$	\$

2.3A: Suppliers

Trade creditors and accruals	270,041	300,008
Total suppliers	270,041	300,008

Average days of settlement are 20 days (2023: 20 days).

	2024	2023
	\$	\$

2.3B: Other payables

Salaries and wages	221,608	244,258
Superannuation	34,697	38,549
Leave balance transfers	212,583	143,106
Other	9,811	23,612
Total other payables	478,699	449,525

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

Funding

This section identifies OIGIS funding structure.

3.1 Appropriations

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

Annual Appropriations for 2024

	Annual Appropriation ¹ \$	Adjustments to appropriation ² \$	Total appropriation \$	Appropriation applied in 2024 (current and prior years) \$	Variance ³ \$
Departmental					
Ordinary annual services	13,596,000	477,418	14,073,418	(11,926,232)	2,147,186
Capital Budget ⁴	284,000	-	284,000	(21,898)	262,102
Total departmental	13,880,000	477,418	14,357,418	(11,948,130)	2,409,288

1. As at 30 June 2024, \$179,000 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. 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 \$284,000.

Annual Appropriations for 2023

	Annual Appropriation \$	Adjustments to appropriation ¹ \$	Total appropriation \$	Appropriation applied in 2023 \$	Variance ² \$
Departmental					
Ordinary annual services	12,592,000	547,561	13,139,561	(11,138,080)	2,001,480
Capital Budget ³	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. 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. 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.

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 \$3,758,000.

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

	2024	2023
	\$	\$
Departmental		
Appropriation Act (No. 1) 2020-21 - Supply Act ¹	-	974,330
Appropriation Act (No. 1) 2020-21 - DCB ¹	-	287,332
Appropriation Act (No. 1) 2020-21 - DCB - Supply Act ¹	-	584,000
Appropriation Act (No. 1) 2021-22 ²	608,229	12,784,006
Appropriation Act (No. 1) 2021-22 - DCB ²	252,102	274,000
Appropriation Act (No. 3) 2022-23 - Supply Act ³	7,345,000	7,345,000
Appropriation Act (No. 1) 2022-23 - Supply Act	5,794,561	5,794,561
Appropriation Act (No. 3) 2022-23 - DCB - Supply Act	2,192,000	2,192,000
Appropriation Act (No. 1) 2022-23 - DCB - Supply Act	1,566,000	1,566,000
Appropriation Act (No. 1) 2023-24 ⁴	14,039,576	-
Appropriation Act (No. 1) 2023-24 - DCB	284,000	-
Cash and cash equivalents	805,045	521,658
Total departmental	32,886,513	32,322,887

1. Appropriation lapsed on 1 July 2023.

2. Appropriation will lapse on 1 July 2024.

3. As at 30 June 2024, \$31,000 of the Appropriation Act (No. 3) 2022-23 - Supply Act was withheld under section 51 of the PGPA Act.

4. As at 30 June 2024, \$179,000 of the Appropriation Act (No. 1) 2023-24 was withheld under section 51 of the PGPA Act.

3.2 Net Cash Appropriation Arrangements

	2024	2023
	\$	\$
Total comprehensive income - as per the Statement of Comprehensive Income	440,756	1,805,214
<i>Plus</i> : depreciation/amortisation of assets funded through appropriations (departmental capital budget funding and/or equity injections) ¹	1,642,618	917,764
<i>Plus</i> : depreciation of right-of-use assets ²	-	2,488
<i>Less</i> : lease principal repayments ²	-	(2,523)
Net Cash Operating Surplus	2,083,374	2,722,943

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

	2024	2023
	\$	\$
4.1A: Employee provisions		
Leave	1,615,440	1,722,283
Total employee provisions	1,615,440	1,722,283

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 2024. 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 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:

	2024	2023
	\$	\$
Short-term employee benefits	1,398,720	1,522,518
Post-employment benefits	177,315	193,666
Other long-term employee benefits	19,254	21,924
Total key management personnel remuneration expenses¹	1,595,289	1,738,108

The total number of key management personnel that are included in the above table are 6 (2023: 6). Substantively, 5 key management personnel positions remain in place during 2024, 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 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 (2023: 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 2024 there were no contingent assets or liabilities (2023: nil).

Unquantifiable Contingencies

As at 30 June 2024 there were no unquantifiable contingent assets or liabilities (2023: 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

	2024	2023
	\$	\$
5.2A: Categories of financial instruments		
Financial Assets		
Financial assets at amortised cost		
Cash and cash equivalents	805,045	521,658
Total financial assets at amortised cost	805,045	521,658
Total financial assets	805,045	521,658
Financial Liabilities		
Financial liabilities measured at amortised cost		
Suppliers	270,041	300,008
Total financial liabilities measured at amortised cost	270,041	300,008
Total financial liabilities	270,041	300,008

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	
	2024 \$	2023 \$
Non-financial assets		
Leasehold improvements	11,429	1,342,000
Property, plant and equipment	673,896	929,342
Total non-financial assets	685,325	2,271,342

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. No revaluation occurred in 2023-24. 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 practice 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

	2024	2023
	\$	\$
Assets expected to be recovered in:		
No more than 12 months		
Cash and cash equivalents	805,045	521,658
Trade and other receivables	31,089,788	31,829,176
Prepayments	247,701	238,212
Total no more than 12 months	32,142,534	32,589,046
More than 12 months		
Leasehold improvements	11,429	1,342,000
Property, plant and equipment	673,896	929,342
Intangibles	265	56,609
Total more than 12 months	685,590	2,327,951
Total assets	32,828,124	34,916,997
Liabilities expected to be settled in:		
No more than 12 months		
Suppliers	270,041	300,008
Other payables	478,699	449,525
Employee provisions	757,160	758,751
Total no more than 12 months	1,505,900	1,508,284
More than 12 months		
Employee provisions	858,280	963,532
Total more than 12 months	858,280	963,532
Total liabilities	2,364,180	2,471,816

Appendix A: Entity resource statements and resource for outcomes

Figure 5.1: Entity Resource Statement and Resource for Outcomes 2023–24

	Actual available appropriation for 2023–24 \$'000 (a)	Payments made 2023–24 \$'000 (b)	Balance remaining 2023–24 \$'000 (a) – (b)
Departmental			
Annual appropriations – prior year departmental	30,478	11,948	18,530
Annual appropriations – ordinary annual services	13,880	–	13,880
Annual appropriations – s 74 relevant agency receipts	477	–	477
Annual appropriations – other services – non-operating	–	–	–
Total departmental annual appropriations	44,835	11,948	32,887
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)	44,835	11,948	32,887
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)	44,835	11,948	32,887

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 2023-24 \$'000 (a)	Actual expenses 2023-24 \$'000 (b)	Variation 2023-24 \$'000 (a) - (b)
Program 1.1: Office of the Inspector-General of Intelligence and Security			
Departmental expenses			
Departmental appropriation ¹	13,596	11,368	2,228
Special appropriations	-	-	-
Special accounts	-	-	-
Expenses not requiring appropriation in the Budget year ²	781	1,692	(911)
Total expenses for Program 1.1	14,377	13,060	1,317
Outcome 1 totals by appropriation type			
Departmental expenses			
Departmental appropriation ¹	13,596	11,368	2,228
Special appropriations	-	-	-
Special accounts	-	-	-
Expenses not requiring appropriation in the Budget year ²	781	1,692	(911)
Total expenses for Outcome 1	14,377	13,060	1,317
	Budget 2023-24	Actual 2023-24	Variation 2023-24
Average Staffing Level (number)	60	40	20

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

Overview


The IGIS continues to identify a generally strong culture of compliance within the agencies. Where inspections identify any concerns, they are only occasionally systemic in nature. The level of cooperation from agencies that the IGIS receives is generally very good, as is the access to facilities, systems, information and people.

The IGIS has continued its focus on ensuring sound 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. Sound record keeping in operational decision-making 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 enables the IGIS to confirm what has been done and to understand the reasons why a particular action was taken, or not taken. The IGIS will continue this focus in the next reporting year.

The intelligence agencies


Office of National Intelligence

Key statistics




3

Inspections commenced




4

Inspections completed




0

Compliance incidents reported




2

Ministerial letters sent to relevant minister




2

Senior-level meetings held



0

Inquiries commenced



0

Inquiries completed

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 the National Security Committee of Cabinet. ONI produces all source assessments on matters relating to political, strategic or economic significance to Australia. 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*

Responsible minister: Prime Minister

Office of National Intelligence

In 2023–24, the IGIS undertook inspections of ONI's activities pursuant to section 9A of the IGIS Act. The IGIS did not commence any inquiries under section 8 of the IGIS Act in relation to ONI.

The IGIS conducted one preliminary inquiry relating to ONI, which is reported on in 'Cross-agency activities' later in this section.

The IGIS implemented a risk-based approach to its inspections of ONI. Due to the nature of ONI's role, the IGIS undertook fewer oversight activities in relation to its activities compared to the activities of other intelligence agencies.

Two scheduled meetings were held between the Inspector-General, the IGIS's executives team and ONI senior executives in November 2023 and May 2024. These meetings were a valuable opportunity to discuss organisational priorities and challenges, along with oversight and inspection activities.

Access to systems, personnel and information

In 2023–24, ONI provided the IGIS with appropriate facility access and direct access to ONI systems to support our oversight activities. The IGIS experienced some delays in access to systems, information and personnel to finalise inspections in a timely manner, due to limited resource availability in the relevant ONI work area. However, this improved in the second half of 2023–24.

Inspections

The IGIS undertook 3 inspections of ONI activities in 2023–24. Of these, one inspection remains underway and will be reported on in 2024–25.

The IGIS completed 2 inspections that commenced in 2022–23.

The IGIS identified propriety-related issues in the 4 completed inspections. No issues of legality were identified. A high-level summary of the findings and recommendations for each of these appears below.

Rules to Protect the Privacy of Australians

The Prime Minister issues written rules – *Rules to Protect the Privacy of Australians* (the Privacy Rules) – to regulate ONI's collection and communication of identifying information about Australians. The IGIS reviewed ONI's compliance with the Privacy Rules as governed by the *Office of National Intelligence Act 2018* (ONI Act) and ONI's internal guidelines. Under the ONI Privacy Rules, ONI can only collect or communicate this information in specific circumstances where needed to properly perform its functions. Records of instances where ONI has collected or communicated this information are kept by ONI and reviewed annually by the IGIS. To provide further independent assurance, the IGIS reviews ONI reporting for references to Australian persons and uses this information to cross-check records provided by ONI.

The inspection identified no noncompliance with legislation; however, the IGIS identified 14 instances of noncompliance with ONI's internal guidelines. ONI had commenced actioning systematic improvements to address the identified issues prior to the delivery of the inspection findings. The IGIS found these steps to be reasonable and appropriate, and therefore did not make any recommendations related to these findings.

The IGIS will continue to review ONI's compliance with the Privacy Rules in 2024–25.

Internal security investigations

The IGIS routinely conducts inspections in other agencies relating to internal security investigations, particularly where there may be an impact on an individual's clearance. ONI had not previously been subject to an inspection on this topic; therefore this inspection focused on the governance arrangements surrounding internal security investigations.

The IGIS identified no legality concerns; however, the inspection made one propriety finding relating to a lack of detailed policies and procedures to govern the undertaking of sensitive internal security investigations, including where there may be an impact on an individual's clearance. The IGIS recommended that ONI develop or update its policies and guidance on internal security investigations. The IGIS will review ONI's progress in implementing this recommendation at a future inspection.

ONI's human rights assessments and foreign engagement authorities

The IGIS reviewed ONI's compliance with section 13 of the ONI Act and internal guidance relating to cooperation with entities in connection with the performance of ONI's functions. The inspection focused on ONI's process for assessing and approving engagement with a foreign authority, including assessment of a foreign authority's regard for human rights.

The inspection made 2 propriety findings relating to noncompliance with internal record-keeping requirements and the communication of inaccurate human rights risks to ONI staff. The IGIS did not consider that the inaccurate communication adversely affected any individual's human rights. Four recommendations were made in relation to improving record keeping and ONI staff awareness of relevant requirements and processes.

ONI's analytic integrity

The IGIS undertook an inspection of ONI's policies and processes that ensure ONI can demonstrate the analytic integrity, including analytic rigour, contestability and independence of judgement, of its intelligence assessment products and activities. This inspection focused on a small sample of intelligence assessment products produced under significant time pressure. The IGIS reviewed the tasking and scope of the products, and whether ONI could demonstrate that consultation and internal approval processes were transparent and free from bias.

The IGIS identified no legality concerns. The inspection did not find any evidence that any product lacked analytic integrity, and found that ONI was able to demonstrate analytic integrity with adequate records, per its internal policy, in the majority of products reviewed. The inspection made one finding of noncompliance with ONI's records management requirements which ensure analytic integrity can be readily demonstrated, and made one recommendation to address the issue.

Compliance incidents

ONI did not report any compliance incidents to the IGIS in 2023–24.

Australian Security Intelligence Organisation

Key statistics



25

Inspections commenced



27

Inspections completed



37

Compliance incidents reported



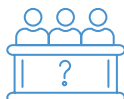
2

Ministerial letters sent to relevant minister



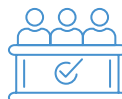
4

Senior-level meetings held



1

Inquiry commenced



2

Inquiries completed

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, undertaking security vetting and security clearance related activities, and collecting and communicating foreign intelligence. In addition to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), ASIO is bound by Minister's Guidelines that set out principles that govern ASIO's work; provide guidance on obtaining, correlating and evaluating intelligence; 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 Security Intelligence Organisation

In 2023–24, the IGIS undertook inquiries into and inspections of ASIO's activities.

Inquiries were undertaken into specific issues or matters identified through the IGIS's other oversight activities. In 2023–24, one inquiry in relation to ASIO, initiated by a complaint made to the IGIS, was commenced under section 8 of the IGIS Act. In addition, we finalised 2 inquiries that commenced during 2022–23, including one initiated by a complaint made to the IGIS.

The IGIS conducted one preliminary inquiry relating to ASIO, which is reported on in 'Cross-agency activities' later in this section.

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

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

Four scheduled meetings were held between the Inspector-General, the Director-General of Security, the IGIS's senior leadership team and ASIO senior executives in August and November 2023 and February and June 2024. Separately the IGIS sought briefings from ASIO on specific matters to support our oversight activities. ASIO provided additional briefings on matters it considered appropriate to bring to the IGIS's attention.

Access to systems, personnel and information

In 2023–24, ASIO provided the IGIS with appropriate direct access to ASIO systems and facilities to support our oversight work. Overall, for individual inspections and inquiries, ASIO provided access to appropriate personnel and information in a timely manner to enable the IGIS's oversight activities.

Inquiries

Of the 2 inquiries finalised by the IGIS in relation to ASIO in the reporting period, one is reported on in 'Complaints and public interest disclosures' later in this section and one is detailed in the following paragraph.

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 staff of an intelligence agency under section 18 of the ASIO Act and section 65(1) of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). The inquiry followed a preliminary inquiry in which the Director-General of Security provided information to the IGIS about current practices for authorising the communication of information. The inquiry found that before 5 April 2023, the Director-General of Security had not authorised particular persons approved to exercise authority under a warrant issued pursuant to Part 2-2 of the TIA Act to communicate lawfully intercepted information to other persons, as required by section 65(1) of the TIA Act. The relevant authority was given by the Director-General on 5 April 2023.

Inspections

The IGIS undertook 25 inspections of ASIO activities in 2023–24.

Of these 25 inspections, 3 remained underway at the end of the financial year. This includes inspections relating to a cross-agency examination of warranted collection activity, the liaison and exchange of information with foreign authorities, and ASIO's internal investigations. The IGIS's findings on these inspections will be reported in 2024–25.

In addition to the 22 inspections commenced and completed in 2023–24, we completed a further 5 inspections that commenced in 2022–23.

Of the 27 inspections completed in 2023–24, the IGIS did not identify any legality or propriety concerns in 19 inspections looking into the following matters:

- case inspection (2 inspections)
- warrants (2 inspections)
- human source management (2 inspections)
- covert online operations
- testing authorisations
- compartments and records
- compliance remediation and monitoring (2 inspections)
- SIOs
- visa and citizenship referrals (2 inspections)
- section 13B notices
- temporary exclusion orders
- public interest disclosures (PIDs)
- TOP SECRET-Privileged Access vetting capability
- foreign liaison and exchange of information.

In some instances the IGIS made recommendations, based on compliance observations, directed to improving the clarity of, and compliance with, ASIO's internal policies and procedures, or to promote stronger compliance practices, particularly in regard to the quality of record keeping. In one inspection focused on ASIO's technical collection and retention, we identified some data management issues.

The IGIS identified matters relating to legality or propriety in 8 of the 27 completed inspections. High-level descriptions of the findings and recommendations appear below.

Human source management

The IGIS conducts regular inspections of ASIO's human source management. Although the majority of inspections during 2023–24 identified no legality or propriety issues, one inspection identified a number of propriety concerns about ASIO's management of a particular case. At the time of the inspection, ASIO had already independently identified similar concerns and commenced remediation of the case. The IGIS was satisfied that these concerns, while serious, did not represent systemic issues with ASIO's human source management.

Retained items

The IGIS conducted an inspection of ASIO's management of items retained during search operations. In particular, the IGIS identified concerns about ASIO's processes for the longer-term retention of these items. The IGIS was unable to identify the basis on which some items were continuing to be retained, or evidence that periodic review of the retention of these items had occurred. The Inspector-General considered there was a real prospect that one or more of the items had been retained beyond the period referred to in section 25(4C) of the ASIO Act. The IGIS considered that ASIO's proposed approach to address the concerns raised and ensure compliance with its legislative obligations regarding the longer-term retention of items was appropriate. The IGIS will revisit these issues in a future inspection.

Security assessments

The IGIS conducted an inspection of adverse and qualified security assessments furnished by ASIO, with a particular focus on cases where the subject of the assessment was not entitled to review through the Administrative Appeals Tribunal or the Independent Reviewer of Adverse Security Assessments. The IGIS raised concerns in one case about whether ASIO's records properly supported the assessment that was reached.

Device access orders under section 34AAD of the ASIO Act and ASIO's use of section 313 notices and industry assistance requests under the *Telecommunications Act 1997*

This inspection is conducted annually. Its scope includes ASIO's use of device access orders under section 34AAD of the ASIO Act, notices provided under section 313 of the *Telecommunications Act 1997* (Telecommunications Act) and industry assistance requests issued under Part 15 of the Telecommunications Act.

In its inspection started in 2022–23 but completed in 2023–24, the IGIS raised concerns in relation to one device access order, specifically about the accuracy of reporting provided to the Attorney-General. The IGIS recommended that ASIO reconsider the report it had provided and make corrections where required. The IGIS also commented on ASIO's response to a recommendation arising from the IGIS's 2021–22 inspection about ASIO's device access order policy and recommended that consideration be given to further amendments to this policy. In relation to section 313 notices, the IGIS recommended that a standard template be developed to help ensure that legal and policy requirements are considered and met. For industry assistance requests, the IGIS identified concerns about ASIO's compliance with section 3.5 of the Minister's Guidelines concerning consideration of the proportionality of immunities. The IGIS recommended that ASIO's templates be updated to promote compliance with this obligation.

In the inspection conducted in 2023–24, the IGIS identified similar concerns to those identified in the previous inspection concerning the proportionality considerations required by section 3.5 of the Minister's Guidelines for industry assistance requests. The IGIS recommended that ASIO give further consideration to staff training and internal monitoring of compliance with this obligation. In relation to section 313 notices, the IGIS recommended that ASIO consider additional procedural guidance for staff. In addition, the 2023–24 inspection paid particular attention to device access orders and the issues of accuracy of reporting identified in the previous inspection. The IGIS did not identify any concerns about ASIO's use of these orders during 2023–24. The IGIS will revisit these topics in a 2024–25 inspection.

Foreign intelligence collection

In 2022–23, the IGIS conducted an inspection of ASIO's activities in support of the foreign intelligence function set out in section 17(1)(e) of the ASIO Act. This was the first recent inspection focused solely on this function. The inspection identified issues with ASIO's warrant revocation processes and potential legislative noncompliance that had not previously been reported. In addition, the inspection raised questions about ASIO's compliance with Part 4 of the Minister's Guidelines and the potential need for the inclusion of updated guidance on foreign intelligence collection in the Minister's Guidelines. It also identified concerns about the completeness of ASIO's responses to some inspection questions. Following further investigation, ASIO confirmed several instances of legislative noncompliance and made internal recommendations to reduce the likelihood of similar incidents.

Separately the IGIS provided input to an external review of the Minister's Guidelines, to address the matters we had identified. In line with the IGIS's risk-based approach to the inspection program, we will continue to conduct targeted inspections of foreign intelligence collection activities during 2024–25.

Assumed identities

Part IAC of the *Crimes Act 1914* (Crimes Act) sets out the legal requirements for ASIO's management of assumed identities. In an inspection commenced in 2022–23 and completed in 2023–24, the IGIS reviewed ASIO's use of assumed identities. The IGIS found that ASIO's assumed identity administration system is largely effective in ensuring ASIO's compliance with its legal obligations. However, noting that the Crimes Act is prescriptive in its requirements, the inspection identified several instances of potential legislative noncompliance that it recommended ASIO investigate further. ASIO's subsequent investigation confirmed that legislative noncompliance had occurred and made internal recommendations to reduce the likelihood of similar noncompliance occurring. The IGIS will review the effectiveness of this remediation in future inspections.

Warrants

The IGIS conducted an inspection that focused on ASIO's reporting to the Attorney-General of warrant-related noncompliance, as well as ASIO's implementation of the record-keeping requirements set out in section 24(3A) of the ASIO Act and section 12(4) of the TIA Act. These requirements were introduced by the *National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Act 2022* and require the Director-General 'as soon as practicable' after the authority of a warrant (or, for the purposes of the ASIO Act, a device recovery provision) is exercised to make a written record that identifies each person who exercised that authority. The IGIS did not identify any concerns about ASIO's reporting to the Attorney-General. However, the IGIS identified concerns about the timeliness and accuracy of records produced for the purposes of section 24(3A) and section 12(4). The IGIS recommended that ASIO review its relevant policies and procedures to clearly articulate this obligation for relevant staff.

Other reviews required under legislation

In addition to its regular inspection program, the IGIS 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 2023–24, 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 IGIS reviewed each authorisation and report immediately following notification to the Inspector-General. Separately the IGIS conducted a periodic inspection to examine the activities undertaken under SIOs in greater detail. The IGIS did not identify any legality or propriety concerns in this inspection.

Compulsory questioning

ASIO's compulsory questioning powers, including provisions relating to the IGIS's oversight of the questioning or apprehension of a person, are contained in Part III Division 3 of the ASIO Act. The IGIS was not notified of any use of ASIO's compulsory questioning powers; therefore the Inspector-General did not attend any questioning sessions during 2023–24.

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 section 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 as soon as practicable. The IGIS did not receive any use of force notifications in 2023–24.

Compliance incidents

The IGIS independently reviews all compliance incidents that ASIO reports. In doing so, we may seek additional information or undertake further review. The IGIS'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, we conduct 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 IGIS 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 IGIS on propriety grounds. As with other compliance incidents, we review these matters and may seek additional information, undertake further investigation and provide additional recommendations.

In 2023–24, ASIO reported 37 compliance incidents to the IGIS. This included notification of incidents that on further assessment by ASIO were determined to be compliant.

ASIO also provided notification of 14 incidents outside its 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 IGIS reviewed matters of legislative noncompliance reported by ASIO. These incidents and the IGIS's findings, where the matter has been finalised in the reporting period, are outlined below. Four incidents remained under assessment by ASIO at the end of 2023–24 and will be reported in 2024–25.

Telecommunications (Interception and Access) Act 1979

Noncompliance with section 7 and section 63 of the TIA Act – unauthorised telecommunications interception: 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. 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. ASIO notified the IGIS of 12 incidents that were noncompliant with section 7 and/or section 63 of the TIA Act, or potentially noncompliant with section 7(1)(b). Nine of these incidents were errors in warrant documentation, including the addition of services to a warrant that were not used by the subject of the warrant, delays in disconnecting interception of services that were not used by the subject of the warrant and, for one incident, the list of persons authorised to execute the authority of the warrant being approved by an ASIO officer who did not have the authority to do so. In relation to all incidents, on identifying the error, ASIO ceased interception and requested that the data be deleted.

The remaining 3 incidents occurred as a result of carrier or service provider errors that were outside ASIO's control but resulted in legislative noncompliance for ASIO. In the first incident, a technical issue at the carrier resulted in ASIO being provided with intercepted communications for an incorrect service. The second incident occurred due to an error in carrier systems and resulted in a large quantity of data being erroneously provided to ASIO. In the third incident, an error by the service provider resulted in ASIO receiving data that had not been requested. In relation to each case, ASIO investigated the cause of the incident with the carrier or service provider and requested that the data be deleted. The IGIS was satisfied with ASIO's assessment and remediation of these 12 incidents and will verify data deletion as part of its regular inspection program.

Noncompliance with section 11B(2)(ba) of the TIA Act – error in warrant documentation: ASIO notified the IGIS of an incident where a warrant issued under section 11B of the TIA Act contained an error in the identification of one of the telecommunications devices. On identifying the error, ASIO varied the warrant to remove the device. Data had not been collected, so data deletion was not required. ASIO assessed this incident to be noncompliant with section 11B(2)(ba) of the TIA Act but considered that it did not invalidate the warrant. The IGIS agreed with this assessment and considered ASIO's remediation to be appropriate.

Noncompliance with section 15(1A)(d) and section 15(1B)(d) of the TIA Act – failure to provide certified copies of warrants: ASIO notified the IGIS that it had failed to provide certified copies of warrant instruments to 2 carriers in accordance with section 15 of the TIA Act. This incident arose from changes in the way these notices were delivered to carriers which resulted in notices not being received by the carriers for several months. The carriers take action on connection and disconnection requests via a separate system rather than on receipt of the certified copies of warrant instruments. On identifying the issue, ASIO provided all outstanding certified copies and established an alternative system to provide these instruments until a technical solution is implemented. ASIO assessed that the incident had resulted in noncompliance with section 15(1A)(d) and section 15(1B)(d) of the TIA Act. The IGIS agreed with this assessment and considered ASIO's remediation to be appropriate.

Noncompliance with section 175 of the TIA Act – errors in telecommunications data

authorisations: Section 175 of the TIA Act empowers certain ASIO personnel to authorise the disclosure of historical telecommunications data by telecommunications carriers or carriage service providers in connection with the performance of ASIO's functions. The ASIO personnel who can give an authorisation are described by section 175(2) as an eligible person. ASIO notified the IGIS of 7 noncompliance incidents relating to authorisations for telecommunications data under section 175 of the TIA Act. In relation to each incident, there was an error in the authorisation made by the eligible person. The IGIS agreed with ASIO's assessment that each incident was noncompliant with section 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. In addition, the IGIS agreed with ASIO's assessment that one of the incidents was also noncompliant with section 3.7 of the Minister's Guidelines.

Potential noncompliance with section 181 of the TIA Act – authorisations provided to wrong service provider:

ASIO notified the IGIS of an incident where an authorisation made under section 175 of the TIA Act was sent to the wrong service provider. ASIO identified the error the following day; however, the authorisation had already been actioned by the service provider. ASIO initially reported the matter as a potential noncompliance with section 181A of the TIA Act; however, following legal advice, ASIO concluded that while an error had been made, there was no legislative noncompliance. Data was deleted and a new authorisation was issued. The IGIS agreed with ASIO's assessment and considered the remediation to be appropriate.

ASIO notified the IGIS of a separate incident where an authorisation under section 176 of the TIA Act was provided to the wrong service provider. Although the error was identified almost immediately, the authorisation had already been processed by the service provider. No data was provided to ASIO and a new authorisation was issued to the correct service provider. As with the above incident, ASIO assessed that there was no legislative noncompliance. The IGIS agreed with this assessment.

Australian Security Intelligence Organisation Act 1979

Noncompliance with section 16(1C) of the ASIO Act – furnishing security clearance suitability

assessments: Section 16(1C) provides that the Director-General can delegate the power to furnish a security clearance suitability assessment to an ASIO employee or ASIO affiliate who holds, or is acting in, a position equivalent to or higher than an Executive Level 1 position. This delegation was introduced by the *Australian Security Intelligence Organisation Amendment Act 2023*. ASIO notified the IGIS of 4 incidents related to noncompliance with section 16(1C), where non-prejudicial security clearance suitability assessments had been furnished by an officer who did not have authority to do so. The IGIS agreed with ASIO's assessment that these incidents were noncompliant with section 16(1C) and was satisfied with ASIO's remediation action. The IGIS notes that section 16(1C) was subsequently amended by the *National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Act 2024*, which received Royal Assent on 21 May 2024.

Noncompliance with section 21A of the ASIO Act – failure to notify the Inspector-General of a voluntary assistance request:

Section 21A of the ASIO Act requires the Director-General to notify the Inspector-General within 7 days of the Director-General making a request under section 21A(1)(a). ASIO notified the IGIS that it had identified that a required notification had not been provided to the Inspector-General within 7 days. The error was identified during preparation of ASIO's 2022-23 Annual Report. ASIO assessed that it was noncompliant with section 21A, and the IGIS agreed with this assessment.

Noncompliance with section 30 of the ASIO Act – warrant revocation: Section 30(1) of the ASIO Act provides that where the Director-General is satisfied that the grounds for a warrant have ceased to exist, the Director-General must inform the Attorney-General and take steps to discontinue action authorised under the warrant as soon as practicable. ASIO notified the IGIS of an incident where an error in ASIO's processes meant that the Attorney-General was not informed as soon as practicable that the grounds for a warrant had ceased to exist. On identifying the incident, ASIO provided the required advice to the Attorney-General. ASIO assessed the incident as noncompliant with section 30(1)(a) of the ASIO Act and ASIO's internal procedure for warrant revocation. The IGIS agreed with ASIO's assessment and remediation.

Potential noncompliance with the ASIO Act – execution of search activity under an identified person warrant: ASIO notified the IGIS of an incident where an error in implementing a procedure resulted in 2 searches being conducted of an individual in circumstances where only one search authority had been authorised by the Director-General. Following consideration of the specific circumstances of the incident and legal advice, ASIO assessed that the error did not result in noncompliance with the ASIO Act. The IGIS agreed with this assessment.

Minister's Guidelines to ASIO

Noncompliance with section 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 IGIS of an incident where a service intercepted under a warrant was used by a family member of the target rather than the target themselves. This information was known to ASIO but not identified until after the service was added to the warrant. On identification of the issue, ASIO ceased the interception and deleted data that had been collected. ASIO assessed this incident as noncompliant with section 3.4 of the Minister's Guidelines. The IGIS agreed with ASIO's assessment and remediation and will verify data deletion as part of its regular inspection program.

Crimes Act 1914

Noncompliance 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 IGIS of 2 incidents. The first incident related to 2 errors in a request for assumed identity evidence. The error was not identified for several years. ASIO assessed that the incident was noncompliant with section 15K(4)(b) and section 15KX(3) of the Crimes Act, and the IGIS agreed with that assessment.

The second incident related to an incorrect date of birth being used to obtain evidence of an assumed identity. It was an historical error that occurred when ASIO relied on a paper-based system for managing assumed identities and was identified when new evidence was sought by the relevant officer. ASIO assessed that the incident resulted in 3 instances of noncompliance with section 15K(4)(b) of the Crimes Act. The IGIS agreed with ASIO's assessment. The IGIS notes that ASIO's current processes, including an electronic assumed identities administration system, reduce the likelihood of these types of incidents occurring.

Finalisation of 2022–23 compliance incidents

Several compliance incidents that were reported during 2022–23 were finalised during 2023–24.

The following incidents were found to involve legislative noncompliance. Five additional incidents relating to potential noncompliance with the TIA Act, ASIO Act or Crimes Act were determined on further investigation to be compliant.

Noncompliance with section 7 of the TIA Act – unauthorised telecommunications interception:

ASIO notified the IGIS of 2 incidents relating to warrants obtained under section 11B of the TIA Act. In the first incident, a service was added to the warrant in error. ASIO assessed that this incident was noncompliant with section 7 and section 63 of the TIA Act. The IGIS agreed with ASIO's assessment and remediation action. In the second incident, a carrier error resulted in the interception of an incorrect service. ASIO assessed that this incident was noncompliant with section 7 of the TIA Act. The IGIS agreed with this assessment and ASIO's remediation and will verify data deletion as part of its regular inspection program.

Noncompliance with section 13 of the TIA Act – warrant revocation: Section 13 of the TIA Act requires the Director-General, in circumstances where the Director-General is satisfied that the grounds on which a warrant was issued have ceased to exist, to inform the Attorney-General 'forthwith' and take steps to ensure that interception is discontinued. ASIO notified the IGIS of an incident where an error in ASIO's processes meant that the Attorney-General was not informed of the intention to revoke the warrant until 26 days after the Director-General was satisfied that the grounds for the warrant had ceased to exist. The IGIS agreed with ASIO's assessment that the matter was noncompliant with section 13 of the TIA Act.

Noncompliance with section 175 of the TIA Act – errors in telecommunications data

authorisations: ASIO notified the IGIS of 2 incidents that it assessed to be noncompliant with section 175 of the TIA Act as a result of errors in the authorisation given by the eligible person. The IGIS agreed with ASIO's assessment and remediation and will verify data deletion as part of its regular inspection program.

Noncompliance with section 24(1) of the ASIO Act – access to restricted data: 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 IGIS of an incident where an ASIO staff member who was not listed on an authorisation list for a warrant accessed restricted data. ASIO assessed the incident to be noncompliant with section 24(1) of the ASIO Act on the basis that the officer was not authorised to execute the authority of the warrant. The IGIS agreed with ASIO's assessment.

Potential noncompliance with Division 3 of Part VIIC of the Crimes Act – spent convictions:

ASIO notified the IGIS that it had identified that spent conviction information may be present in its holdings contrary to Division 3 of Part VIIC of the Crimes Act. At the time of ASIO's notification, Division 3 and the Crimes Regulations permitted ASIO to access spent conviction information for the purposes of assessing prospective employees or prospective members of the agency, or persons proposed to be engaged as consultants to, or to perform services for, the agency or a member of the agency. ASIO was not permitted to have spent conviction information for other purposes. Following a recommendation from the Comprehensive Review of the Legal Framework of the National Intelligence Community, the *National Security Legislation Amendment (Comprehensive Review and Other Measures No. 2) Act 2023* expanded ASIO's powers to use, record and disclose spent conviction information. ASIO assessed that it was not possible to reach a definitive determination of ASIO's compliance prior to legislative change and concluded that it was potentially noncompliant with Division 3 of Part VIIC of the Crimes Act. In its consideration of this incident, ASIO identified additional issues associated with state and territory spent

conviction legislation. The IGIS accepted ASIO's assessment of potential noncompliance with the Crimes Act. ASIO's remediation of the incident remains ongoing. The IGIS will monitor this through its regular oversight activities.

Noncompliance with section 3.7 of the Minister's Guidelines – accuracy of information:

ASIO notified the IGIS of an incident where an authorisation under section 176 of the TIA Act relied on incorrect data provided by a partner agency. ASIO assessed that the incident was noncompliant with section 3.7 of the Minister's Guidelines as the relevant area within ASIO had conducted insufficient checks to determine the accuracy of the data before it was included in the authorisation. The IGIS agreed with ASIO's assessment and remediation and will verify data deletion as part of its regular inspection program.

Australian Secret Intelligence Service

Key statistics



16

Inspections
commenced



16

Inspections
completed



15

Compliance
incidents reported



2

Ministerial letters
sent to relevant
minister



3

Senior-level
meetings held



2

Inquiries
commenced



0

Inquiries
completed

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 Secret Intelligence Service

In 2023-24, the IGIS undertook both inquiries into and inspections of ASIS's activities.

Inquiries were undertaken into specific issues or matters identified through the IGIS's other oversight activities. In 2023-24, 2 inquiries in relation to ASIS were commenced under section 8 of the IGIS Act; both inquiries were initiated through complaints or disclosures made to the IGIS in a previous reporting period.

The IGIS conducted one preliminary inquiry relating to ASIS, which is reported on in 'Cross-agency activities' later in this section.

The IGIS implemented a risk-based approach to its inspections of ASIS, given the breadth of ASIS's functions under section 6 of the *Intelligence Services Act 2001* (IS Act).

The IGIS continued to independently review all compliance incident reports from ASIS relating to noncompliance with legislation, ASIS's Privacy Rules, or internal policies and procedures.

Three scheduled meetings were held between the Inspector-General, the IGIS's senior leadership team and ASIS senior executives in August 2023, November 2023 and March 2024. These meetings were a valuable opportunity to discuss organisational priorities and challenges, along with oversight and inspection activities.

Access to systems, personnel and information

In 2023–24, ASIS provided the IGIS with appropriate facility access and direct access to ASIS systems to support oversight work. The IGIS had previously experienced some delays in accessing relevant ASIS records, which hampered our ability to finalise inspections in a timely manner. ASIS and the IGIS worked collaboratively to identify solutions to improve access, which resulted in a significant improvement to the IGIS's ability to have timely access to ASIS records in 2023–24.

Inspections

The IGIS undertook 16 inspections of ASIS activities in 2023–24.

Of these 16 inspections, 3 inspections that commenced in 2023–24 remain underway, including inspections of specific intelligence activities, operations or programs, one of which is a cross-agency inspection. The IGIS's findings on these inspections will be reported in 2024–25.

In addition, the IGIS completed another 3 inspections that commenced in 2022–23.

Of the 16 inspections completed in 2023–24, the IGIS did not identify any legality or propriety concerns in 13 inspections looking into the following matters:

- ministerial submissions (6 inspections)
- ASIS's use and management of weapons
- a specific thematic-focused intelligence collection program
- a specific geographic-focused intelligence collection program
- overturned presumptions of nationality (cross-agency inspection)
- compliance frameworks and practices for IS Act section 13B notices (cross-agency inspection)
- human rights assessments
- internal security investigations.

In some instances, the IGIS made recommendations based on compliance observations directed to improving the clarity of, and compliance with, ASIS's internal policies and procedures, or to promote stronger compliance practices, in particular with regard to improving the quality of record keeping.

The IGIS identified matters relating to legality or propriety in the remaining 3 completed inspections. A high-level summary of the findings and recommendations is provided below. Due to the sensitive nature of ASIS's use of weapons, a summary of this inspection is also included, though no issues of legality or propriety were identified.

Operational files related to a specific geographic intelligence collection program

The IGIS identified instances of noncompliance with internal policies in one inspection of operational files related to a specific geographic intelligence collection program. This included one instance of noncompliance with internal record keeping policies and one instance of noncompliance with ASIS's human rights procedures when ASIS engaged with a liaison partner without an extant assessment of the human rights risks. The IGIS did not consider that this instance of noncompliance adversely affected any individual's human rights. The inspection provided 2 recommendations designed to strengthen ASIS's ability to demonstrate compliance with internal policies.

Operational files related to a specific ASIS function

The IGIS identified one propriety concern in relation to records management in an inspection of a specific enabling function within ASIS. The IGIS reviewed operational files relating to activities undertaken or supported by this specific ASIS function over an 18-month period. The IGIS made one recommendation for ASIS to improve their record keeping practices, particularly in relation to operational activities and key decision-making.

Use of weapons

In 2023–24, the IGIS reviewed ASIS's management of weapons and the associated qualifications of ASIS officers, to ensure compliance with legislation and internal governance. The IGIS reviewed internal records, policies and procedures in relation to Schedules 2 and 3 of the IS Act.

The IGIS did not identify any instances of noncompliance with legislation or policy, or any propriety concerns. The IGIS continues to be satisfied that there is a requirement for a limited number of ASIS officers to have access to weapons for self-defence to perform their duties effectively, and that ASIS has appropriate management controls in place.

Operational files related to ASIS activities overseas

The IGIS undertook one inspection of ASIS's operational files at an overseas location for a specified time period. The IGIS did not identify any instances of noncompliance with legislation; however, the inspection did identify 2 instances of noncompliance with ASIS's internal policies and one propriety concern relating to human rights risk management procedures. The IGIS did not consider that this instance of noncompliance adversely affected any individual's human rights.

The inspection provided 3 recommendations designed to strengthen ASIS's compliance with internal policies and improve ASIS's approach to human rights risk management.

Rules to Protect the Privacy of Australians

The Minister for Foreign Affairs issues written rules – *Rules to Protect the Privacy of Australians* (the Privacy Rules) – to regulate ASIS's communication and retention of intelligence information about Australian persons. The IGIS reviews ASIS's compliance with the Privacy Rules as part of all relevant inspections and does not conduct a standalone Privacy Rules inspection.

The IGIS has observed ASIS to have a robust Privacy Rules compliance program; while several compliance incidents related to compliance with the Privacy Rules are identified in 'Compliance incidents' below, these are not assessed to be indicative of systemic issues.

Notification of overturned presumptions of nationality

Under the Privacy Rules, ASIS must provide the IGIS with access to all of ASIS's intelligence holdings and report to the IGIS any noncompliance with the rules. ASIS must also report to the IGIS when it determines that a person, relevant to intelligence activities, previously presumed to be foreign is an Australian person – known as 'overturning a presumption of nationality' (OPN). This usually occurs when ASIS 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 noncompliance with legislation or the Privacy Rules.

In 2023–24, the IGIS reviewed 3 specific reports provided by ASIS in which the application of ASIS's Privacy Rules resulted in a presumption of nationality being overturned. Two additional reports were included as part of other compliance incident reporting.

In each of the 5 cases reviewed, the IGIS determined that the initial presumption of nationality was reasonable, and that ASIS took appropriate measures to protect the privacy of Australian persons.

ASIS's OPN program as a whole was reviewed under a cross-agency inspection and is reported on in 'Cross-agency activities' later in this section.

Compliance incidents

The IGIS independently reviews all compliance incidents reported by ASIS. In doing so, the IGIS may seek additional information or undertake further investigation. The IGIS's review includes consideration of ASIS's remediation action, and any relevant legal advice on which ASIS has relied. The IGIS may provide further recommendations to remediate the incident or minimise the risk of recurrence.

In 2023–24, ASIS provided 15 compliance incident notifications to the IGIS. Of the 15 incidents, 4 remain under investigation and 3 had no findings of noncompliance. The IGIS's review of 2 compliance incident notifications provided in 2022–23 also concluded in 2023–24; one of these had no findings of noncompliance.

Themes, findings and recommendations relating to the remaining 9 incidents are outlined below.

Section 15 (1A) of the *Intelligence Services Act 2001*

The IGIS found one instance in which ASIS was noncompliant with section 15(1A) of the IS Act. ASIS failed to apply the Privacy Rules when communicating information concerning Australian persons. When considering if a failure to apply the Privacy Rules amounts to a breach of legislation, the IGIS considers incidents of non-application of the Privacy Rules on a case-by-case basis, with reference to the seriousness of the incident and the context in which decisions to not apply the Privacy Rules were made. The IGIS assessed that this incident could have been avoided if ASIS had undertaken appropriate checks and if internal processes had been correctly applied. In addition, there were 3 instances of non-application of the Privacy Rules that were not considered breaches of section 15 (1A) of the IS Act due to the specific context and circumstances. The IGIS made recommendations for all ASIS officers to complete mandatory training on the Privacy Rules and related internal policies, and other recommendations specific to each instance.

Non-recording of the Privacy Rules

The IGIS found 4 instances in which ASIS did not properly record application of the Privacy Rules, in contravention of ASIS internal policy. The IGIS provided recommendations to ASIS relevant to the specific circumstances of each incident.

Noncompliance with Privacy Rule 1

The IGIS found 2 instances in which ASIS did not appropriately apply Privacy Rule 1, constituting 2 propriety findings. While Privacy Rule 1 is a presumption, an incorrect presumption of nationality can still give rise to issues of propriety, particularly if there was known evidence to the contrary, or an absence of evidence that reasonable due diligence was undertaken before applying the presumption. The IGIS provided recommendations to ASIS relevant to the specific circumstances of each incident.

Noncompliance with ASIS policy

The IGIS found one instance in which ASIS did not comply with internal policy, constituting one propriety finding. As ASIS identified appropriate remediation measures, no recommendations were made in relation to this incident.

Timeliness of notification to the national intelligence community

The IGIS found 3 instances in which ASIS delayed notifying NIC agencies of an OPN. These have been recorded as propriety findings, as delays in informing NIC agencies increase the risk that Australian persons may inadvertently have their privacy infringed. The IGIS recommended that ASIS update relevant policies and improve mandatory training to ensure all ASIS staff understand their obligations under the Privacy Rules.

Australian Signals Directorate

Key statistics



20

Inspections commenced



17

Inspections completed



29

Compliance incidents reported



2

Ministerial letters sent to relevant minister



2

Senior-level meetings held



0

Inquiries commenced



0

Inquiries completed

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 policymakers 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 Signals Directorate

In 2023–24, the IGIS undertook inspections of ASD's activities pursuant to section 9A of the IGIS Act. The IGIS did not commence any inquiries under section 8 of the IGIS Act in relation to ASD.

The IGIS implemented a risk-based approach to its inspections of ASD, given the breadth of ASD's activities performed under section 7 of the IS Act. In 2023–24, the IGIS continued the approach from the previous reporting period to focus inspections on areas of growth under ASD's Project REDSPICE (Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers).

The IGIS continued to independently review all compliance incidents reported by ASD relating to noncompliance with legislation, ASD's privacy rules, or ASD's internal policies and procedures.

Two scheduled meetings were held between the Inspector-General, the IGIS's senior leadership team, the Director-General of ASD and ASD senior executives in October 2023 and March 2024. These meetings were a valuable opportunity to discuss organisational priorities and challenges, along with oversight and inspection activities.

Access to systems, personnel and information

In 2023–24, ASD provided the IGIS with appropriate direct access to ASD systems and facilities to support its oversight work. Further, for individual inspections and preliminary inquiries, ASD provided access to appropriate personnel and information in a timely manner to enable the IGIS's oversight activities.

Preliminary inquiries

The Inspector-General conducted an own-motion preliminary inquiry relating to ASD which is reported on in 'Cross-agency activities' later in this section.

An own-motion preliminary inquiry that commenced in 2022–23 remained underway at the end of 2023–24. Further details about this matter are provided in 'Complaints and public interest disclosures' later in this section.

Inspections

The IGIS undertook 20 inspections of ASD's activities in 2023–24. Of these, 16 were completed during the reporting period and 4 remained underway, including inspections of the accuracy of information communicated in ministerial submissions; the legality and propriety of ASD's ministerial authorisations; a cross-agency inspection relating to a warranted collection activity; and a review of a specific collection capability. The IGIS's findings in relation to these inspections will be reported in 2024–25.

In addition, the IGIS completed one inspection that commenced during 2022–23.

Of the 17 inspections completed in 2023–24, the IGIS did not identify legality or propriety concerns in 16 inspections looking into the following matters:

- the legality and propriety of ASD's 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 (4 inspections)
- the application of ASD's privacy rules made under the IS Act (4 inspections)
- targeted inspections of ASD's compliance with its obligations under ministerial directions, the *Telecommunications (Interception and Access) Act 1979* and the IGIS's previous inspection findings (2 inspections)
- ASD's cyber-focused activities under section 7(1)(d) and (f) of the IS Act
- a cross-agency inspection of the frameworks and processes for overturned presumptions of nationality.

In some instances, the IGIS made recommendations based on compliance observations directed at improving the clarity of, and compliance with, ASD's internal policies and procedures, or to promote stronger compliance practices, particularly in regard to improving the quality of record keeping.

During one of the ministerial authorisation inspections outlined above, ASD identified and reported an incident of legislative noncompliance. Further details of this matter are provided in 'Compliance incidents' below.

The IGIS's inspection of ASD's Responsible Release Framework for Cyber Security Vulnerabilities identified propriety concerns as outlined below.

Responsible Release Framework for Cyber Security Vulnerabilities

The IGIS conducted an inspection of ASD's administration of its Responsible Release Framework for Cyber Security Vulnerabilities. This inspection identified a range of deficiencies in relation to the completeness of records relating to decisions to retain or release cyber vulnerabilities, including the sufficiency of internal governance arrangements around the process and the lack of timeliness around decision-making, all of which were inconsistent with ASD's public-facing commitments outlined in the framework.

The IGIS noted that at the time of the inspection, ASD had begun taking steps to address some of the areas of concern we identified. The IGIS intends to further review ASD's responsible release framework in a future inspection.

Rules to Protect the Privacy of Australians

The Minister for Defence issues written rules – *Rules to Protect the Privacy of Australians* (the Privacy Rules) – to regulate the communication and retention by ASD of intelligence information about Australian persons. In 2023–24, the IGIS undertook 4 inspections of ASD's application of the Privacy Rules and identified no legality or propriety concerns. Each inspection confirmed that ASD has comprehensive policies and procedures in place to manage the communication and retention of intelligence information concerning Australian persons. The IGIS will continue its regular review of ASD's implementation of the Privacy Rules in 2024–25.

Overtaken presumptions of nationality

Under the Privacy Rules, ASD must provide the IGIS with access to all of ASD's intelligence holdings and report to the IGIS any noncompliance with the rules. ASD must also report to the IGIS when it determines that a person, relevant to intelligence activities, 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 noncompliance with legislation or the Privacy Rules.

In 2023–24, the IGIS reviewed 29 reports provided by ASD in which the application of the Privacy Rules resulted in a presumption of nationality being overturned, including 3 reports received during a previous reporting period.

In each of the 29 cases reviewed, the IGIS determined that the initial presumption of nationality was reasonable, and that ASD took appropriate measures to protect the privacy of Australian persons. The IGIS 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 Privacy Rules.

The IGIS observed one instance of noncompliance with internal policy that ASD identified and reported to the IGIS. The IGIS also made observations regarding the timeliness of some actions ASD undertook as part of its OPN processes.

ASD's OPN program as a whole was reviewed under a cross-agency inspection, which is reported on 'Cross-agency activities' later in this section.

Compliance incidents

The IGIS independently reviews all potential compliance incidents reported by ASD. The IGIS often requires additional information or technical briefings from ASD while investigating incidents, to ensure that circumstances surrounding the incident can be fully understood and we can reach 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 IGIS.

In 2023–24, ASD provided the IGIS with 29 notifications of potential compliance incidents at the start of ASD's internal investigation process, including those that were ultimately assessed to be compliant. ASD also continued its investigation of a further 11 potential compliance incidents from previous reporting periods. Of these 40 initial notifications, ASD provided the IGIS with 14 finalised compliance incident reports. Two of these resulted from one initial notification, due to the nature of the compliance incident. ASD also provided the IGIS with information regarding 4 other notifications of potential incidents of noncompliance which ASD had determined to be compliant. The IGIS conducted an independent review of these potential compliance incidents and agreed they did not represent noncompliance with legislation or with ASD's internal policies and procedures. Twenty-three incidents remained under internal ASD investigation at the end of 2023–24 and will be reviewed by the IGIS on receipt of the finalised reports.

In 2023–24, the IGIS completed its review of 10 compliance incident reports, including 9 provided during the reporting period and one provided in the previous reporting period. All 10 incidents were confirmed by the IGIS as matters of legislative noncompliance, resulting in 15 instances of noncompliance with legislation. At the end of the reporting period, 5 compliance incident reports were still under review by the IGIS.

Themes, findings and recommendations relating to the compliance incidents reviewed by the IGIS in 2023–24 are outlined below.

Telecommunications (Interception and Access) Act 1979

Two instances of noncompliance with section 7(1)(a) and section 63(1) of the TIA Act: In May 2023, ASD confirmed 2 occasions on which it was noncompliant with both section 7(1)(a) and section 63(1) of the TIA Act, following 2 incidents that took place in June and July 2020. In both incidents ASD inadvertently collected communications in the course of performing its proper functions. In reviewing these incidents, the IGIS agreed that each instance separately constituted a breach of section 7(1)(a) and section 63(1) of the TIA Act.

The IGIS found that the incidents occurred due to insufficient policies and procedures being in place to guide analysts in the performance of their work. The IGIS considered that the actions taken by ASD immediately following the incident, along with subsequent policy and systems development, were appropriate in the circumstances.

Two instances of noncompliance with section 7(1)(c) of the TIA Act: In October 2023 and February 2024, ASD confirmed 2 incidents of noncompliance with section 7(1)(c) of the TIA Act, in which ASD erroneously enabled the interception of communications passing over a telecommunications system. In both instances, no unauthorised communications were intercepted. The first incident occurred in February 2023 and the second in October 2023. In reviewing these incidents, the IGIS agreed that each instance separately constituted a breach of section 7(1)(c) of the TIA Act.

In response to both incidents, ASD released updated guidance to staff and identified additional controls to be implemented to improve quality assurance processes and minimise the risk of similar incidents occurring in future. The IGIS considered that these actions were appropriate in response to the incidents. The IGIS will review these new controls as part of future inspection activity.

Noncompliance with section 63(1)(a) of the TIA Act: In October 2023, ASD confirmed one instance of noncompliance with section 63(1)(a) of the TIA Act, after an incident in September 2022 in which data collected by a partner agency was inadvertently forwarded to ASD. The data was subsequently ingested into ASD systems. In this incident, a misconfiguration of a system controlled by the other agency resulted in unauthorised communications being passed to ASD. ASD has removed the data involved in the incident from its systems.

In reviewing this incident, the IGIS determined that it resulted from circumstances outside of ASD's control. The IGIS considered that ASD acted promptly and appropriately to remediate the situation.

Other legislation

Noncompliance with section 127(2) of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act): In February 2022, ASD confirmed that it had been noncompliant with section 127(2) of the AML/CTF Act, after an incident in July 2021 in which ASD disseminated AUSTRAC information to foreign agencies. In reviewing the incident, the IGIS agreed that it constituted a breach of section 127(2) of the Act and determined that it occurred as a result of lack of familiarity with ASD's internal policies regarding the dissemination of AUSTRAC information. In response, ASD issued updated internal policy advice to staff regarding dissemination of AUSTRAC information.

Four instances of noncompliance where activities were inconsistent with the terms of a legal authorisation: In February 2024, ASD confirmed that it had undertaken activities that were noncompliant with the terms of a legal authorisation on 4 occasions in March and April 2023. The effect of the incidents was that the authorisation received was insufficient to authorise the full scope of the activities undertaken. The incidents occurred due to an error in preparing the relevant authorisation documentation which was not identified before the activities through existing internal checks and safeguards.

In response to the incident, ASD updated its existing processes to provide greater guidance to staff, as well as introducing additional mandatory training for staff who conduct these activities. The IGIS assessed that ASD took appropriate steps in response to this incident to minimise the risk of incidents of this nature occurring in the future.

Noncompliance with section 15LE of the Crimes Act: In October 2023, ASD confirmed that it was noncompliant with section 15LE of the Crimes Act, in that it had not provided a report on its management of assumed identities to the Inspector-General as soon as practicable after the end of the 2021-22 financial year. ASD confirmed that it did not issue any assumed identities during 2021-22 and was in the process of developing its governance arrangements to support future issuance of assumed identities under section 15LE of the Crimes Act. The IGIS will monitor the development of these arrangements and the future issuance of assumed identities through its future inspections.

Noncompliance with section 9(5) of the Intelligence Services Act: In January 2024, ASD confirmed that it was noncompliant with section 9(5) of the IS Act when it identified that a ministerial authorisation for a specified activity was not available for inspection by the Inspector-General. In reviewing the incident, the IGIS observed that the authorisation had been consistently renewed since 2001. The IGIS confirmed that ASD has significantly improved its record-keeping processes since 2001, which should mitigate the risk of a future recurrence of this incident. ASD subsequently sought a new ministerial authorisation for the specified activity, which is available for inspection by the IGIS.

Noncompliance with section 8(3) of the Intelligence Services Act: In October 2023, ASD reported that it was noncompliant with section 8(3) of the IS Act, after an incident in September 2023. The incident involved ASD producing intelligence on an Australian individual before the commencement of a ministerial authorisation. In response, ASD has updated internal guidance to minimise the risk of similar incidents occurring in the future. In reviewing the incident, the IGIS agreed that it constituted an instance of noncompliance with section 8(3) of the IS Act, and considered that ASD had undertaken appropriate actions to minimise the risk of similar incidents occurring in the future.

Other reviews

In addition to inspection activities, the IGIS was also consulted and provided input on potential changes to ASD's Privacy Rules.

Australian Geospatial-Intelligence Organisation

Key statistics



7

Inspections commenced



6

Inspections completed



2

Compliance incidents reported



2

Ministerial letters sent to relevant minister



2

Senior-level meetings held



0

Inquiries commenced



0

Inquiries completed

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 the Australian Government's 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

Australian Geospatial-Intelligence Organisation

In 2023–24, the IGIS undertook inspections of AGO's activities pursuant to section 9A of the IGIS Act. The IGIS did not commence any inquiries under section 8 of the IGIS Act in relation to AGO.

The IGIS conducted one preliminary inquiry relating to AGO, which is reported on in 'Cross-agency activities' later in this section.

The IGIS implemented a risk-based approach to its inspections of AGO, given the breadth of AGO's activities performed under section 6B of the IS Act. In 2023–24, the IGIS focused its deep-dive inspections on areas of higher risk or sensitivity or areas that it had not previously inspected.

The IGIS continued to independently review all potential compliance incidents reported by AGO relating to noncompliance with legislation or AGO internal policies and procedures.

Two scheduled meetings were held between the Inspector-General, the IGIS's senior leadership team, the Director of AGO and AGO senior executives in August 2023 and February 2024. These meetings were a valuable opportunity to discuss organisational priorities and challenges, along with oversight and inspection activities.

Access to systems, personnel and information

In 2023–24, AGO provided the IGIS with appropriate direct access to AGO systems and facilities to support its oversight work. Generally, for individual inspections AGO provided access to appropriate personnel and information in a timely manner to enable the IGIS's oversight activities.

Inspections

The IGIS undertook 7 inspections of AGO activities in 2023–24. Of these, 6 were completed and one – a cross-agency inspection relating to warranted collection activity – remained underway at the end of 2023–24.

In all 6 completed inspections, the IGIS did not identify legality or propriety concerns. The inspections covered the following topics or activities:

- application of AGO's *Rules to Protect the Privacy of Australians* made under the IS Act
- ministerial authorisations to undertake certain activities
- Director of AGO approvals
- provision of support to the ADF under section 6B(1)(g) of the IS Act
- provision of geospatial products to partners
- a cross-agency inspection of the frameworks and processes for overturned presumptions of nationality.

In some instances, the IGIS provided findings and recommendations based on compliance observations, directed to improving the clarity of, and compliance with, AGO's internal policies and procedures, or to promote stronger compliance practices, particularly in regard to the quality of record keeping. With regard to the inspection of the provision of support to the ADF under section 6B(1)(g) of the IS Act, the IGIS made further specific findings related to the sufficiency of training and guidance material, along with the currency and adequacy of legal advice held about activities undertaken.

Rules to Protect the Privacy of Australians

The Minister for Defence issues written rules – *Rules to Protect the Privacy of Australians* (the Privacy Rules) – to regulate the communication and retention by AGO of intelligence information about Australian persons. In 2023–24, the IGIS undertook one inspection of AGO's application of the Privacy Rules and identified no legality or propriety concerns. The inspection did make a number of recommendations regarding processes for the application of the Privacy Rules and guidance for analysts relating to record keeping. The IGIS will continue its regular review of AGO's implementation of the Privacy Rules in 2024–25.

Compliance incidents

In 2023–24, AGO reported 2 compliance incidents to the IGIS. On further assessment by AGO, both incidents were determined to be compliant.

Compliance with internal foreign release policy

AGO reported one potential instance of noncompliance with its internal foreign release policy where an error was made in the clearance process for the product. The IGIS undertook an independent review of the incident and agreed that the matter was compliant and AGO's response and actions were timely, appropriate and well documented.

Compliance with AGO Privacy Rules

AGO reported one potential instance of noncompliance in the application of the AGO Privacy Rules to an intelligence product. The IGIS reviewed the matter and agreed that the incident was compliant and AGO's response and actions were appropriate.

Other reviews

In addition to inspection activities, the IGIS was also consulted and provided input on potential changes to AGO's Privacy Rules.

Defence Intelligence Organisation

Key statistics



2

Inspections commenced



3

Inspections completed



0

Compliance incidents reported



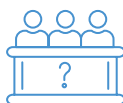
2

Ministerial letters sent to relevant minister



2

Senior-level meetings held



0

Inquiries commenced



0

Inquiries completed

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 the Defence Force.

Relevant Act: *Intelligence Services Act 2001*

Responsible minister: Minister for Defence

Defence Intelligence Organisation

In 2023-24, the IGIS undertook inspections of DIO's activities pursuant to section 9A of the IGIS Act. The IGIS did not commence any inquiries under section 8 of the IGIS Act in relation to DIO.

The IGIS conducted one preliminary inquiry relating to DIO, which is reported on in 'Cross-agency activities' later in this section.

The IGIS implemented a risk-based approach to its inspections of DIO. Due to the nature of DIO's role, the IGIS undertook fewer oversight activities in relation to DIO's activities compared to the activities of other intelligence agencies. In 2023-24, the IGIS focused its inspections on DIO's activities in areas of higher risk or sensitivity.

Two scheduled meetings were held between the Inspector-General, the IGIS's senior leadership team, the Chief of Defence Intelligence and DIO senior executives in November 2023 and June 2024. These meetings were a valuable opportunity to discuss organisational priorities and challenges, along with oversight and inspection activities.

Access to systems, personnel and information

In 2023–24, DIO provided the IGIS 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 to enable the IGIS's oversight activities.

Inspections

The IGIS undertook and completed 2 inspections of DIO's activities in 2023–24.

One inspection that commenced in 2022–23 was completed in 2023–24.

One inspection that was planned to occur in 2023–24 was carried over to the 2024–25 reporting period. This inspection related to a specific program that DIO undertakes with foreign partners.

In one of the 3 completed inspections, the IGIS did not identify legality or propriety concerns. This inspection related to DIO's application of its privacy rules made under the IS Act. A high-level summary of the 3 completed inspections appears below.

Specified program

The IGIS inspected a program of specified activities, which is established and governed by a Five-Eyes Memorandum of Understanding. This inspection followed an earlier inspection of the same program which was completed in March 2022.

This inspection identified propriety concerns, including that activities conducted under the program may be beyond DIO's mandate; that the heavy reliance on foreign partners could introduce additional propriety concerns in the conduct of the program; and that the record-keeping practices associated with the program were deficient. Of further concern for the IGIS was that some of these issues were identified in the 2022 inspection and had not been sufficiently remediated.

The IGIS made several recommendations as a result of the inspection, including that DIO should consider revising its mandate to include the activities conducted within the program. The IGIS provided visibility of its findings and recommendations to the Minister for Defence. In response to the IGIS's findings and recommendations, the Chief of Defence Intelligence wrote to the Inspector-General to outline the remediation action that DIO had already taken or would take. The IGIS will monitor these actions in a future inspection.

Analytic integrity

The IGIS undertook an inspection of DIO's approach to ensuring the analytic integrity of its intelligence assessment products and activities. The purpose of the inspection was to provide assurance that DIO products are analytically rigorous, that DIO processes are transparent and that the resulting intelligence assessments are free from bias and external influence. This inspection focused on the area of intelligence assessment management, as this had been an area of concern in a previous inspection in 2022–23.

Despite progress and improvements since the 2022–23 inspection, the IGIS considered that, within the products reviewed, DIO was unable to consistently demonstrate appropriate analytic integrity. A continuing key area of deficiency related to DIO's product management processes and, in particular, record keeping. The IGIS made a number of findings and recommendations to address identified concerns.

DIO accepted the findings and recommendations and has committed to continuing its efforts to mature its analytical integrity approach. The IGIS will monitor these actions in a future inspection.

Compliance with Rules to protect the privacy of Australian persons

The Minister for Defence issues written rules – *Rules to Protect the Privacy of Australians* (the Privacy Rules) – to regulate the communication and retention by DIO of intelligence information about Australian persons. In 2023–24, the IGIS undertook one inspection of DIO's application of the Privacy Rules and identified no legality or propriety concerns. The inspection confirmed that overall DIO had a strong culture of compliance with the Privacy Rules. The IGIS will continue its regular review of DIO's implementation of the Privacy Rules in 2024–25.

Compliance incidents

DIO did not report any compliance incidents to the IGIS in 2023–24.

Other reviews

In addition to inspection activities, the IGIS reviewed DIO's proposed changes to its mandate.

Australian Criminal Intelligence Commission and Australian Federal Police

Key statistics



4

Inspections commenced



4

Inspections completed



3

Compliance incidents reported



4

Ministerial letters sent to relevant minister



0

Senior-level meetings held



0

Inquiries commenced



0

Inquiries completed

Agency overview

In September 2021, the IGIS's jurisdiction was expanded with the enactment of the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*. The Act provided an additional power, the network activity warrant (NAW), for the Australian Criminal Intelligence Commission (ACIC) and Australian Federal Police (AFP) to identify and disrupt serious online crime. The IGIS has oversight responsibility for this warrant power and undertakes inspections to confirm the legality and propriety of ACIC's and the AFP's activities in obtaining, managing and using NAWs. The IGIS does not have jurisdiction for the broader activities, intelligence or otherwise, of ACIC and the AFP.

Relevant Act: *Surveillance Devices Act 2004*

Responsible minister: Attorney-General

Australian Criminal Intelligence Commission and Australian Federal Police

In 2023–24, the IGIS undertook inspections of ACIC's and the AFP's activities in relation to their use and management of NAWs. The IGIS did not commence any inquiries under section 8 of the IGIS Act in relation to these agencies.

Access to systems, personnel and information

In 2023–24 both agencies provided the IGIS with appropriate access to people and information and the required support to enable the IGIS's oversight activities.

ACIC inspections and compliance matters

Inspections

In the reporting period, the IGIS undertook 2 inspections regarding ACIC's use of NAWs, examining records and policies relating to the applications for, exercise of, and conclusion of all relevant NAWs.

The IGIS did not identify any matters of legality or propriety in the course of these inspections.

Compliance incidents

During the reporting period, ACIC failed to meet the required notification time frame for reporting the extension of a NAW to the Inspector-General pursuant to section 27KQ(7)(b) of the *Surveillance Devices Act 2004* on one occasion.

ACIC also proactively identified that information in relation to NAWs may have been provided to the IGIS pursuant to section 49D of the *Surveillance Devices Act 2004* without an appropriate internal delegation to report to the IGIS being in place. The IGIS notes that ACIC is currently seeking legal advice to clarify this matter and reviewing its delegations with a view to addressing the matter as necessary.

AFP inspections and compliance matters

Inspections

In the reporting period, the IGIS undertook 2 inspections regarding the AFP's use of NAWs, examining records and policies relating to the application for, exercise of, and conclusion of all relevant NAWs. These inspections identified the following compliance incidents.

The IGIS identified a failure by the AFP to comply with its reporting obligations to the Attorney-General pursuant to section 49(2E) of the *Surveillance Devices Act 2004*. The report to the Attorney-General did not include all relevant variations to the NAW and contained inaccurate or incomplete information relating to the end date for data access, the details of premises at which a computer was located, and the details of any use of a surveillance device under the warrant. On identification of this failure, the AFP undertook an internal review of associated processes and undertook remedial actions, including providing updated and accurate information to the Attorney-General.

Compliance incidents

The IGIS identified that the AFP failed to meet the required notification time frames for reporting to the Inspector-General pursuant to section 27KQ(7)(b) of the *Surveillance Devices Act 2004* on 2 occasions, relating to one extension and one variation to NAWs. Following notification and internal review, the AFP identified 3 further instances of noncompliance with this section. These related to 2 extensions and one variation to NAWs. Following identification of these issues, the AFP undertook remedial action. No further failures were identified.

Cross-agency activities

Key statistics



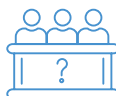
1

Preliminary inquiry
commenced



1

Preliminary inquiry
completed



0

Inquiries
commenced



0

Inquiries
completed

Overview

In 2023–24, there were no inquiries and one own-motion preliminary inquiry that reviewed the activities of multiple agencies. Inspections relating to multiple agencies were also conducted; however, the statistics relating to these are reported against each agency independently.

Cross-agency inspection and inquiry activities

Inquiries

During 2023–24, the IGIS conducted no cross-agency inquiries, one cross-agency preliminary inquiry, and 4 inspections that reviewed the activities of multiple agencies.

Preliminary inquiry

On 24 January 2024, the Inspector-General initiated an own-motion preliminary inquiry into the use of artificial intelligence (AI) by agencies within the national intelligence community. The purpose of the preliminary inquiry was to:

- confirm whether under section 14(2) of the IGIS Act the Inspector-General could, and should, inquire further into the use of AI in the 6 agencies
- provide assurance that the agencies are operating AI systems legally, with propriety and in accordance with human rights
- understand the use of these systems and consider impacts on the IGIS's oversight capabilities.

The preliminary inquiry determined that the Inspector-General is authorised to make further inquiries but that further inquiries were not required. The IGIS did not identify any legality, propriety or human rights concerns with regard to the extant use of AI systems; nor did it identify any drivers for immediate changes to its oversight approach.

The IGIS found that ethical and legal considerations are a foundation of the agencies' AI development strategies and ultimately are considered in the processes of approval for the use of AI systems.

The IGIS found that the NIC's current use of AI is primarily focused on augmenting human capabilities or judgement rather than replacing them with autonomous decision-making. A small number of agencies did express a desire to further explore systems with more autonomy, but to do so in a considered manner.

The IGIS made 3 recommendations that encouraged agencies to continue investing in national AI policy discussions and adapting their AI governance, auditability, transparency and explainability capabilities at the same time as investing in the potential operational opportunities of AI.

The IGIS published the report to its website at www.igis.gov.au/resources/publications.

Inspections

During 2023–24, the IGIS undertook 4 cross-agency inspection activities, looking into agency activities related to:

- compliance with the Crimes Act requirements for annual reporting on use and management of assumed identities
- compliance frameworks and processes for overturned presumptions of nationality when undertaking intelligence activities
- compliance frameworks and procedures in ASIO and ASIS for the management of notices issued under section 13B of the IS Act
- practices and procedures for managing compliance incidents relating to a particular intelligence collection warrant issued by the Attorney-General.

Use and management of assumed identities

The Crimes Act imposes reporting, administrative and audit regimes on agencies that use assumed identities. Section 15LG of the Crimes Act requires ASIO, ASIS, ASD and ONI to conduct 6-monthly audits of assumed identity records. Section 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 IGIS conducted reviews of the assumed identities annual reporting provided by ASIO, ASIS, ASD and ONI for 2022–23. As agencies' reporting for 2023–24 will cover the creation and use of assumed identities up to 30 June 2024, this reporting is not available to the IGIS in the current reporting period and will be reported in 2024–25.

- ASIO's annual reporting did not identify any issues related to its use and management of assumed identities.
- ASIS's annual reporting did not identify any issues related to its use and management of assumed identities.
- ASD did not authorise any assumed identities in 2022–23.
- ONI's annual reporting did not identify any issues related to its use and management of assumed identities.

Where applicable, compliance incidents and inspection activities relating to the use and management of assumed identities by ASIO, ASIS, ASD and ONI are described earlier in this report in the sections detailing the oversight activities for each agency.

Overtaken presumptions of nationality

In October 2023, the IGIS commenced an inspection of multiple agencies' (ASIS, ASD and AGO) compliance frameworks and processes for overturned presumptions of nationality (OPNs).

The foreign intelligence collection agencies in the IGIS's jurisdiction all have restrictions on collecting intelligence on Australian persons and entities. In order to operationalise those restrictions, the agencies must make presumptions about an individual's or entity's nationality based on the information they have available to them at the time. Overturning a presumption of nationality is when, on obtaining further information, an agency changes its previous presumption, which will ultimately affect what intelligence it can collect or retain about the person.

This inspection had 3 primary purposes:

- to understand how agencies notify each other when overturning a presumption of nationality and to determine the effectiveness and timeliness of these arrangements
- to determine whether the agencies' internal policies, frameworks and knowledge management systems are fit for purpose for managing OPNs
- to identify if agencies appropriately communicate OPN decisions to the IGIS, in accordance with policy and legislative requirements.

The IGIS did not identify any breaches of legislation or policy or identify any propriety concerns in conducting this inspection.

The IGIS confirmed there was, in general, timely notification of OPNs between agencies.

The IGIS noted that a variety of systems and databases were used across the agencies to manage the storage and communication of nationality decisions. The IGIS recommended that agencies consider whether these databases and systems should include a central repository for capturing OPN decisions.

The IGIS noted that all agencies recognised the importance of having internal guidance/policies available for analysts to assist with the management of OPN decisions. However, there was some variability in the availability of these guides and whether they were in draft or finalised.

ASIO and ASIS compliance frameworks and practices relating to 13B notices

In January 2024, the IGIS commenced an inspection of ASIO and ASIS regarding compliance frameworks and processes for the management of notices issued under section 13B of the IS Act. The IGIS selected a sample of 13B notices issued between 1 January 2021 and 30 November 2023.

The inspection focused on 3 key areas:

- to understand how both agencies coordinate the management of section 13B notices and to determine the effectiveness of these arrangements
- to determine whether the agencies' internal policies, frameworks and knowledge management systems are fit for purpose for managing section 13B notices
- to identify if agencies appropriately met the legislative requirements associated with section 13B notices.

The IGIS did not identify any breaches of legislation or policy and did not identify any propriety concerns. The IGIS did make a range of observations and recommendations to ASIO and ASIS about opportunities to improve governance and compliance processes and practices to ensure that compliance with legislation and policy can be more effectively demonstrated.

Managing compliance incidents in relation to a warranted collection activity

At the end of 2023–24, the IGIS's inspection of multiple agencies in relation to a warranted collection activity remained underway. Relevant findings and recommendations will be reported in the 2024–25 Annual Report.

Complaints and public interest disclosures

Key statistics



64

IGIS Act complaints received*



1

PID Act disclosures allocated



655

Other correspondence handled^

* Includes one matter that is under assessment to determine whether it meets the threshold to be a PID Act disclosure

^ Includes purported complaints that did not fall within the jurisdiction of the IGIS Act or PID Act

The Inspector-General has a broad jurisdiction to receive and inquire into complaints and investigate disclosures concerning the conduct of ASIO, ASIS, ASD, AGO, DIO and ONI, and of ACIC and the AFP in relation to their intelligence functions regarding network activity warrants (NAWs).

Matters that are brought to the Inspector-General may fall within the jurisdiction of the IGIS Act or the PID Act, or both. The Inspector-General also receives a large number of complaints and other correspondence that do not fall within the jurisdiction of either Act. 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 the Inspector-General’s jurisdiction. Staff assisting the Inspector-General review all correspondence received to determine whether a matter falls within the jurisdiction of the IGIS Act or the PID Act.

Table 6.1: Complaints and PID statistics

	2023-24 FY (1 July 2023 – 30 June 2024)	2022-23 FY (1 July 2022 – 30 June 2023)	2021-22 FY (1 July 2021 – 30 June 2022)
Complaints within the jurisdiction of the IGIS Act	64	34	80
Visa and citizenship complaints	40	70	141
PID Act disclosures allocated	1	6	10
Other correspondence not within the jurisdiction of the IGIS Act or PID Act*	655	599	431

* Each of these matters usually involves more than one item of correspondence or phone call with staff assisting the Inspector-General.

Complaints

Non-visa and citizenship related complaints

The number of complaints received in 2023–24 was 64. This is greater than the number of complaints in 2022–23 (34) and fewer than the number of complaints received in 2022–21 (80).

Table 6.2: Complaints received by agency

Agency	Number of complaints
ASD	15
ASIO	41
ASIS	7
DIO	1

Staff assisting the Inspector-General sought complaints-related information from agencies by requesting information, speaking with relevant agency staff, reviewing files and undertaking independent searches of agency databases to identify issues of legality or propriety. Most matters were 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:

- data breaches and information sharing
- recruitment and organisational suitability assessments
- employment grievances
- agency misconduct and surveillance
- processes for conducting security assessments for government functions
- agency inaction
- analytic integrity and related processes.

In response to the complaints received in the reporting period, the Inspector-General:

- commenced 32 preliminary inquiries
- commenced one inquiry.

In addition, the Inspector-General:

- commenced 3 preliminary inquiries in response to complaints received in the previous reporting period
- commenced an inquiry in response to a complaint received in a previous reporting period
- commenced an inquiry in response to a public interest disclosure made to the IGIS (see ‘Public Interest disclosures’)
- commenced one own-motion preliminary inquiry after receiving a number of complaints about a matter (see ‘Own-motion preliminary inquiries’).

The intelligence agencies provided information and documents to the Inspector-General in response to those preliminary inquiries and inquiries. At the conclusion of each preliminary inquiry and each inquiry, the intelligence agencies were notified of the Inspector-General's or delegate's decision to finalise the matter, and any findings or recommendations for their further consideration and action.

In the reporting period, the Inspector-General closed 64 complaint matters. Of these, 47 were received in the 2023–24 reporting period and 17 were received in a previous reporting period. The 64 matters were closed on the following grounds:

- section 11(2)(a) of the IGIS Act – one matter
- section 11(2)(c) of the IGIS Act – 62 matters
- completion of inquiry under Part II, Division 3 of the IGIS Act – one matter (see 'Complaints inquiries').

In this reporting period, the Inspector-General prepared 3 reports to agencies under section 25B of the IGIS Act at the conclusion of preliminary inquiries, making a total of 5 recommendations. All of these recommendations were accepted and actioned by the relevant agencies.

At the conclusion of the reporting period, 20 complaints remained open. This included 17 complaints received in the reporting period and 3 received in a previous reporting period.

During the reporting period, the Inspector-General did not employ any person under subsection 32(3) of the IGIS Act or delegate powers set out under subsection 32AA(1) of the IGIS Act

Visa and citizenship application complaints

The Inspector-General also receives complaints concerning the processing of visa and citizenship applications, particularly regarding the length of time taken to finalise applications. However, the Inspector-General's jurisdiction only extends to cases where the delays are a result of processes or practices within the intelligence agencies over which the Inspector-General has jurisdiction.

The Inspector-General did not identify any systemic compliance issues in the visa and citizenship complaints reviewed in 2023–24.

Own-motion preliminary inquiries

As previously reported in 2022–23, the Inspector-General commenced an own-motion preliminary inquiry on 23 January 2023 into ASD's administration of PIDs under the PID Act. That preliminary inquiry remains ongoing as at the end of this reporting period.

In July 2023, the Inspector-General received a number of complaints relating to a data breach by ASIO. The data breach occurred when ASIO sent a group email to unsuccessful job applicants in which all of the applicants' email addresses were visible to all other recipients. In response to those complaints, the Inspector-General commenced an own-motion preliminary inquiry on 7 August 2023.

The preliminary inquiry was concluded during the reporting period with the Inspector-General issuing a report to ASIO under section 25B of the IGIS Act. In deciding that further inquiry was not warranted, the Inspector-General found that the data breach was the result of human error and was satisfied that ASIO had identified steps to prevent similar incidents in the future. In addition, the Inspector-General made 2 recommendations to ASIO.

Complaints inquiries

During the reporting period, the Inspector-General concluded the inquiry into a complaint made by Mr Daniel Duggan in relation to ASIO. The Inspector-General concluded that none of the allegations in Mr Duggan's complaint raised issues of legality or propriety. During the course of this inquiry, the Inspector-General identified one other activity that transcended the bounds of propriety in one respect, and communicated this issue to the relevant minister and agency. ASIO amended relevant procedures in response to this issue.

The Inspector-General also commenced inquiries into 2 complaints, one of which was received in the previous reporting period. These inquiries were ongoing as at 30 June 2024.

Public interest disclosures

The Inspector-General has key responsibilities under the PID Act, including:

- receiving, allocating 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
- overseeing the operation of the PID scheme in the intelligence agencies.

As at 30 June 2024, some matters which have been raised with the Inspector-General are being considered as potential PIDs. It is not always apparent when a matter is first raised with the Inspector-General whether the reporting person is 'a public official' within the definition of the PID Act, and it may not be clear whether the conduct would meet the threshold for 'disclosable conduct'. If these matters are considered to be PIDs, they will be reported on in the next reporting period.

In the reporting period, the Inspector-General assessed 16 matters that resulted in a decision not to allocate the disclosure. A decision not to allocate was made in 11 instances because the conduct was not disclosable conduct (personal work-related grievances); in 4 instances because the conduct was not disclosable conduct (conduct other than personal work-related grievances); and in one instance because the person making the disclosure (which related to alleged maladministration) was not a public official.

During the reporting period, the Inspector-General allocated one disclosure relating to an intelligence agency to the Office for investigation. The matter that was the subject of the allocation decision was raised with the Inspector-General in the previous reporting period. It was found to meet the threshold to be a PID – and allocated to the Inspector-General – in 2023–24. This matter relates to alleged maladministration. Following the allocation decision, the Inspector-General exercised his power under section 49(1) of the PID Act to decide not to investigate the matter under the PID Act. Instead, the Inspector-General commenced an inquiry under the IGIS Act. That inquiry is ongoing.

Two disclosures allocated to the IGIS in 2022–23 were still under investigation as at 30 June 2024.

At the end of 2023–24, the Inspector-General's office had 20 authorised officers under the PID scheme; this includes the Inspector-General, who is also the principal officer. These authorised officers were contactable via secure email and phone.

The Inspector-General did not allocate any disclosures to the intelligence agencies for investigation in the reporting period. No disclosures were allocated to the Inspector-General by an intelligence agency.

Overseeing the operation of the PID scheme in the intelligence agencies

In accordance with section 44(1A)(b) of the PID Act, intelligence agencies – and ACIC and the AFP in relation to their intelligence functions regarding NAWs – are required to report to the Inspector-General about PIDS. This includes informing the Inspector-General when a PID is allocated to an intelligence agency (or ACIC and the AFP where relevant) for investigation and when an investigation is completed.

The Inspector-General was notified of 7 PIDs received by the intelligence agencies or by ACIC or the AFP during the reporting period. In one instance an agency decided to reallocate a disclosure to another agency because the conduct did not relate to the intelligence agency.

The agencies advised the Inspector-General of the actions taken in each matter and discussed PID-related issues with IGIS staff as necessary.

In total, intelligence agencies informed the Inspector-General that they completed investigating 5 disclosures. This included the completion of one investigation of a disclosure allocated by an agency in 2022–23.

Of the 5 completed investigations, 3 were completed within 90 days and 2 were completed in 91 to 180 days. For both investigations that exceeded 90 days, the relevant agencies sought and obtained extensions from the Inspector-General in accordance with section 52(4)(d) of the PID Act. In the course of conducting the 5 completed investigations, the agencies identified no claims or evidence of detrimental action taken against the discloser; nor did the agencies receive any complaints about reprisals, outside of the investigative process, during the reporting period.

The 7 disclosures received in the reporting period concerned 12 instances of suspected disclosable conduct. One investigation found at least one finding of disclosable conduct, and 4 investigations were finalised with no findings of disclosable conduct. Of these investigations, one resulted in a recommendation that the matter be referred for investigation under section 47(3) of the Act. Two investigations commenced by intelligence agencies in the reporting period remain ongoing.

The intelligence agencies reported that they did not assess any matters that resulted in a decision not to allocate a disclosure during the reporting period.

The Inspector-General also has statutory responsibilities for assisting intelligence agency staff in their obligations under the PID Act and for conducting education and awareness-raising exercises. During the reporting period, the Inspector-General's staff provided assistance and guidance to officials within the intelligence agencies about the operation of the scheme. The Inspector-General's staff also alerted agencies to PID Act training courses and relevant fora that may be of interest to their officials.

Section Seven

Annexures



Annexure 7.1

Other mandatory information

Section 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 section 311A of the *Commonwealth Electoral Act 1918*.

The IGIS 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 section 516A of the *Environment Protection and Biodiversity Conservation Act 1999*.

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

Through its co-location with AGD, the IGIS 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 IGIS premises at 3-5 National Circuit, Barton, ACT.

Utilities consumption for the IGIS was not separately measured. For this reason, ecologically sustainable development and details of environmental performance cannot be quantified in this annual report.

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

- 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 2023-24 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 IGIS's tenancy arrangement with AGD, the IGIS 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 IGIS's electricity, natural gas and waste emissions will be included in AGD's emissions reporting.

Table 7.1: Greenhouse gas emissions inventory – location-based method 2023-24

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	-	-
Solid Waste*	N/A	N/A	-	-
Refrigerants*†	-	N/A	N/A	-
Fleet and other vehicles	0.214	N/A	0.054	0.268
Domestic Commercial flights	N/A	N/A	7.026	7.026
Domestic Hire Car*	N/A	N/A	0.024	0.024
Domestic Travel Accommodation*	N/A	N/A	4.988	4.988
Other energy	-	N/A	-	-
Total kg CO₂-e	0.214	-	12.092	12.306

Note: the table above presents emissions related to electricity usage using the location-based accounting method.
CO₂-e = Carbon Dioxide Equivalent.

* indicates emission sources collected for the first time in 2023-24. The quality of data is expected to improve over time as emissions reporting matures.

† indicates optional emission source for 2023-24 emissions reporting.

Table 7.2: Electricity greenhouse gas emissions 2023–24

Emission source	Scope 12 t CO ₂ -e	Scope 3 t CO ₂ -e	Total t CO ₂ -e	Percentage of electricity use
Electricity (location-based approach)	-	-	-	0.00%
Market-based electricity emissions	-	-	-	0.00%
Total renewable electricity	-	-	-	0.00%
<i>Mandatory renewables 1</i>	-	-	-	0.00%
<i>Voluntary renewables 2</i>	-	-	-	0.00%

Note: the table above presents emissions related to electricity usage using both the location-based and the market-based accounting methods. CO₂-e = Carbon Dioxide Equivalent.

1 Mandatory renewables are the portion of electricity consumed from the grid that is generated by renewable sources. This includes the renewable power percentage.

2 Voluntary renewables reflect the eligible carbon credit units surrendered by the entity. This may include purchased large-scale generation certificates, power purchasing agreements, GreenPower and the jurisdictional renewable power percentage (ACT only).

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.	Mandatory	iv–v
17AJ(b)	Annexures	Alphabetical index.	Mandatory	136–142
17AJ(c)	Preliminaries	Glossary of abbreviations and acronyms.	Mandatory	vii–viii
17AJ(d)	Annexures	List of requirements.	Mandatory	127–135
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	6
17AE(1)(a)(ii)	Section 2	A description of the organisational structure of the entity.	Mandatory	11

PGPA Rule Reference	Part of Report	Description	Requirement	Page
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	7
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	36
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	16-27
17AD(c)(ii)	Report on Financial Performance			
17AF(1)(a)	Section 5	A discussion and analysis of the entity's financial performance.	Mandatory	51-78
17AF(1)(b)	Section 5	A table summarising the total resources and total payments of the entity.	Mandatory	77-78

PGPA Rule Reference	Part of Report	Description	Requirement	Page
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 and corruption systems).	Mandatory	46
17AG(2)(b)(i)	Preliminaries	A certification by accountable authority that fraud and corruption risk assessments have been conducted and fraud and corruption 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 and corruption that meet the specific needs of the entity are in place.	Mandatory	iii
17AG(2)(b)(iii)	Preliminaries	A certification by accountable authority that all reasonable measures have been taken to deal appropriately with fraud and corruption 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	38–46

PGPA Rule Reference	Part of Report	Description	Requirement	Page
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	39
17AG(2A)(b)	Section 4	The name of each member of the entity's audit committee.	Mandatory	39–41
17AG(2A)(c)	Section 4	The qualifications, knowledge, skills or experience of each member of the entity's audit committee.	Mandatory	39–41
17AG(2A)(d)	Section 4	Information about the attendance of each member of the entity's audit committee at committee meetings.	Mandatory	39–41
17AG(2A)(e)	Section 4	The remuneration of each member of the entity's audit committee.	Mandatory	39–41
External Scrutiny				
17AG(3)	Section 4	Information on the most significant developments in external scrutiny and the entity's response to the scrutiny.	Mandatory	47
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	47
17AG(3)(c)	n/a	Information on any capability reviews on the entity that were released during the period.	If applicable, mandatory	n/a

PGPA Rule Reference	Part of Report	Description	Requirement	Page
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	30-31
17AG(4)(aa)	Section 4	<p>Statistics on the entity's employees on an ongoing and non-ongoing basis, including the following:</p> <p>(a) statistics on full-time employees;</p> <p>(b) statistics on part-time employees;</p> <p>(c) statistics on gender</p> <p>(d) statistics on staff location</p>	Mandatory	33-34
17AG(4)(b)	Section 4	<p>Statistics on the entity's APS employees on an ongoing and non-ongoing 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	33-34
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	35
17AG(4)(c)(i)	Section 4	Information on the number of SES and non-SES employees covered by agreements etc identified in paragraph 17AG(4)(c).	Mandatory	35
17AG(4)(c)(ii)	Section 4	The salary ranges available for APS employees by classification level.	Mandatory	34
17AG(4)(c)(iii)	Section 4	A description of non-salary benefits provided to employees.	Mandatory	35

PGPA Rule Reference	Part of Report	Description	Requirement	Page
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
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	47
Purchasing				
17AG(6)	Section 4	An assessment of entity performance against the <i>Commonwealth Procurement Rules</i> .	Mandatory	48
Reportable consultancy contracts				
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	48
17AG(7)(d)	Section 4	A statement that "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."	Mandatory	48

PGPA Rule Reference	Part of Report	Description	Requirement	Page
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	49-50
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	50

PGPA Rule Reference	Part of Report	Description	Requirement	Page
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	50
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	48
17AG(10)(b)	Section 4	An outline of the ways in which the procurement practices of the entity support small and medium enterprises.	Mandatory	48
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	51-78

PGPA Rule Reference	Part of Report	Description	Requirement	Page
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	36
17AD(f)	Other Mandatory Information			
17AH(1)(a)(i)	n/a	If the entity conducted advertising campaigns, a statement that <i>"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."</i>	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	124
17AH(1)(b)	n/a	A statement that <i>"Information on grants awarded by [name of entity] during [reporting period] is available at [address of entity's website]."</i>	If applicable, mandatory	n/a
17AH(1)(c)	Section 4	Outline of mechanisms of disability reporting, including reference to website for further information.	Mandatory	37
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	47
17AH(1)(e)	Section 1	Correction of material errors in previous annual report	If applicable, mandatory	4
17AH(2)	Section 4 Section 6 Annexures	Information required by other legislation	Mandatory	37, 79-122, 124-126

Index

A

- abbreviations, vii–viii
- accountable authority, 16, 38
- Accountable Authority Instructions, 48
- acknowledgement of Country, ii
- address and contact information, ii
- Administrative Appeals Tribunal (AAT), 13
- advertising and market research, 124
- AGO *see* Australian Geospatial-Intelligence Organisation (AGO)
- analytic integrity, 83, 110, 119
- ANAO *see* Australian National Audit Office (ANAO)
- annual performance statement
 - accountable authority statement, 16
 - reporting framework, 17
 - results:
 - Objective 1: Inquiries, 18–20
 - Objective 2, Inspections, 20–21
 - Objective 3, Complaints, 22–23
 - Objective 4, Public interest disclosures, 24–25
 - Objective 5, Assurance, 26–27
- annual report corrections, 4
- anti-corruption commission *see* National Anti-Corruption Commission
- Anti-Discrimination and Human Rights Legislation Amendment (Respect at Work) Act 2022*, 2
- Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, 104
- APS *see* Australian Public Service (APS)
- Archives Act 1983*, 6, 13
- artificial intelligence, 2, 9, 12, 114–115
- ASD *see* Australian Signals Directorate (ASD)
- ASIO *see* Australian Security Intelligence Organisation (ASIO)
- ASIS *see* Australian Secret Intelligence Service (ASIS)
- asset management, 47
- Assistant Inspectors-General, 11, 36
- assumed identities, 88, 92, 105, 115
- assurance
 - assisting ministers, 12
 - assuring ministers and parliament, 9, 12–13, 17
 - expert evidence to AAT or OAIC, 13
 - informing the public, 9, 10, 17, 26–27, 47
 - performance results and analysis, 26–27
 - see also* ministers; parliamentary committees
- Attorney-General, 3, 8, 12, 112
 - AFP reporting obligations, 113
 - ASIO reporting obligations, 87, 88, 89, 92, 93
 - IGIS reports provided to, 12, 20
 - powers, 84
 - warrants, 92, 93, 115
- Attorney-General's Department, 3, 30, 41, 42
 - IGIS office co-location with, 42, 124
- Audit Committee, 37, 39–41, 45
- Auditor-General, 19 *see also* Australian National Audit Office (ANAO)
- audits
 - financial statements audit report, 47, 52–53
 - internal, 40, 45
- AusTender, 48, 50
- AUSTRAC information, 104
- Australian Criminal Intelligence Commission (ACIC), 6, 112–113, 118, 122
- Australian Cyber Security Centre (ACSC), 100
- Australian Defence Force (ADF), 100, 109 *see also* Defence Intelligence Organisation (DIO); Department of Defence
- Australian Federal Police (AFP), 6, 112–113, 118, 122
- Australian Geospatial-Intelligence Organisation (AGO), 3, 6, 106–108
 - complaints against *see* complaints
 - compliance incidents, 108
 - IGIS engagement with, 106, 107
 - IGIS role in respect of, 6
 - inspections, 106–107
 - key statistics, 106
 - legislation and responsible minister, 106
 - overview, 106
 - privacy rules changes, 108
 - privacy rules compliance, 107, 108
 - public interest disclosures, 118, 121–122
 - record keeping, 107
- Australian Human Rights Commission, 42
- Australian Human Rights Commission Act 1986*, 42
- Australian Information Commissioner, 13, 42
- Australian National Audit Office (ANAO), 47
 - access clauses in contracts, 50
 - financial statements audit report, 47, 52–53
- Australian National University, National Security College, 31, 42

- Australian persons' privacy protections *see* Privacy Rules
- Australian Public Service (APS)
 - APS Academy, 30
 - APS Census Action Plan, 3, 31
 - APS Values, Employment Principles and Code of Conduct, 30
 - Net Zero 2030 emissions reporting, 125–126
 - Public Service Act 1999*, 35
- Australian Public Service Commissioner, 3
- Australian Secret Intelligence Service (ASIS), 3, 6, 95–99
 - assumed identities, 115
 - complaints against, 119 *see also* complaints
 - compliance incidents, 98
 - human rights procedures, 96, 97
 - IGIS engagement with, 95, 96
 - IGIS role in respect of, 6
 - inquiries, 95
 - inspections, 95, 96–97
 - key statistics, 95
 - legislation and responsible minister, 95
 - ministerial directions, 95
 - notification of overturned presumptions of nationality (OPN), 98–99
 - operational files, 97
 - overview, 95
 - Privacy Rules non-compliance, 98–99
 - public interest disclosures, 118, 121–122
 - record keeping, 96, 97, 98
 - weapons use, 96, 97
- Australian Security Intelligence Organisation (ASIO), 3, 6, 84–94
 - assumed identities, 88, 92, 115
 - complaints against, 119, 120–121 *see also* complaints
 - compliance incidents, 89–94
 - device access orders, 87
 - foreign intelligence collection, 84, 88
 - human source management, 86
 - IGIS engagement with, 85
 - IGIS role in respect of, 6, 7
 - inquiries, 85
 - inspections, 84–88
 - key statistics, 84
 - legislation and responsible minister, 84
 - ministerial directions, 7
 - Minister's Guidelines, 84, 88
 - non-compliance with Minister's Guidelines, 85, 87–88, 91, 92, 94
 - overview, 84
 - public interest disclosures, 118, 121–122
 - record keeping, 86, 87, 88
 - retained items, 87
 - security assessments, 87
 - special intelligence operations, 84, 89
 - use of powers, 89
 - warrants, 88, 89, 90–91, 93
- Australian Security Intelligence Organisation Act 1979* (ASIO Act), 12, 13, 84
 - device access orders, 87
 - foreign intelligence collection function, 88
 - non-compliance, 91–92, 93
 - record keeping requirements, 88
 - use of force notifications, 89
- Australian Signals Directorate (ASD), 3, 6, 100–105
 - assumed identities, 105, 115
 - complaints against, 119, 120 *see also* complaints
 - compliance incidents, 102–105
 - IGIS engagement with, 100, 101
 - IGIS role in respect of, 6
 - inquiries, 100
 - inspections, 100, 101–102
 - key statistics, 100
 - legislation and responsible minister, 100
 - ministerial authorisations, 100, 101, 104, 105
 - overturned presumptions of nationality (OPN), 102–103
 - overview, 100
 - preliminary inquiries, 101
 - privacy rules changes, 105
 - privacy rules compliance, 102
 - Project REDSPICE, 100
 - public interest disclosures, 118, 121–122
 - record keeping, 102, 105
 - Responsible Release Framework for Cyber Security Vulnerabilities, 102
- Australian Transaction Reports and Analysis Centre (AUSTRAC), 104

B

- Bogaart, Karla, 39
- Brookes, Chris, 11, 36
- Business Continuity Plan, 45

C

Canada

National Security and Intelligence Review Agency, 44

capability reviews

Oversight Capability Review, 3, 31–32

Census Action Plan, 2, 31

Chief of the Defence Force, 110

citizenship application-related complaints, 2, 4, 23, 118, 120

committees, 38–41

Commonwealth Contracting Suite, 48, 50

Commonwealth Fraud Control Framework 2024, 46

Commonwealth Indigenous Procurement Policy, 48

Commonwealth Ombudsman, 19, 20, 43, 47

Commonwealth Procurement Rules, 48

communications interception *see*

Telecommunications (Interception and Access) Act 1979 (TIA Act)

complaints, 2, 6

agencies, 119

IGIS function and powers, 9, 118–121

inquiries, 119–120, 121

non-visa related, 119–120

own-motion preliminary inquiries, 120

performance results and analysis, 22–23

statistics, 4, 23, 118, 119

visa or citizenship related, 4, 23, 118, 120

compliance discipline, 2, 80

compliance incidents, 4, 8, 20, 117

ACIC, 113

AFP, 113

AGO, 108

ASD, 103–105

ASIO, 89–94

ASIS, 98

DIO, 111

ONI, 83

Comprehensive Review of the Legal Framework of the National Intelligence Community (Richardson Review), 32

consultants, 48–49

consultative processes, 30

contact information, ii

contracts, 48–50

convictions

spent conviction information, 93–94

Cook, Katherine, 36

corporate governance, 3, 38–41

Corporate Plan, 16, 17, 18

corporate support, 41, 42

corrections to previous annual reports, 4

correspondence handled, 118

corruption *see* ethical standards; fraud control

Crimes Act 1914, 115

assumed identities reporting, 115

non-compliance, 88, 92, 93–94, 104

Cronan, Paul, 11, 36

cross-agency inspection and inquiry activities, 114–117

cyber security, 100, 102

D

data collection and retention, 104 *see also*

Telecommunications (Interception and Access) Act 1979 (TIA Act)

Defence Intelligence Organisation (DIO), 3, 6, 109–111

analytic integrity, 110

complaints against, 119 *see also* complaints

compliance incidents, 111

IGIS engagement with, 109, 110

IGIS role in respect of, 6

inspections, 110–111

key statistics, 109

legislation and responsible minister, 109

overview, 109

privacy rules compliance, 111

public interest disclosures, 118, 121–122

record keeping, 111

specified program, 110

definitions, vii–viii

Department of Defence, 106, 109

Secretary of Defence, 18, 19, 109

see also Minister for Defence

Deputy Inspectors-General, 11, 36

device access orders, 87

DIO *see* Defence Intelligence Organisation (DIO)

Director of AGO, 107

Director-General of Security, 88, 91–92, 93

authorisations, 85

disability reporting, 37

disclosures

public interest *see* public interest disclosures

diversity and inclusion initiatives, 30

Duggan, Daniel, 121

E

ecologically sustainable development and
environmental performance, 124
emissions reporting, 125–126
employees *see* staff
enterprise agreement, 3, 35
entity resource statement, 77–78
ethical standards, 10, 30, 46 *see also* fraud control
Executive Board, 30, 31, 37, 38, 45
Executive Director, Enterprise Management Unit,
11, 36
executives *see* Key Management Personnel; Senior
Executive Service officers
exempt contracts, 50
expenses for outcome, 78
expert evidence to AAT or OAIC, 13
external scrutiny of IGIS, 47–50

F

financial services, 42
financial statements, 54–78
audit report, 47, 52–53
entity resource statement, 77–78
firearms *see* weapons use
Five-Eyes Intelligence Oversight and Review
Council (FIORC), 3, 27, 43–44
Five-Eyes Memorandum of Understanding, 110
force
use-of-force notifications, 89
foreign intelligence collection, 84, 88, 100, 116
Fraud and Corruption Control Plan and Guidance, 3
fraud control, iii, 3, 45, 46
Freedom of Information Act 1982, 6, 13, 47, 50
functions *see* roles and functions

G

geospatial intelligence agency *see* Australian
Geospatial-Intelligence Organisation (AGO)
governance *see* corporate governance;
information governance framework
Governance Directorate, 45
greenhouse gas emissions reporting, 125–126

H

health *see* workplace health and safety
human resources management *see* staff
human rights, 7, 8, 17, 19, 21, 42, 83, 114
legislation, 2
non-compliance with procedures, 96, 97
human source management, 86

I

identities, assumed, 88, 92, 104, 115
Indigenous businesses, commitment to, 48
information and communications technology (ICT),
42
information governance framework, 3
Information Publication Scheme, 47
information security authority *see* Australian
Signals Directorate (ASD)
innovation program, 31
inquiries, 2, 4, 6, 8
ASD, 100, 101
ASIO, 85
ASIS, 95
complaints inquiries, 2, 119–120
cross-agency, 114–115
notification and reporting requirements, 12
performance results and analysis, 18–20
preliminary inquiries, 2, 8, 9, 12, 101, 114
inquiries by parliamentary committees *see*
parliamentary committees
inspections, 2, 4, 6, 8
ACIC, 112–113
AFP, 112–113
AGO, 106–107
ASD, 100, 101–102
ASIO, 86–88
ASIS, 95–97
cross-agency, 114–117
DIO, 109–111
ONI, 81, 82–83
performance results and analysis, 20–21
see also compliance incidents
Inspector-General of Intelligence and Security
approach, 10
investigative powers, 6
key activities, 8–9
letter of transmittal, iii
organisation chart, 11
Oversight Capability Review, 3, 31–32
purpose, 7–10, 12, 17
remuneration, 35–36
review of year, 2–3
role and functions, 2, 6, 8–10, 12–13, 112, 118–122
statutory office holder, 35
Technical Advisor, 3, 32
Inspector-General of Intelligence and Security Act
1986, iii, 2, 6, 7, 8, 12, 13, 16, 17, 19–25, 118

complaints handling *see* complaints
 inquiries *see* inquiries
 inspections *see* inspections
Inspector-General of Intelligence and Security and Other Legislation Amendment (Modernisation) Act 2023, 2
 Integrity Agencies Group, 3, 42
 intelligence agencies
 human rights obligations, 7, 8, 17, 19, 21, 42, 83, 96, 97, 114
 IGIS engagement with, 2, 3, 9, 26–27, 80
 IGIS oversight of (list of agencies), 6 *see also* Inspector-General of Intelligence and Security
 public interest disclosure obligations, 122
 record keeping *see* record keeping
 use of artificial intelligence, 9, 12, 114–115
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); and Australian Criminal Intelligence Commission (ACIC); Australian Federal Police (AFP)
Intelligence Services Act 2001, 95, 100, 106, 109
 ASIO and ASIS compliance, 116–117
 non-compliance, 98, 104–105
 privacy rules *see* Privacy Rules
Intelligence Services Legislation Amendment Bill 2023, 12, 13
 internal audit, 40, 45
 international engagement, 3, 27, 43–44

J

Jessup, Christopher, 11, 36 *see also* Inspector-General of Intelligence and Security

K

Key Management Personnel, 35, 36, 71

L

leadership development, 30–31
 learning and development, 30–31, 46
 legislation governing intelligence agencies, 81, 84, 95, 100, 106, 109, 112
 legislative reviews and changes, 2, 12–13, 26
 letter of transmittal, iii

M

market research, 124
 Minister for Defence, 100, 102, 106, 107, 109, 110, 111
 Minister for Foreign Affairs, 95, 97
 Minister for Home Affairs, 84
 ministerial authorisations, 95, 100, 101, 104, 105, 106, 107
 ministerial directions, 7, 17, 95, 100, 101, 106
 ministerial letters, 23, 81, 84, 95, 100, 106, 109, 112
 ministers
 reporting to, 12, 17, 19–23, 26–27
 requests from, 8, 12
 responsible for intelligence agencies, 81, 84, 95, 100, 106, 109, 112
 Minister's Guidelines to ASIO, 84, 88
 non-compliance, 85, 87–88, 91, 92, 94
 Moore, Stephen, 40

N

National Anti-Corruption Commission, 42
National Anti-Corruption Commission Act 2022, 2
 National Intelligence Academy, 30
 National Intelligence Community, 2, 28, 84
 Comprehensive Review of the Legal Framework of the National Intelligence Community (Richardson Review), 32
 use of artificial intelligence, 114–115
 see also intelligence agencies
 National Museum of Australia, Cultural and Corporate Shared Services Centre, 42
 National Security and Intelligence Review Agency (Canada), 44
 National Security College, 31, 42
National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Act 2022, 88
National Security Legislation Amendment (Comprehensive Review and Other Measures No. 2) Act 2023, 93
National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023, 13
 nationality
 overturning a presumption of nationality (OPN), 97–98, 99, 116
 Net Zero 2030 emissions reporting, 125–126
 network activity warrants (NAWS), 6, 112, 113, 118, 122
 non-compliance with law, standards or procedures

see compliance incidents
non-consultancy contracts, 50
non-salary benefits, 35 *see also* remuneration
Notzon-Glenn, Bronwyn, 36

O

Office of National Intelligence (ONI), 3, 6, 81–83, 118
analytic integrity, 83
assumed identities, 115
compliance incidents, 83
IGIS engagement with, 81, 82
IGIS role in respect of, 6
inspections, 81, 82–83
internal security investigations, 82
key statistics, 81
legislation and responsible minister, 81
overview, 81
privacy rules compliance, 82
public interest disclosures, 118, 121–122
record keeping, 83
Office of National Intelligence Act 2018, 81, 82, 83
Office of the Australian Information Commissioner, 13, 42
Office of the Commonwealth Ombudsman, 19, 20, 43, 47
Office of the Inspector-General of Intelligence and Security *see* Inspector-General of Intelligence and Security
ONI *see* Office of National Intelligence (ONI)
organisation chart, 11
organisational profile, 33–37
outcome, 17
resources for outcome, 77–78
see also annual performance statement
Oversight Capability Review, 3, 31–32
overturning a presumption of nationality (OPN), 98–99, 102, 116

P

parliamentary committees
IGIS submissions and appearances, 3, 12–13, 26–27, 47
Parliamentary Joint Committee on Intelligence and Security (PJICIS)
IGIS submissions and appearances, 3, 12–13, 47
People Capability Framework, 30
performance pay, 37
performance results and discussion *see* annual

performance statement
personal information protection *see* Privacy Rules
portfolio
Attorney-Generals, 3, 42
Portfolio Budget Statements, 16, 17
Prime Minister, 6, 8, 12, 17, 81, 82
Privacy Rules, 82, 97, 102, 107, 111
non-compliance, 98–99, 108
procurement *see* purchasing and procurement
professional development *see* learning and development
Project REDSPICE, 100
Public Governance, Performance and Accountability Act 2013, iii, 38, 39, 46, 48, 52, 55, 60
Public Governance, Performance and Accountability (Financial Reporting) Rule 2015, iii, 60
Public Governance, Performance and Accountability Rule 2014, iii, 48
compliance statement, 127–135
public information, 9, 10, 17, 26–27, 47
Public Interest Disclosure Act 2013, 6, 9, 24–25, 118, 120, 121–122
Public Interest Disclosure Amendment (Review) Act 2023, 2
public interest disclosures, 2, 8
IGIS function and powers, 6, 9, 121–122
intelligence agency obligations, 122
performance results and analysis, 24–25, 120
statistics, 4, 118
Public Service Act 1999, 35
purchasing and procurement, 48–50
purpose, 7–10, 12, 17

Q

Quiggin, Peter, 40

R

Reconciliation Action Plan, 30
record keeping, 80
AGO, 107
ASD, 102, 105
ASIO, 86, 87, 88
ASIS, 96, 97, 104
DIO, 111
Office, 16
ONI, 83
recruitment, 3, 32, 33, 35
REDSPICE, 100

regulation see ministerial authorisations;
ministerial directions; Privacy Rules

remuneration, 34–36, 71

reporting framework, 17 see also annual
performance statement

resources for outcome, 77–78

review of year, 2–3

Richardson Review, 32

risk management, 45–46

risk-based proactive inspections, 8 see also
inspections

roles and functions

- IGIS, 2, 6, 8–10, 12–13, 112, 118–122
- intelligence agencies, 81, 84, 95, 100, 106, 109,
112

Rules to Protect the Privacy of Australians see
Privacy Rules

S

Secretary of Defence, 18, 19, 109 see also
Department of Defence; Minister for Defence

security clearance processes, 3, 33, 35, 84

Security Plan, 45

Senate Legal and Constitutional Affairs Legislation
Committee, 13, 47

Senior Executive Service officers, 34–36 see also
Key Management Personnel

senior management committees, 38

signals intelligence see Australian Signals
Directorate (ASD)

small business participation in procurement, 48

special intelligence operations, 84, 89

spent conviction information, 93–94

staff

- APS Census Action Plan, 3, 31
- average staffing level, 33, 78
- consultative processes, 30
- diversity and inclusion, 4, 30, 34
- employment arrangements, 4, 33, 35
- Key Management Personnel, 35, 36, 71
- learning and development, 30–31, 46
- non-salary benefits, 35
- performance agreements, 31, 46
- profile, 4, 33–37
- recruitment and retention, 3, 32, 33, 35

- remuneration, 34–36
- workforce planning, 30, 33
- workplace health and safety, 37

staff presentations at public forums, 26, 27

stakeholder engagement, 42–44

Stanbridge, Sarah, 11, 36

Surveillance Devices Act 2004, 112, 113

*Surveillance Legislation Amendment (Identify and
Disrupt) Act 2021*, 6, 112

T

Technical Advisor role, 3, 32

Telecommunications Act 1997, 87

*Telecommunications (Interception and Access) Act
1979* (TIA Act), 101

- ASD non-compliance, 103–104
- ASIO non-compliance, 90–91, 93
- record keeping requirements, 88

training and development, 30–31, 46

transparency, 7, 9, 10, 26–27, 47 see also assurance

U

use of weapons, 96, 97

use-of-force notifications, 89

V

values, 10, 30, 46

Vandenbroek, Sarah, 40

visa-related complaints, 4, 23, 118, 120

W

warrants, 84, 88, 89, 90–91, 92, 93, 115

- network activity warrants (NAWS), 6, 112, 113,
118, 122

weapons use, 96, 97

website, ii, 9, 31, 47

whistleblower protection scheme see public
interest disclosures

Work Health and Safety Act 2011, 37

workforce see staff

workplace health and safety, 37

Y

year at a glance, 4

