



IGIS

OFFICE OF THE
INSPECTOR-GENERAL
OF INTELLIGENCE
AND SECURITY

ANNUAL REPORT 2024-25

IGIS.GOV.AU

Acknowledgement of Country

The Office of the Inspector-General of Intelligence and Security is located on Ngunnawal and Ngambri Country.

We acknowledge the Ngunnawal and Ngambri peoples as Traditional Custodians of these lands and waterways, and the continuation of the cultural, spiritual and educational practices of Aboriginal and Torres Strait Islander peoples across Australia.

We pay our respects to Elders past and present.

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 2025



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



IGIS

OFFICE OF THE
INSPECTOR-GENERAL
OF INTELLIGENCE
AND SECURITY

The Hon Michelle Rowland MP
Attorney-General
Parliament House
CANBERRA ACT 2600

Dear Attorney-General

Office of the Inspector-General of Intelligence and Security Annual Report 2024–2025

I am pleased to present the Office of the Inspector-General of Intelligence and Security annual report for the period 1 July 2024 to 30 June 2025.

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 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 my office has prepared fraud risk assessments and a fraud control plan; that my office has fraud prevention, detection, investigation and reporting mechanisms that meet its needs; and that I have taken all reasonable measures to deal with fraud relating to my office. There have been no instances of fraud identified during the period.

Yours sincerely

The Hon Christopher Jessup KC
Inspector-General of Intelligence and Security
2 September 2025

Contents

Contact information	ii
Letter of transmittal	iii
About this report	vi
Section One: Review by the Inspector-General	1
Inspector-General's review	2
Year at a glance 2024–25	5
Section Two: Overview	7
About us	8
Purpose	9
Our key activities	10
Our approach	12
Organisational chart	13
Providing assurance	14
Section Three: Annual Performance Statement	17
2024–25 Annual Performance Statement	18
Reporting framework	19
Performance review 2024–25	20
Section Four: Management and accountability	31
Our staff and culture	32
Organisational profile	35
Corporate governance	42
Stakeholders	45
Risk oversight and management	48
External scrutiny	50

Section Five: Financial statements	55
Financial Statements	56
Section Six: Review of intelligence agencies	85
Overview	86
Intelligence agencies	88
Australian Security Intelligence Organisation	88
Australian Secret Intelligence Service	101
Australian Signals Directorate	108
Australian Geospatial-Intelligence Organisation	116
Defence Intelligence Organisation	120
Office of National Intelligence	123
Australian Criminal Intelligence Commission and Australian Federal Police	127
Cross-agency activities	129
Complaints and public interest disclosures	132
Section Seven: Annexures	141
Annexure 7.1	142
Annexure 7.2	145
Glossary	156
Index	158

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 2024–25 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 2025–26.

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 2024–25.

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.

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.

Over the last year, the Office of the Inspector-General of Intelligence and Security (IGIS) has continued its core role in delivering independent oversight of Australia's intelligence agencies. Broadly split into 2 categories, our oversight of these agencies is both proactive and reactive.

This year, our proactive oversight has been undertaken through the risk-based inspection program delivered annually in accordance with section 9A of the IGIS Act. This was a daily, fundamental activity for the IGIS in 2024–25. Oversight teams commenced 82 inspections and completed and issued findings for 74.

Our reactive oversight work is undertaken in response to notifications or engagement from the agencies or the general public. This includes compliance matters identified by the agencies and disclosed to us, and the receipt and assessment of complaints and public interest disclosures under the IGIS Act and the *Public Interest Disclosure Act 2013* (PID Act).

In 2024–25, we received 64 complaints and closed 41. Two investigations were completed under the PID Act. Over the same period, we also completed one inquiry under the IGIS Act that came about via a public interest disclosure by a former public official.

Our oversight teams receive a high degree of cooperation and support from agencies in our jurisdiction. This year, where noncompliance, either with the law or with appropriate standards of propriety, was encountered, the matters were towards the less serious end of the spectrum and were readily corrected once drawn to the attention of the agency. My staff routinely review the implementation of findings, to ensure that compliance issues have been addressed and practices and policies are in place to reduce the likelihood of recurrence.

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

Legislation affecting the work of the IGIS

Prior to the 2025 federal election, the Intelligence Services Legislation Amendment Bill 2023 (ISLAB) was being considered by the Parliamentary Joint Committee on Intelligence and Security. The ISLAB contained provisions which would, if passed, have significantly expanded our jurisdiction to cover oversight of the entirety of the Australian Criminal Intelligence Commission and the intelligence functions of the Australian Transaction Reports and Analysis Centre (AUSTRAC), the Australian Federal Police and the Department of Home Affairs. The ISLAB lapsed with the proroguing of the 47th Parliament. At the time of writing, the government has introduced the Strengthening Oversight of the National Intelligence Community Bill 2025 to the parliament to expand our jurisdiction along the same lines as envisaged in the ISLAB.

The IGIS continues to be actively engaged in proposed reforms to the PID Act and we are keen to ensure the whistleblowing framework remains fit for purpose and accessible for public officials to report wrongdoing.

Over the last year I have reflected on 3 aspects in which the provisions of the PID Act are problematic in their application to the work of the Inspector-General. All are sourced in the circumstance that, for intelligence agencies, the Inspector-General is an 'authorised internal recipient' of a disclosure where the disclosed information relates to conduct within an intelligence agency.

The first problem arises under subsection 28(3) of the PID Act, which provides that a public interest disclosure may be made without the discloser asserting that the disclosure is made for the purposes of that Act. The result of this provision is that correspondence which fits the description of a complaint under section 10 of the IGIS Act may also be a disclosure under the PID Act. Both Acts embody obligations upon the Inspector-General – subject to limited exceptions – to conduct an investigation or an inquiry, as the case requires. These overlapping provisions may be handled under specific carve-out provisions in the legislation (such as paragraph 11(2)(c) of the IGIS Act or section 49 of the PID Act), but the application and timing of the processes involved must be handled very carefully by experienced staff. As explained here, I have found subsection 28(3) of the PID Act to be uncondusive to the efficient and expeditious disposition of complaints received by, and disclosures made to, the IGIS.

The second problem arises under the reporting provisions of section 51 of the PID Act. Subsection (4) of that section sets out certain requirements as to the provision of a report of an investigation under that Act, but omits to refer to a situation in which the investigation has been conducted by the Inspector-General. Paragraph (b) of the subsection appears to have the effect that such a report should not be given to the Ombudsman, and paragraph (a) relates only to notification to the discloser. Where the investigation was conducted by an officer of the agency in which the disclosed conduct was alleged to have occurred, no doubt the report would find its way to the relevant senior executive in that agency. But where the investigation was conducted by the Inspector-General, the obligation to provide the report to such an executive may be implicit, but is not explicit, in the PID Act. Where the disclosed conduct was that of the head of the agency himself or herself, the absence from the PID Act of any provision along the lines of subsection 21(1B) and paragraph 22(1)(b) of the IGIS Act is conspicuous.

The third problem is concerned with whether the subject matter of an IGIS Act inquiry which commenced life as a PID Act disclosure is IGIS Act propriety, PID Act disclosable conduct, or something else again. I have been able to proceed with my inquiries relying on an interpretation that the subject matter of an IGIS Act inquiry which had been brought under that Act by a decision by the principal officer under section 49 of the PID Act would be PID Act disclosable conduct. However, the matter is not settled.

Engagement with the agencies, parliament and the public

In 2024–25, I contributed to inquiries conducted by the Parliamentary Joint Committee on Intelligence and Security via submissions and appearance before the committee. I have held at least biannual meetings with the leadership and senior executives of the Australian Security Intelligence Organisation, Australian Secret Intelligence Service, Australian Signals Directorate, Office of National Intelligence, Defence Intelligence Organisation and Australian Geospatial-

Intelligence Organisation and kept relevant ministers informed of findings in relation to the agencies in their respective portfolios. Engagement with the Attorney-General's Department, as our portfolio 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.

I was pleased to host members of the Five Eyes Intelligence Oversight and Review Council at the annual conference held in Canberra and Sydney in November 2024. This was an important opportunity for our international oversight partners to engage with the Attorney-General and the head of the agencies we oversee on issues relevant to oversight. We also showcased the work of the IGIS, and engaged with our partners to identify emerging challenges to intelligence oversight globally.

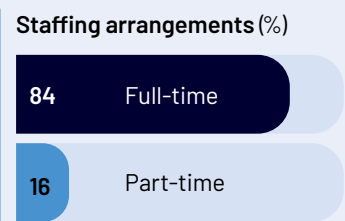
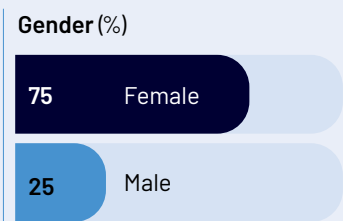
We continue to invest in continuous review and improvement. The IGIS has implemented the recommendations of the IGIS Oversight Capability Review and the actions identified in our 2024 Australian Public Service (APS) Census Action Plan. Our corporate governance framework continues to be strengthened with ongoing work to update a range of policies and procedures.

Staffing levels across the IGIS 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. We continue to implement strategies to improve workforce retention. Over the coming year, we will maintain our focus on strategic human resources initiatives to attract talent, retain high-quality staff and provide a rewarding and intellectually stimulating work environment.

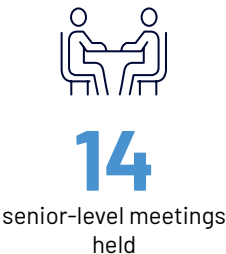
I thank all staff of my office for their professionalism and dedication over the year. Our work is important, and it is critical to independent and credible oversight of the Australian intelligence community. It will only become more so in the coming years as the national conversation becomes more highly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

Year at a glance 2024–25

Staffing profile as at 30 June 2025



Oversight activities



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:

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

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 by the Australian Criminal Intelligence Commission (ACIC) and the Australian Federal Police (AFP).

Purpose

We provide independent assurance to ministers, the parliament, and the public on whether Australia's intelligence and security agencies under our jurisdiction are acting with legality, with propriety and consistently with human rights.



Our key activities

We deliver on our purpose through our key activities. The key activities reflect our role as set out in the IGIS Act. The Inspector-General is supported in undertaking these 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 can look proactively at an issue or an area of an agency activity that may pose a significant risk; or reactively in response to a complaint; or at the request of the Prime Minister, the Attorney-General or the relevant responsible minister. When undertaking inquiries, we have investigative powers similar to those of a royal commission, including the power to compel persons to answer questions and produce documents and to take sworn evidence.

A preliminary inquiry into the actions of an intelligence agency may be initiated either proactively at the Inspector-General's own motion or in response to a complaint. This process provides the means for the Inspector-General to undertake preliminary investigations to determine whether further inquiry into the action is necessary.

Risk-based proactive inspections

Conducting regular proactive and independent inspections provides assurance that intelligence agencies are operating with legality, with propriety and in accordance with human rights.



Our inspections are carried out by inspection teams, each specialising in the oversight of one or more of the intelligence agencies. We undertake cross-agency inspections to review related activities where agencies in jurisdiction either work collaboratively or have similar legislative obligations.

We ensure our inspections are prioritised according to risk, informed by our oversight inspection teams' knowledge of the individual intelligence agencies and the environment in which they operate. Impacts on Australian persons and on Australia's domestic and foreign relationships are key considerations in assessing risk. In practice, this means our focus is often on:

- agency activities requiring the most intrusive powers
- new or novel capabilities and activities
- areas where issues have previously been identified.

To support these inspections, the intelligence agencies self-report instances of potential non-compliance and provide us with advice as to the context in which the activities were conducted. A classified summary report of key inspections and other activities is provided periodically to each relevant responsible minister.



Managing complaints

As part of our scrutiny of the activities of intelligence agencies and our public assurance role, we can inquire into complaints made about the agencies we oversee, including the use of network activity warrants by the AFP and ACIC. We receive and where appropriate investigate complaints about the conduct of intelligence agencies from a range of people – including the agencies current or former staff and other people who have had dealings with the agencies.

Complaints are received through a range of channels and, depending on the complaint's seriousness, can be resolved without further action, be subject to a preliminary inquiry or proceed to an inquiry. Complaints may, for example, result in further engagement between an intelligence agency and the complainant, recommendations being made to the intelligence agency with respect to its conduct, and intelligence agencies updating policies and procedures where necessary. 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, in the main, not made public by the IGIS, due to our secrecy obligations and considerations of personal privacy.

Handling public interest disclosures

The Inspector-General can receive public interest disclosures (PIDs) about intelligence agencies from current or former public officials including members of intelligence agencies. For the purposes of the Inspector-General's PID jurisdiction, certain IGIS staff are authorised officers for the purposes of the *Public Interest Disclosure Act 2013* (Cth) (PID Act).

These officers, and the Inspector-General, are able to receive disclosures of information and then determine if it is appropriate to allocate the handling of the disclosure to one or more of the intelligence agencies or to allocate the disclosure to the Inspector-General to investigate. The purpose of a PID investigation is to establish whether any instances of disclosable conduct have occurred.



Providing assurance to ministers, parliament and the public

The IGIS provides assurance to ministers, the parliament and, to the extent possible, the public that there is effective oversight and scrutiny of intelligence agencies. Our program of inspections and conduct of inquiries into the activities and procedures of intelligence agencies, as well as the management of complaints and PIDs, contribute to this assurance.

A crucial element of assurance is communicating information about our role and our work. We accomplish this through a series of complementary activities, including making 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 – taking national security considerations into account – details of inspection, inquiry, complaint and PID activities and findings for each agency. A classified summary report of key inspections and other activities is also provided periodically to each relevant responsible minister.

The IGIS's executive also regularly meets with each agency's senior officers and provides regular classified 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 successful delivery of our mission. This includes independence in selecting matters for inspection or inquiry and in 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 an individual mandate. We have a strong understanding of the intelligence agencies beyond their purpose and functions. This includes their operational planning, capabilities, risk management processes and approach to compliance. We also ensure we 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 areas of significant risk or concern.



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 legal or propriety risk and activities with the potential to adversely affect the lives or rights of Australians. Our focus is on identifying serious, systemic or cultural problems in the activities of agencies within our jurisdiction, so that agencies can address these issues.

Open

We share as much information as possible regarding our oversight/assurance activities with complainants, the public, the parliament and ministers. The classified nature of the information we review may restrict what we can release publicly. Nevertheless, we include as much information as possible about our oversight of intelligence agency activities in our annual report, in unclassified inquiry and preliminary inquiry reports, and in responses to complaints. Classified information is provided regularly to ministers and the parliament.

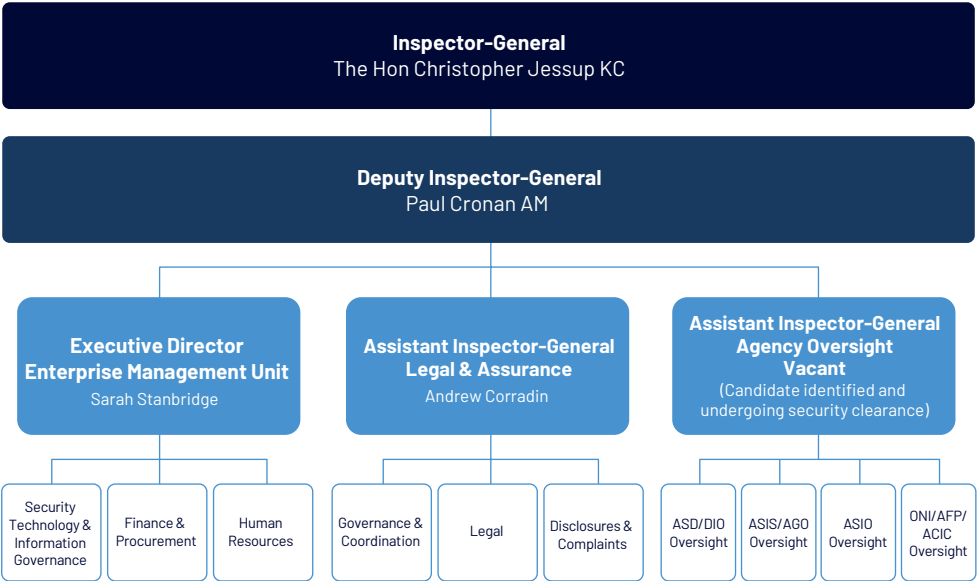


Influential

IGIS oversight is a key component of the oversight framework within which intelligence agencies operate. Inspections, inquiries and investigating complaints make a positive contribution to compliance; they lead to effective changes in agency processes and foster a culture of compliance. We work cooperatively with other oversight bodies to avoid duplication. Our submissions to parliamentary committees contribute to informed debate about the activities of the agencies, as well as the policies which guide those activities.

Organisational chart

Figure 2.1: IGIS organisation structure at 30 June 2025



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 2024–25, 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 2024–25, 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 or the head of the relevant agency on a completed preliminary inquiry into an intelligence agency. In 2024–25, the Inspector-General provided 5 section 25B preliminary inquiry reports. These 5 preliminary inquiry reports were made in relation to ASIO (one report), ASIS (one report) and ASD (3 reports). They are discussed further under the specific intelligence agency headings in Section 6.

Additionally, in 2024–25, 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 the IGIS conducts inspection and review activities.

During 2024–25, the Inspector-General received no requests from the Prime Minister or ministers to conduct an inquiry under the IGIS Act.

Assuring parliament and the public

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

Parliamentary Joint Committee on Intelligence and Security

During 2024–25, the IGIS made a submission to the Review of Administration and Expenditure No. 23 (2023–24) by the Parliamentary Joint Committee on Intelligence and Security (submission 8), and the Inspector-General and senior staff appeared before the committee in a private hearing.

Senate Legal and Constitutional Affairs Legislation Committee

In 2024–25, the IGIS made a submission to the Senate Legal and Constitutional Affairs Legislation Committee in relation to its review of the provisions of the Oversight Legislation Amendment (Robodebt Royal Commission Response and Other Measures) Bill 2024 (submission 5).

The IGIS submission noted support for amendments that implemented the government's response to recommendations from the Report of the Royal Commission into the Robodebt Scheme. These amendments would have the effect of ensuring oversight bodies are strongly positioned to undertake independent, impartial and rigorous investigations into the dealings of government agencies, which the submission noted was critical to the improvement and maintenance of public trust in public administration.

Evidence to the Administrative Review Tribunal and Australian Information Commissioner

Under the *Archives Act 1983* and the *Freedom of Information Act 1982* (FOI Act), the Inspector-General may be called on to provide the Administrative Review Tribunal (ART) 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 ART and the Australian Information Commissioner are required to seek evidence from the Inspector-General. There are equivalent provisions in the Archives Act for the ART. 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 the 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 2024–25, the Inspector-General received 5 requests for evidence from the Australian Information Commissioner in relation to freedom of information exemptions. The Inspector-General declined to give evidence in those matters because, in the Inspector-General's opinion, he was not appropriately qualified to do so.

Section Three

Annual Performance Statement



2024–25 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 2024–25, as required under paragraph 39(1)(a) of the *Public Governance, Performance and Accountability Act 2013* (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 2024–25 and the Portfolio Budget Statements (PBS). In preparing the annual performance statement, we draw data from our corporate record-keeping systems.

Reporting framework

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

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, senior 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.

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

Corporate Plan

IGIS purpose:

We provide independent assurance to ministers, the Parliament, and the public as to whether Australia's intelligence and security agencies under our jurisdiction are acting with legality, propriety and consistency with human rights.

Annual Performance Statement

Reports against the performance framework.

Performance review 2024–25

In 2024–25, 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 2024–25. 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 inform 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		
 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
1.1 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) is informed. [IGIS Act, s 15]	 Achieved
	When preparing a report, any opinions that are critical of an individual or agency's actions or activities are provided to the individual, agency head or responsible minister for comment before completion. [IGIS Act, s 17]	 Achieved
	The final report from an inquiry is provided to the agency head and responsible minister. [IGIS Act, s 22]	 Achieved
	Overall assessment	Achieved

Analysis

During 2024–25, 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 2024–25 was provided to the responsible minister and head of agency on the same day it had been approved by the Inspector-General, and the report included clearly articulated findings. Two draft inquiry reports were also provided to the respective agency heads on the same day they were internally approved. The IGIS implemented the remaining recommendations of the Oversight Capability Review where possible and implemented all recommendations relevant to the conduct of inquiries.

Measure 1.2 is assessed as achieved. Before the commencement of the inquiry initiated in 2024–25, the responsible minister and head of agency were 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 and the responsible minister.

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

Objective 2: Inspections



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

Performance measure	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.	 Achieved
	All inspection activities in the inspection plan are commenced during the annual cycle.	 Substantially Achieved
	Preliminary investigations into proactively reported compliance incidents are completed in a timely manner.	 Achieved
	Inspection outcomes, including findings and recommendations, are clearly communicated to the agency and promote meaningful reviews of policy, process, procedure, training or technology.	 Achieved
	Implement the recommendations of the internal Oversight Capability Review relevant to inspections.	 Achieved
Overall assessment		Achieved
2.2 Conduct inspections consistent with the IGIS Act	Responsible ministers are provided with a biannual report outlining the key inspection activities each year. [IGIS Act, s 25A]	 Achieved
	Annual inspection plans are reviewed in accordance with key priorities and risks before being provided to agency heads in July. [IGIS Act, s 9A(1)]	 Achieved
Overall assessment		Achieved

Analysis

During 2024–25, 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. A small number of inspections were deferred to the 2025–26 inspection cycle due to administrative reasons and resourcing constraints. Further, a number of inspections were commenced but not finalised during 2024–25 due to the complexity and/or volume of material required to be assessed. The IGIS ensured it prioritised the inspections it would continue to deliver to maximise assurance for parliament, ministers and the public.

The IGIS's review of compliance incidents continued to be timely in 2024–25, with any delays (either from the relevant agency or internally) monitored through the Executive Board briefing process. The Executive Board paid particular attention to the time taken by intelligence agencies to obtain legal advice in relation to their own identified compliance incidents, and will continue to monitor this issue.

All inspection findings are communicated to agencies, and the work of the agencies to address the inspection recommendations is actively monitored by IGIS.

Implementation of the Oversight Capability Review has been finalised, 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 June 2024, and responsible ministers were provided with biannual reports in August 2024 and February 2025.

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	A timely decision is made after receipt of a matter that: - the matter is not within authority or - the complaint is within authority, but there will be no inquiry, or - there will be an inquiry. [IGIS Act, s 11]	 Substantially Achieved
	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
	If a report is prepared under s 25B of the IGIS Act following the making of preliminary inquiries, the report is provided to the relevant minister or agency head in a timely manner. [IGIS Act, s 25B]	 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]	N/A
	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.	 Achieved
	Overall assessment	Achieved

Analysis

During 2024–25, 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 30 visa or citizenship complaints. In addition, the IGIS considered 358 other matters to determine whether they fell within the Inspector-General's jurisdiction.

The IGIS undertook significant actions to review and improve its complaints-handling processes during this reporting period. For the complaints that were finalised in the reporting period, an outcome was provided to the complainant in a timely manner where it was 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 receipt of a disclosure, best endeavours are made to allocate the handling of the disclosure or decide not to allocate the disclosure within 14 days after the requirement arises. [PID Act, s 43(3), (4) and (11)]	 Partially achieved
	After a decision to allocate a disclosure to another agency, notice is provided in a timely manner to: • if relevant, the principal officer of the agency to which the disclosure is allocated, and • if reasonably practicable, the discloser. [PID Act s 44]	 Achieved
	After a decision not to allocate a disclosure, the discloser is informed in a timely manner of: • the decision and the reasons for the decision, and • details of any action or proposed action to refer the conduct to be investigated under another law or power, or • any courses of action that might be open to the discloser* under another law or power. [PID Act s 44A] *Removed the word 'disclosure' and replaced with 'discloser' to align wording to the PID Act.	 Substantially Achieved

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 allocation of a disclosure to the Inspector-General, the discloser is informed in a timely manner that: - 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]	 Substantially 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.	 Achieved
	Overall assessment	Substantially achieved

Analysis

During 2024–25, the IGIS substantially achieved its objective to receive and, where appropriate, investigate disclosures about suspected wrongdoing within an intelligence agency in a timely manner.

In the reporting period, the Inspector-General assessed 20 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 IGIS allocated 4 matters to intelligence agencies for investigation under the PID Act.

In the majority of cases the disclosers were notified of these decisions in a timely way.

Two PID investigations were finalised during this reporting period. It is important to note that 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.

There was considerable effort to strengthen the IGIS's disclosure processes in 2024–25 and this will continue into future reporting periods.

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 comments 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 experts across the national security community, the legal profession, oversight bodies, and academia in Australia and internationally.	 Achieved
	IGIS executive participates in at least biannual meetings with each agency's senior officers to understand agency priorities and share oversight key issues and findings.	 Achieved
	Provide regular updates to the agencies' ministers on the key issues for each agency and the Inspector-General.	 Achieved
Overall assessment		Achieved

Analysis

During 2024–25, 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 made a number submissions to parliamentary inquiries, hearings and other reviews of national security matters as detailed on pages 14–15 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. After the 2025 election, the Inspector-General provided a classified briefing for the incoming Attorney-General on the role of the IGIS.

The IGIS *Annual Report 2024–25* is publicly available on our website and transparency.gov.au. The annual report provides as much detail as possible – with consideration for protective security requirements – on inspection and inquiry activities relating to each agency, as well as complaint and PID findings.

During 2024–25, senior IGIS officers delivered a number of presentations to the public or national security experts in Australia on both the role of the IGIS and other topics of interest.

On the international stage, the IGIS hosted the 2024 Five Eyes International Oversight Review Council meeting in Canberra and Sydney. During this week-long event, the IGIS facilitated discussion on a host of relevant topics in conjunction with the agencies we oversee. In hosting the event, the IGIS delivered presentations, led working groups and hosted short-term visits from bilateral partners.

In the reporting period, the IGIS participated in biannual meetings with 4 agencies and triannual meetings with the other 2 agencies in our jurisdiction. These meetings included visits to domestic offices 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 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.

We are a small yet highly specialised agency and our staff undergo rigorous psychological and vetting processes to ensure the highest standards of professionalism and integrity. The classified nature of our work instils a strong sense of purpose and ethics, creating a mission-driven culture where every team member understands their critical role in supporting the Inspector-General to provide independent assurance to ministers, parliament and the public.

Our unique function and the diverse scope of our operations attracts professionals from a wide range of backgrounds and skill sets. Each staff member brings their unique expertise and perspective, contributing to a dynamic and collaborative APS workplace.

We remain committed to growing the IGIS's workforce to meet our funded average staffing level (ASL) and to support IGIS employees through individually tailored flexible working arrangements, professional development opportunities, and wellbeing programs.

Flexible work

At IGIS we understand that flexibility is important to achieving a good work-life balance and contributes to positive outcomes for our employees' health and wellbeing. The nature of our work does place restrictions on some aspects of flexible working, but we strive to be as flexible as the restrictions allow and to consider the diverse circumstances of our employees.

Underpinning our implementation of flexible working arrangements, trust within our workforce and in their commitment to delivering work outcomes is at the forefront. This is enabled by our culture, behaviours and processes and by an individual's capacity to work independently and their ability to actively contribute to the workplace.

IGIS's flexible working arrangements include:

- flexible working hours, where employees manage their hours of work in a flexible manner either on an ad hoc basis or as an ongoing arrangement. This can also include working compressed hours or having altered start/finish times. This is available to all staff – from APS levels and executive levels to the Senior Executive Service (SES)
- flex time, which enables APS-level (APS 1 to APS 6) employees to set their own patterns of attendance at work, within specified limits
- hybrid working, where there is an agreement for employees to work some days in the office and some days at home. This may also occur on an ad hoc basis when an employee needs flexibility
- part-time working hours, which are available to employees who want or need to work less than 37.5 hours per week
- remote work, where an employee primarily works from a location other than the Canberra office.

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 (D&I Committee) progresses initiatives to strengthen and reinforce a workplace culture where all forms of diversity are valued and respected. The D&I Committee is sponsored by the D&I Champion and led by the D&I Chair, and comprises volunteer members from across the agency. It plays a key role in providing strategic advice on the IGIS inclusion and diversity strategy.

The D&I Committee works closely with the IGIS Social Club, with our human resources (HR) team, 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 2024–25 the D&I Committee continued embedding D&I into office culture and planning, and building the IGIS's understanding of D&I issues through events, resource packs and education. The key driver of the committee's activities in 2024–25 was the need to effectively focus limited resources on issues where the committee could have the most impact, given the size of the agency. Accordingly, the committee focused its efforts on key initiatives identified as important to IGIS staff – such as Autism Awareness Month and celebrating cultural and linguistic diversity. In concert with the larger networks in AGD and the wider APS, the committee will continue its work into 2025–26.

IGIS Reconciliation Action Plan

During 2024–25, the HR team, working with the D&I Committee, finalised the first IGIS Reconciliation Action Plan (RAP), which was launched in June 2025. Our Reflect RAP is an important step as the IGIS grows, and is the cornerstone of the IGIS's commitment to reconciliation. The RAP is more than words on paper; it represents the IGIS's commitment to action.

Through the RAP, the IGIS is building cultural capability to ensure our workplace is safe and welcoming for Aboriginal and Torres Strait Islander people. In 2024–25, our office had no staff who identified as Aboriginal and/or Torres Strait Islander. While the IGIS is small and specialised, it is vital there are no barriers to having the best people doing the important work of our office. That includes removing barriers due to a lack of cultural understanding or to prejudice, whether conscious or unconscious.

Implementation of the RAP is underway and the IGIS will continue to work with Reconciliation Australia, our APS colleagues, and Aboriginal and Torres Strait Islander people, including the traditional owners of the land on which we work, as we continue our reconciliation journey.

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 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 Australian Public Service Commission (APSC), the National Intelligence Academy and a range of other providers. In addition, the IGIS participated in the APS Graduate Development Program for the first time in 2024–25. The IGIS's 'participating agency' status with the Australian National University (ANU) National Security College provides access to the ANU's sought-after executive development programs, in addition to their range of shorter professional development programs.

Census Action Plan

In November 2024, we published on our website the results of the 2024 Australian Public Service Census for IGIS, and IGIS's 2024 APS Census Action Plan. Our Census Action Plan was developed and agreed through consultation with IGIS employees. The plan identified 7 actions.

During the reporting period, we progressed action items from the Census Action Plan and, where resourcing priorities allowed, completed some of those actions.

For example, in November 2024, we finalised and implemented the IGIS rewards and recognition program. We delivered the first round of awards under this new framework in January 2025: Australia Day awards and length-of-service recognition.

The IGIS will continue publishing its APS Census highlights report and Census Action Plan on the IGIS website annually, and will continue working with IGIS employees to make continuous improvements to our workplace. To enable us to better understand our results, the APSC provided a detailed session on the 2024 results analysis to the IGIS Executive and EL 2s.

Technical Advisor role

The IGIS has a dedicated Technical Advisor who delivers advice and guidance on the IGIS's oversight activities.

During 2024–25, the IGIS continued to fill the Technical Advisor role through a secondment, accessing the practical technical expertise found in the intelligence community. The seconded Technical Advisor has been able to support oversight staff in their scoping, planning and execution of inspections; drive in-house training opportunities; and provide expertise to the IGIS executive where required.

Given the value provided by having contemporary intelligence community expertise in the Technical Advisor role, the IGIS is considering the option of establishing the position as a rotating secondment. This would allow us to bring into the IGIS continually updated knowledge which aligns with our inspection programs.

Organisational profile



49

Ongoing employees*



16%

On part-time arrangements



100%

are engaged to work from Canberra#

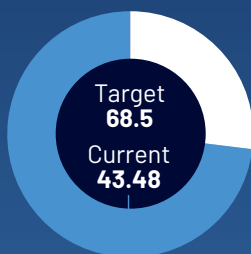
* Including 6% on long-term leave.

2 employees worked remotely from New South Wales and Tasmania.

No employees identified as Aboriginal and/or Torres Strait Islander.

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 68.5 in the reporting period, due to a combination of:

- a competitive labour market
- the necessary duration of the psychological and Top-Secret Positive Vetting clearance pipeline
- staff leaving the agency.

To address workforce growth challenges, a range of recruitment strategies were progressed, including participating in graduate entry recruitment, accessing existing merit pools, secondments within the national intelligence community, employee referral programs, and refreshed advertising approaches.

Recruitment environment

The IGIS continues to experience the impact of labour market shortages across a range of critical skill sets in both operational and corporate areas. The changing nature of work, digital transformation and an increasing demand for skills have all contributed to a competition for talent. The IGIS's security overlay, by necessity, lengthens our recruitment lifecycle. 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

In 2024–25, the IGIS conducted a significant number of recruitment campaigns to strengthen its workforce of specialist oversight and corporate officers:

- Multiple recruitment rounds were advertised and completed for a number of roles across the APS 4–6 and EL 1–2 levels.
- Bulk recruitment for operational roles was conducted.

One SES Band 1 role was filled during the reporting period. Another was advertised and a candidate is progressing through the Top-Secret Positive Vetting clearance process. These recruitment activities attracted large numbers of candidates, with a significant number progressing further in our recruitment pipeline. At 30 June 2025, the majority of these candidates are still progressing through relevant processes.

Exploring new approaches

The IGIS has implemented creative recruitment strategies such as:

- a temporary employment register
- a talent register portal to identify candidates for transfers under section 26 of the Public Service Act 1999 (PS Act)
- secondments across the national intelligence community
- employee referral programs
- alternative recruitment pathways
- accessing merit lists from other APS agencies
- creative advertising.

To support workforce retention and capability, the IGIS enhanced its workforce analytics function to inform executive decision-making, expanded the use of pulse surveys, enhanced wellbeing initiatives and strengthened flexible work options. The IGIS also continued to build closer relationships with international partners by exploring training and capability-sharing opportunities, and continued to ensure staff had access to a range of training and development opportunities.



Case Study: Employee Value Proposition

The IGIS's Employee Value Proposition initiative was a comprehensive deep dive to gain feedback from staff and provide the Executive Board with deeper insight into employee engagement, motivation and organisational culture. Through a combination of surveys, interviews and focus groups, the process explored what employees value about working in the IGIS, what would retain them, and how we can use these factors in our attraction strategy. The findings identified key strengths, areas for improvement, and push and pull factors for the workforce. During 2024–25, our staff retention rate stabilised from trends seen in the previous reporting period. Initiatives to continue the positive trajectory are progressing. Staff engagement is a high priority to ensure these initiatives align with the career expectations of IGIS employees.

Table 4.1: Overview of substantive IGIS staffing profile

As at 30 June 2024							
At 30 June 2025							
APS classification (salary range 2024–25)	Male	Female	Uses a different term	Total	Male	Female	Uses a different term
APS classification							
APS 4 (\$78,908–\$85,853)	0	3	0	3	0	1	0
APS 5 (\$87,840–\$95,284)	2	1	0	3	1	1	0
APS 6 (\$100,244–\$112,652)	2	9	0	11	2	7	0
Executive Level 1 \$121,089–\$134,987)	5	12	0	17	4	8	0
Executive Level 2 (\$140,938–\$167,436)	1	12	0	13	2	11	0
SES Band 1 (\$240,568–\$271,879)	1	0	0	1	1	0	0
SES Band 2 (\$302,065–\$339,158)	1	0	0	1	1	0	0
Total	12	37	0	49	11	28	0

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 the IGIS's pay increases at the relevant classification level.

Employment frameworks

All IGIS officers are employed under the PS Act. Since 14 March 2024, all non-SES officer salaries and conditions have been made under the IGIS Enterprise Agreement 2024–2027. There are currently 3 SES officer positions in the agency, with 2 being filled as at 30 June 2025. During 2024–25, the remuneration for SES officers moved to a collective determination, made under subsection 24(1) of the PS Act. This determination outlines the terms and conditions of engagement.

The agreement allows for individual flexibility arrangements to be entered into between the agency and an employee in respect of remuneration arrangements, overtime and penalty rates, allowances, working hours and leave. As at 30 June 2025, 47 employees were covered by the enterprise agreement; 8 of these employees also had an Individual Flexibility Arrangement. Of the Individual Flexibility Arrangements, 7 relate to remuneration arrangements and 1 relates to leave arrangements.

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 \$1,367.

Employees have 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 now set out in the collective determination. General performance discussions between the Inspector-General and SES officers 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	Termination	Total remuneration ⁴
The Hon Christopher Jessup KC Inspector-General (1 July 2024 to 30 June 2025)	\$485,423	\$76,587	\$29,932	-	-	-	-	\$591,941
Paul Cronan Deputy Inspector-General (1 July 2024 to 30 June 2025)	\$313,961	\$22,824	\$45,640	\$8,088	-	-	-	\$390,513
Chris Brookes Assistant Inspector-General (1 July 2024 to 28 February 2025)	\$139,590	\$20,603	\$29,945	\$3,616	-	-	-	\$193,753
Clare Menzies Acting Assistant Inspector-General (3 March 2025 to 30 May 2025)	\$53,519	\$1,152	\$8,610	\$1,282	-	-	-	\$64,562
Andrew Corradin Assistant Inspector-General (26 August 2024 to 30 June 2025)	\$211,121	\$38,760	\$27,427	\$5,349	-	-	-	\$282,656
Sarah Stanbridge Executive Director (1 July 2024 to 30 June 2025)	\$193,463	\$6,285	\$38,158	\$5,178	-	-	-	\$243,084

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 for part of the year 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 statements⁵.

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 meetings of the Executive Board, Leadership Group and Audit and Risk Committee and, as the need arises, directly with the Inspector-General through the Health and Safety Representative, SES, directors and staff.

Throughout 2024–25, 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.

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) 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 APSC'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 and corruption prevention and control
- business continuity framework, policy and response.

To meet the objectives of each component, committees and the Executive Board support the Inspector-General and senior executives to fulfil their corporate and governance responsibilities.

The Executive Board is the IGIS's primary decision-making body. 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 PGPA Act.

In addition to the Executive Board, the Audit and Risk Committee and the D&I Committee are focused on core business areas, as well as enabling functions such as staff consultation, leadership, audit and D&I. The committees provide a range of advice and support the IGIS in key decision-making. 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 and Risk Committee

The IGIS Audit and Risk Committee (ARC) is established in accordance with the PGPA Act. The ARC'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 ARC are structured according to the PGPA Act. The IGIS Audit and Risk Committee Charter is available on our website.

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

Table 4.3 IGIS Audit and Risk Committee membership

Committee member	Qualifications, knowledge, skills and experience	Meetings attended	Total annual remuneration
Ms Karla Bogaart Chair (External member)	Ms Bogaart holds a Bachelor of Commerce majoring in Accounting and is a Fellow Member of the Institute of Chartered Accountants. Ms Bogaart has over 30 years' experience in chartered accounting in the private sector. Ms Bogaart was previously Chair for the Audit Committee at CIT Solutions from 2020 to 2024.	1 August 2024	\$20,000
		8 August 2024	
		28 November 2024	
		26 March 2025 22 May 2025	
Mr Stephen Moore (External member)	Mr Moore holds a Bachelor of Economics (Honours), Econometrics and Quantitative Economics and a Graduate Diploma (with merit) in Econometrics and Quantitative Economics; and is a fellow of the Australia and New Zealand School of Government Executive Fellows Program. Mr Moore has experience as a senior leader in public service agencies working on ICT security and applications, governance and customer experience, as well as experience in the private sector.	8 August 2024	\$2,904
		28 November 2024	
		26 March 2025	
		22 May 2025	

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.	1 August 2024 8 August 2024 28 November 2024 26 Mar 2025 22 May 2025	\$18,750

Internal audit

Internal audit provides independent and objective assurance and advice to the Inspector-General, through the ARC, that the IGIS 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 has 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 continued to work with the external provider on the IGIS internal audit program. An internal audit commenced at the end of 2024–25 on reviewing the IGIS’s business continuity plan. This internal audit will be finalised in 2025–26.

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.

Inspectors-General Forum

During 2024-25, a group of 8 Commonwealth Inspectors-General met biannually to foster a community of practice. The group comprised the Inspectors-General of Intelligence and Security, Water Compliance, Defence, Aged Care, Taxation, Biosecurity, Animal Welfare and Live Animal Exports and Inspector of the National Anti-Corruption Commission. The purpose of the Inspectors-General Forum is for each Inspector-General to share their experiences and discuss recent challenges, developments, and improvements in the way their offices conduct oversight functions. The aim is to improve oversight of Commonwealth functions and agencies.

Corporate support

In addition to selected corporate support, including HR and financial services, provided by AGD under a memorandum of understanding, the Australian Signals Directorate provides IGIS with ICT system support.

Integrity Agencies Group

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 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 2024–25, the Australian Human Rights Commission did not refer any such matters to the Inspector-General.

Office of the Australian Information Commissioner

IGIS officers and the 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 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 2024–25, the Inspector-General and IGIS officers deepened engagement with the Five Eyes Intelligence Oversight and Review Council (FIORC) by hosting the annual face-to-face meeting in Canberra and Sydney. 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 met to exchange and share views on subjects of mutual interest and concern, compare best practices in review and oversight methodology and explore areas where cooperation is appropriate. Specific topics discussed included:

- international compliance and oversight
- short-term visits and secondments
- information sharing and cross-jurisdiction inspections
- technological challenges
- geopolitical challenges
- preparing for the future
- the career of an oversight officer.

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 London in October 2025.

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 members of Canada's NSIRA for a short-term visit in January 2024. The visit built institutional links between the IGIS and NSIRA and identified similarities, differences and opportunities in Australia's and Canada's operating environments and oversight approaches.

Key areas for cooperation and collaboration included:

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

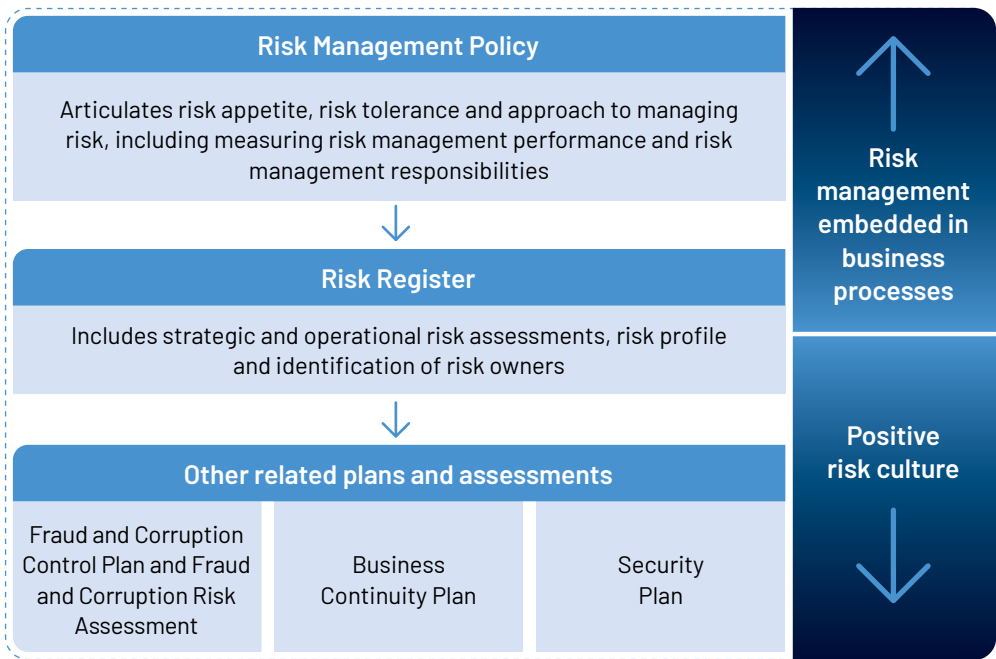
Risk oversight and management

The IGIS is committed to a risk-aware culture promoting proactive risk management and informed decision-making.

The identification and effective management of risk is an integral part of business planning and governance processes. We manage risk through our Risk Management Policy and Framework, which provides a structured and consistent approach to identifying, analysing and mitigating risk.

Identifying risks and determining how to reduce them to an acceptable level underpins our strategic plan, branch plans, fraud and corruption control measures, and business continuity arrangements.

The Risk Management Framework has been developed to make risk management efficient, effective and applied consistently across the IGIS.



The IGIS monitors and reviews risk against the following categories:



The IGIS is continuing to integrate, strengthen and embed risk management into its work. While the strategic risks being managed are growing as a result of a range of factors including an expanding workforce, an evolving jurisdiction and changes in the national security environment, we will manage these risks through robust planning and further strengthening stakeholder relationships.

Ethical standards

During 2024–25, the IGIS continued its commitment to high ethical standards. These high ethical standards are maintained through:

- APS integrity and values training
- mandatory online fraud and corruption training
- modelling of appropriate behaviours by SES officers
- a requirement that all officers maintain Top-Secret Positive Vetting 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.

Fraud and corruption control

The IGIS's fraud and corruption control strategies comply with the Commonwealth Fraud and Corruption 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 and corruption control framework. The IGIS updated its Fraud and Corruption Risk Assessment in 2025.

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

The IGIS had no reports of fraud and corruption in 2024–25.

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 2024–25. 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 November 2024. The IGIS also attended public and private hearings of the Parliamentary Joint Committee on Intelligence and Security and provided submissions on a range of inquiries. Where security classifications permit, the IGIS's submissions, its 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

The IGIS is an exempt agency for the purposes of the *Freedom of Information Act 1982* and as such the Information Publication Scheme 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:

- that procurement methods are efficient and cost-effective and take account of the IGIS's security needs, specialised role and size
- that value for money is always the primary guiding principle
- participation in mandatory whole-of-government coordinated procurement, such as for 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 2024–25 are shown in the following tables.

Table 4.5: Reportable consultancy contracts 2024–25

Contract types	Number	Expenditure (GST inc.)
New contracts entered into during the reporting period	1	\$35,250.00
Ongoing contracts entered into during a previous reporting period	5	\$144,343.99
Total	6	\$179,603.99

Table 4.6: Reportable consultancy contract expenditure 2024–25

Name of organisation	Organisation ABN	Expenditure (GST inc.)
Bull & Bear Special Assignments Pty Ltd	23 095 856 554	\$35,250.00
Optimum Business Consulting Pty Ltd	48 091 681 462	\$16,000.00
PQQC Consulting	94 484 818 597	\$15,000.00
The ITSM Hub Pty Ltd	89 165 912 087	\$2,904.00
Work Science Pty Ltd	49 118 332 880	\$66,449.99
Yardstick Advisory Pty Ltd	38 158 309 150	\$44,000.00

During 2024–25, one new reportable consultancy contract was entered into involving actual expenditure of \$35,250.00. In addition, 5 ongoing reportable consultancy contracts were active during the period, involving actual expenditure of \$144.353.99.

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 2024–25 are shown in the following tables.

Table 4.7: Reportable non-consultancy contracts 2024–25

Contract types	Number	Expenditure (GST inc.)
New contracts entered into during the reporting period	20	\$651,094.17
Ongoing contracts entered into during a previous reporting period	4	\$63,120.40
Total	24	\$714,214.57

Table 4.8: Reportable non-consultancy contract expenditure 2024–25

Name of organisation	Organisation ABN	Expenditure (GST inc.)
Comcare Australia	41 640 788 304	\$17,977.80
Sparke Helmore Lawyers	78 848 387 938	\$64,146.00
Data#3 Limited	31 010 545 267	\$28,258.81
Comcover	61 970 632 495	\$25,646.20
Wormald Australia Pty Ltd	80 008 399 004	\$42,124.50
CurbyMcLintock Pty Ltd	48 617 098 503	\$39,000.00
Test Grid (Aust) Pty Ltd	35 090 542 911	\$55,000.00
LexisNexis Australia	70 001 002 357	\$25,425.46
IIT Training Pty Ltd	89 001 555 700	\$39,315.93
Australian Public Service Commission	99 470 863 260	\$22,500.00
Technology One Limited	84 010 487 180	\$23,805.14
Horizon One Recruitment Pty Ltd	98 129 885 838	\$30,390.12
Calleo Resourcing Pty Ltd	29 606 001 763	\$3,130.88
Ashurst Australia	75 304 286 095	\$12,400.00
Australian Government Solicitor	69 405 937 639	\$35,796.50
Resolve Software Group Pty Ltd	87 063 320 696	\$194,008.80
OPC IT Pty Ltd	29 008 657 618	\$19,122.42
ADECCO Australia Pty Ltd	91 006 253 336	\$30,820.01
Agora Consulting Pty Ltd	28 604 109 604	\$5,346.00

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 2024–25, the IGIS exempted from publication 9 contracts with the total value of \$365,642.13.

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 2025:

- (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 2025 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 2025 and for the year then ended:

- Statement by the Accountable Authority and Chief Financial Officer;
- Statement of Comprehensive Income;
- Statement of Financial Position;
- Statement of Changes in Equity;
- Cash Flow Statement; and
- Notes to the financial statements, comprising 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 (the Inspector-General) 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 is also responsible for such internal control as the Inspector-General 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 is responsible for assessing the ability of the Entity to continue as a going concern, taking into account whether the Entity's operations will cease as a result of an

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

administrative restructure or for any other reason. The Inspector-General 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



Lesa Craswell
Group Executive Director

Delegate of the Auditor-General

Canberra
8 August 2025

CONTENTS

Certification

Primary financial statements

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

Overview

Notes to the financial statements:

1. Financial Performance
 - 1.1 Expenses
 - 1.2 Own-Source Revenue and Gains
2. Financial Position
 - 2.1 Financial Assets
 - 2.2 Non-Financial Assets
 - 2.3 Payables
 - 2.4 Interest Bearing Liabilities
3. Funding
 - 3.1 Appropriations
 - 3.2 Net Cash Appropriation Arrangements
4. People and relationships
 - 4.1 Employee Provisions
 - 4.2 Key Management Personnel Remuneration
 - 4.3 Related Party Disclosures
5. Managing uncertainties
 - 5.1 Contingent Assets and Liabilities
 - 5.2 Financial Instruments
 - 5.3 Fair Value Measurement
6. Other information
 - 6.1 Current/non-current distinction for assets and liabilities

STATEMENT BY THE ACCOUNTABLE AUTHORITY AND CHIEF FINANCIAL OFFICER

In our opinion, the attached financial statements for the year ended 30 June 2025 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

8 August 2025

Signed.....

Ms Gerlinde Nicolson
Chief Financial Officer

8 August 2025

Statement of Comprehensive Income

for the period ended 30 June 2025

	Notes	2025 \$	2024 \$	Original Budget \$
NET COST OF SERVICES				
Expenses				
Employee benefits	1.1A	8,301,533	7,732,668	11,218,000
Suppliers	1.1B	3,320,454	3,663,159	5,060,000
Depreciation and amortisation	2.2A	817,905	1,642,618	428,000
Finance costs		297,047	-	-
Write-down and impairment of assets	2.2A	3,500	21,641	-
Total expenses		12,740,439	13,060,086	16,706,000
Own-source income				
Own-source revenue				
Revenue from contracts with customers	1.2A	43,747	33,842	-
Other revenue	1.2B	52,000	50,000	86,000
Total own-source revenue		95,747	83,842	86,000
Gains				
Gains from sale of assets		9,905	-	-
Total gains		9,905	-	-
Total own-source income		105,652	83,842	86,000
Net (cost of) services		(12,634,787)	(12,976,244)	(16,620,000)
Revenue from Government	1.2C	16,192,000	13,417,000	16,192,000
Surplus/(Deficit) attributable to the Australian Government		3,557,213	440,756	(428,000)
OTHER COMPREHENSIVE INCOME				
Items not subject to subsequent reclassification to net cost of services				
Changes in asset revaluation reserve		4,557	-	-
Total comprehensive income/(loss)		3,561,770	440,756	(428,000)

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

Budget Variances Commentary

Statement of Comprehensive Income

OIGIS is reporting a total comprehensive income variance of \$3.99m from the original budget due to lower than anticipated staffing levels and supplier expenditure related to the application of AASB 16 *Leases*. Further analysis is included below.

Employee benefits

Employee expenses were \$2.92m (26%) lower than the original budget. OIGIS achieved an actual ASL of 43 for the year against a funded ASL of 69. Factors that contributed to this included the lengthy security clearance (TSPV) process required for all OIGIS staff, external labour market shortages in key skill areas 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 \$1.74m (34%) lower than the original budget. This is partially due to the application of AASB 16 *Leases* that was applied in 2024-25 with the commencement of the new Memorandum of Understanding. Other contributors include lower than anticipated ASL and less expenditure incurred for travel and training expenditure.

Finance Costs

Finance Costs were incurred for the first time in 2024-25 due to the first time adoption of AASB 16 *Leases*.

Depreciation and amortisation

Depreciation and amortisation expenses were \$0.39m higher than the original budget. This is a direct result of the recognition of the Right of Use asset associated with the lease.

Statement of Financial Position

as at 30 June 2025

		2025	2024	Original Budget
	Notes	\$	\$	\$
ASSETS				
Financial assets				
Cash and cash equivalents	2.1A	483,290	805,045	522,000
Trade and other receivables	2.1B	31,458,367	31,089,788	32,562,000
Total financial assets		31,941,657	31,894,833	33,084,000
Non-financial assets				
Leasehold improvements	2.2A	10,000	11,429	-
Property, plant and equipment	2.2A	504,910	673,896	841,000
Right-of-use	2.2A	6,435,397	-	-
Intangibles	2.2A	-	265	507,000
Prepayments		273,717	247,701	238,000
Total non-financial assets		7,224,024	933,291	1,586,000
Total assets		39,165,681	32,828,124	34,670,000
LIABILITIES				
Payables				
Suppliers	2.3A	420,782	270,041	301,000
Other payables	2.3B	380,360	478,699	-
Total payables		801,142	748,740	301,000
Interest bearing liabilities				
Leases	2.4A	6,682,050	-	-
Total interest bearing liabilities		6,682,050	-	-
Provisions				
Employee provisions	4.1A	2,006,546	1,615,440	2,548,000
Total provisions		2,006,546	1,615,440	2,548,000
Total liabilities		9,489,738	2,364,180	2,849,000
Net assets		29,675,943	30,463,944	31,821,000
EQUITY				
Contributed equity		3,975,425	8,325,196	9,322,000
Reserves		247,957	243,400	244,000
Retained surplus/(Accumulated deficit)		25,452,561	21,895,348	22,255,000
Total equity		29,675,943	30,463,944	31,821,000

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 \$1.10m (3%) lower than the original budget. This variance is a combination of the movement of funds of \$3.72m and the unspent appropriation that has materialised due to the surplus generated in 2024-25 as outlined in the Statement of Comprehensive Income budget variances commentary.

Non-financial assets

Non-financial assets have increased by \$5.64m over the original budget due to the initial recognition of the Right of Use asset in accordance with AASB16 *Leases*.

Employee provisions

Employee provisions are \$0.54m (21%) lower than the original budget. This is reflective of the lower actual ASL of 43 compared to a funded ASL of 69 at 30 June 2025.

Statement of Changes in Equity

for the period ended 30 June 2025

		2025	2024	Original Budget
	Notes	\$	\$	\$
CONTRIBUTED EQUITY				
Opening balance		8,325,196	10,747,189	9,031,000
Transactions with owners				
Distributions to owners				
Returns of capital	3.1B	(4,640,771)	(2,705,993)	-
Contributions by owners				
Departmental capital budget		291,000	284,000	291,000
Closing balance as at 30 June		3,975,425	8,325,196	9,322,000
RETAINED EARNINGS				
Opening balance		21,895,348	21,454,592	22,683,000
Comprehensive income				
Surplus/(Deficit) for the period		3,557,213	440,756	(428,000)
Closing balance as at 30 June		25,452,561	21,895,348	22,255,000
ASSET REVALUATION RESERVE				
Opening balance		243,400	243,400	244,000
Comprehensive income				
Other comprehensive income		4,557	-	-
Closing balance as at 30 June		247,957	243,400	244,000
TOTAL EQUITY				
Opening balance		30,463,944	32,445,181	31,958,000
Surplus/(Deficit) for the period		3,557,213	440,756	(428,000)
Other comprehensive income		4,557	-	-
Transactions with owners		(4,349,771)	(2,421,993)	291,000
Closing balance as at 30 June		29,675,943	30,463,944	31,821,000

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 \$4,640,771 were quarantined under s.51 and returned to the Official Public account.

Comprehensive Income and Other Comprehensive Income

Variance is reflective of the surplus generated in 2024-25 as outlined in the Statement of Comprehensive Income.

Cash Flow Statement

for the period ended 30 June 2025

		2025	2024	Original Budget
	Notes	\$	\$	\$
OPERATING ACTIVITIES				
Cash received				
Appropriations		12,190,040	12,175,777	16,468,000
Net GST received		117,393	191,196	100,000
Receipts from services		43,747	33,842	86,000
Other		542,288	443,576	-
Total cash received		12,893,468	12,844,391	16,654,000
Cash used				
Employees		8,559,212	8,279,585	10,791,000
Suppliers		3,296,678	3,837,843	5,160,000
Interest payments on lease liabilities		297,047	-	-
Section 74 receipts transferred to OPA		713,333	443,576	-
Total cash used		12,866,270	12,561,004	15,951,000
Net cash from operating activities		27,198	283,387	703,000
INVESTING ACTIVITIES				
Cash received				
Proceeds from sale of assets		9,905	-	-
Total cash received		9,905	-	-
Cash used				
Purchase of property, plant and equipment		40,702	21,898	994,000
Total cash used		40,702	21,898	994,000
Net cash (used by) investing activities		(30,797)	(21,898)	(994,000)
FINANCING ACTIVITIES				
Cash received				
Contributed equity		40,657	21,898	291,000
Total cash received		40,657	21,898	291,000
Cash used				
Principal payments of lease liabilities		358,813	-	-
Total cash used		358,813	-	-
Net cash from/(used by) financing activities		(318,156)	21,898	291,000
Net increase/(decrease) in cash held		(321,755)	283,387	-
Cash and cash equivalents at the beginning of the reporting period		805,045	521,658	522,000
Cash and cash equivalents at the end of the reporting period	2.1A	483,290	805,045	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 have been considered and do not have a material effect on OIGIS's financial statements.

During 2024-25 OIGIS has applied AASB16 *Leases* for the first time. This occurred in conjunction with the signing of the new Memorandum of Understanding on 1 July 2024. The application of this standard has implications across the financial statements with a decrease in property costs and an increase in finance costs on the Statement of Comprehensive Income and the capitalisation of a Lease Right of Use (RoU) asset and associated depreciation and recognition of a lease liability on the Statement of Financial Position.

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 2025

1.1 Expenses

	2025	2024
	\$	\$
1.1A: Employee benefits		
Wages and salaries	6,580,560	5,162,222
Superannuation		
Defined contribution plans	692,368	548,431
Defined benefit plans	390,771	889,172
Leave and other entitlements	637,834	1,132,843
Total employee benefits	8,301,533	7,732,668

Accounting Policy

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

	2025	2024
	\$	\$
1.1B: Suppliers		
Goods and services supplied or rendered		
Audit Fees	52,000	50,000
Consultants	156,176	347,884
Contractors	38,160	321,627
ICT and communication	1,306,392	1,023,314
Insurance	21,519	24,387
Legal	80,688	30,312
Property ¹	178,696	671,724
Recruitment and HR	347,859	216,525
Security vetting	482,333	464,535
Training	301,578	149,379
Travel	107,703	229,396
Other	236,209	126,902
Total goods and services supplied or rendered	3,309,313	3,655,985
Other suppliers		
Workers compensation expenses	11,141	7,174
Total other suppliers	11,141	7,174
Total suppliers	3,320,454	3,663,159

1. Decrease relates to the application of AASB 16 *Leases* from 1 July 2024.

1.2 Own-Source Revenue and Gains

	2025	2024
	\$	\$

Own-Source Revenue

1.2A: Revenue from contracts with customers

Rendering of services	43,747	33,842
Total revenue from contracts with customers	43,747	33,842

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.

	2025	2024
	\$	\$

1.2B: Other revenue

Resources received free of charge		
Remuneration of auditors	52,000	50,000
Total other revenue	52,000	50,000

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.

	2025	2024
	\$	\$

1.2C: Revenue from Government

Appropriations		
Departmental appropriations	16,192,000	13,417,000
Total revenue from Government	16,192,000	13,417,000

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

	2025	2024
	\$	\$
2.1A: Cash and cash equivalents		
Cash on hand or on deposit	483,290	805,045
Total cash and cash equivalents	483,290	805,045

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.

	2025	2024
	\$	\$
2.1B: Trade and other receivables		
Appropriation receivables		
Appropriation receivable - Operating	30,765,909	26,969,136
Appropriation receivable - DCB	570,093	4,042,000
Total appropriation receivables	31,336,002	31,011,136
Other receivables		
GST receivable from the Australian Taxation Office	12,615	15,481
Inter-agency staff leave transfers	108,226	61,647
Other	1,524	1,524
Total other receivables	122,365	78,652
Total trade and other receivables	31,458,367	31,089,788

Credit terms for goods and services were within 30 days (2024: 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 2025 (2024: 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 2024					
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 1 July 2024	11,429	673,896	-	265	685,590
Additions					
Purchase or internally developed	-	40,702	-	-	40,702
Right-of-use assets	-	-	7,040,863	-	7,040,863
Revaluations and impairments recognised in other comprehensive income	(857)	5,414	-	-	4,557
Write-downs recognised in net cost of services	-	(3,500)	-	-	(3,500)
Depreciation and amortisation	(572)	(211,602)	(605,466)	(265)	(817,905)
Total as at 30 June 2025	10,000	504,910	6,435,397	-	6,950,307
Total as at 30 June 2025 represented by					
Gross book value	10,000	504,910	7,040,863	937,893	8,493,666
Accumulated depreciation, amortisation and impairment	-	-	(605,466)	(937,893)	(1,543,359)
Total as at 30 June 2025	10,000	504,910	6,435,397	-	6,950,307

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 valuation was conducted in 2024-25 by an independent valuer, CBRE.

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

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

Accounting Policy

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

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

Asset Recognition Threshold

Purchases of leasehold improvements and property, plant and equipment are recognised initially at cost in the statement of financial position, except for purchases costing less than \$2,000, which are expensed in the year of acquisition (other than where they form part of a group of similar items which are significant in total).

Lease Right of Use (ROU) Assets

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

Revaluations

Following initial recognition at cost, property, plant and equipment and leasehold improvements (excluding ROU assets) are carried at fair value (or an amount not materially different from fair value) less subsequent accumulated depreciation and accumulated impairment losses. Valuations are conducted with sufficient frequency to ensure that the carrying amounts of assets did not differ materially from the assets' fair values as at the reporting date. The regularity of independent valuations depended upon the volatility of movements in market values for the relevant assets. 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 in 2024-25 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:

	2025	2024
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 cash-generating assets and assets held at cost, including intangibles and ROU assets, were assessed for impairment at 30 June 2025. 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. For non-cash generating assets held at fair value, the recoverable amount is expected to be materially the same as fair value at 30 June 2025.

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 (2024: 3 years).

All software assets were assessed for indications of impairment as at 30 June 2025.

2.3 Payables

	2025	2024
	\$	\$

2.3A: Suppliers

Trade creditors	420,782	270,041
Total suppliers	420,782	270,041

Average days of settlement are 20 days (2024: 20 days).

	2025	2024
	\$	\$

2.3B: Other payables

Salaries and wages	249,264	221,608
Superannuation	51,421	34,697
Leave balance transfers	69,128	212,583
Other	10,547	9,811
Total other payables	380,360	478,699

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

2.4 Interest Bearing Liabilities

	2025	2024
	\$	\$
2.4A: Leases		
Lease liabilities	6,682,050	-
Total leases	6,682,050	-
Maturity analysis - contractual undiscounted cash flows		
Within 1 year	674,938	-
Between 1 to 5 years	2,874,560	-
More than 5 years	4,967,972	-
Total leases	8,517,470	-

Total cash outflow for leases for the year ended 30 June 2025 was \$655,860 (2024: nil).

OIGIS has one motor vehicle lease and one property lease.

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

Accounting Policy

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

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

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

Funding

This section identifies OIGIS funding structure.

3.1 Appropriations

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

Annual Appropriations for 2025

	Annual Appropriation ¹ \$	Adjustments to appropriation ² \$	Total appropriation \$	Appropriation applied in 2025 (current and prior years) \$	Variance ³ \$
Departmental					
Ordinary annual services	16,192,000	713,333	16,905,333	(12,511,795)	4,393,538
Capital Budget ⁴	291,000	-	291,000	(40,657)	250,343
Total departmental	16,483,000	713,333	17,196,333	(12,552,452)	4,643,881

1. No amounts of current year annual appropriation have been withheld under section 51 of the PGPA Act or quarantined for administrative purposes.

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 \$291,000.

Annual Appropriations for 2024

	Annual Appropriation \$	Adjustments to appropriation ¹ \$	Total appropriation \$	Appropriation applied in 2024 \$	Variance ² \$
Departmental					
Ordinary annual services	13,596,000	477,418	14,073,418	(11,926,232)	2,147,186
Capital Budget ³	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. 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. 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 \$284,000.

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

	2025	2024
	\$	\$
Departmental		
Appropriation Act (No. 1) 2021-22 ¹	-	608,229
Appropriation Act (No. 1) 2021-22 - DCB ¹	-	252,102
Appropriation Act (No. 3) 2022-23 - Supply Act ^{2,3}	949,521	7,345,000
Appropriation Act (No. 1) 2022-23 - Supply Act ²	-	5,794,561
Appropriation Act (No. 3) 2022-23 - DCB - Supply Act ^{2,6}	2,192,000	2,192,000
Appropriation Act (No. 1) 2022-23 - DCB - Supply Act ^{2,5}	1,530,250	1,566,000
Appropriation Act (No. 1) 2023-24 ⁴	14,039,576	14,039,576
Appropriation Act (No. 1) 2023-24 - DCB	279,093	284,000
Appropriation Act (No. 1) 2024-25	16,905,333	-
Appropriation Act (No. 1) 2024-25 - DCB	291,000	-
Cash and cash equivalents	483,290	805,045
Total departmental	36,670,063	32,886,513

1. Appropriation lapsed on 1 July 2024.

2. Appropriation will lapse on 1 July 2025.

3. As at 30 June 2025, \$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 2025, \$179,000 of the Appropriation Act (No. 1) 2023-24 was withheld under section 51 of the PGPA Act.

5. As at 30 June 2025, \$1,530,250 of the Appropriation Act (No. 1) 2022-23 - DCB - Supply Act was withheld under section 51 of the PGPA Act.

6. As at 30 June 2025, \$2,192,000 of the Appropriation Act (No. 3) 2022-23 - DCB - Supply Act was withheld under section 51 of the PGPA Act.

3.2 Net Cash Appropriation Arrangements

	2025	2024
	\$	\$
Total comprehensive income - as per the Statement of Comprehensive Income	3,561,770	440,756
Plus: depreciation/amortisation of assets funded through appropriations (departmental capital budget funding and/or equity injections) ¹	212,439	1,642,618
Plus: depreciation of right-of-use assets ²	605,466	-
Less: lease principal repayments ²	(358,813)	-
Net Cash Operating Surplus	4,020,862	2,083,374

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

	2025	2024
	\$	\$
4.1A: Employee provisions		
Leave	2,006,546	1,615,440
Total employee provisions	2,006,546	1,615,440

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 2025. 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 PSS is a defined benefit scheme 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:

	2025 \$	2024 \$
Short-term employee benefits	1,563,287	1,398,720
Post-employment benefits	179,712	177,315
Other long-term employee benefits	23,512	19,254
Total key management personnel remuneration expenses¹	1,766,511	1,595,289

The total number of key management personnel that are included in the above table are 6 (2024: 6). Substantively, 5 key management personnel positions remain in place during 2025, 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 (2024: 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 2025 there were no contingent assets or liabilities (2024: nil).

Unquantifiable Contingencies

As at 30 June 2025 there were no unquantifiable contingent assets or liabilities (2024: 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

	2025	2024
	\$	\$
5.2A: Categories of financial instruments		
Financial Assets		
Financial assets at amortised cost		
Cash and cash equivalents	483,290	805,045
Total financial assets at amortised cost	483,290	805,045
Total financial assets	483,290	805,045
Financial Liabilities		
Financial liabilities measured at amortised cost		
Suppliers	420,782	270,041
Total financial liabilities measured at amortised cost	420,782	270,041
Total financial liabilities	420,782	270,041

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	
	2025	2024
	\$	\$
Non-financial assets		
Leasehold improvements	10,000	11,429
Property, plant and equipment	504,910	673,896
Total non-financial assets	514,910	685,325

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 in 2024-25. 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

	2025	2024
	\$	\$
Assets expected to be recovered in:		
No more than 12 months		
Cash and cash equivalents	483,290	805,045
Trade and other receivables	31,458,367	31,089,788
Prepayments	273,717	247,701
Total no more than 12 months	32,215,374	32,142,534
More than 12 months		
Leasehold improvements	10,000	11,429
Property, plant and equipment	504,910	673,896
Right-of-use	6,435,397	-
Intangibles	-	265
Total more than 12 months	6,950,307	685,590
Total assets	39,165,681	32,828,124
Liabilities expected to be settled in:		
No more than 12 months		
Suppliers	420,782	270,041
Other payables	380,360	478,699
Leases	393,884	-
Employee provisions	873,462	757,160
Total no more than 12 months	2,068,488	1,505,900
More than 12 months		
Leases	6,288,166	-
Employee provisions	1,133,084	858,280
Total more than 12 months	7,421,250	858,280
Total liabilities	9,489,738	2,364,180

Appendix A: Entity resource statements and resource for outcomes

Figure 5.1: Entity Resource Statement and Resource for Outcomes 2024–25

	Actual available appropriation for 2024–25 \$'000 (a)	Payments made 2024–25 \$'000 (b)	Balance remaining 2024–25 \$'000 (a) – (b)
Departmental			
Annual appropriations – prior year departmental	32,026	12,552	19,474
Annual appropriations – ordinary annual services	16,483	–	16,483
Annual appropriations – s 74 relevant agency receipts	713	–	713
Annual appropriations – other services – non-operating	–	–	–
Total departmental annual appropriations	49,222	12,552	36,670
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)	49,222	12,552	36,670
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)	49,222	12,552	36,670

Figure 5.2: Expenses and resources for Outcome 1

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

Outcome 1: Independent assurance for the Prime Minister, ministers and parliament as to whether Australia's intelligence and security agencies act legally and with propriety by inspecting, inquiring into and reporting on their activities.	Budget	Actual	Variation
	2024-25	2024-25	2024-25
	\$'000	\$'000	\$'000
	(a)	(b)	(a) – (b)
Program 1.1: Office of the Inspector-General of Intelligence and Security			
Departmental expenses			
Departmental appropriation ¹	16,192	11,826	4,366
Special appropriations	–	–	–
Special accounts	–	–	–
Expenses not requiring appropriation in the Budget year ²	514	914	(400)
Total expenses for Program 1.1	16,706	12,740	3,966
Outcome 1 totals by appropriation type			
Departmental expenses			
Departmental appropriation ¹	16,192	11,826	4,366
Special appropriations	–	–	–
Special accounts	–	–	–
Expenses not requiring appropriation in the Budget year ²	514	914	(400)
Total expenses for Outcome 1	16,706	12,740	3,966
	Budget	Actual	Variation
	2024-25	2024-25	2024-25
Average Staffing Level (number)	69	43	26

1. Full-year budget, including any subsequent adjustment made to the 2024-25 Budget at Additional Estimates

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

This section provides information on the oversight activities of the IGIS throughout 2024–25. It details the work of the IGIS with respect to our legislative mandate, which includes assessing the activities of intelligence agencies to ensure they act legally, with propriety and consistently with human rights. This section outlines both our proactive and reactive oversight work, with an emphasis on inquiries, inspections, complaints and PIDs.

Subject to the requirements of security, this section provides information on these oversight activities, both specific to the agencies we oversee and with respect to complaints and PIDs, general trends and analysis.

Over the course of 2024–25, the IGIS:

- completed one inquiry under the IGIS Act that came about through the making of a PID by a former public official under the PID Act
- commenced 82 inspections and completed 74
- received 64 complaints, and closed 41
- completed 2 investigations under the PID Act.

IGIS oversight of intelligence agencies can be broadly split into 2 categories – proactive and reactive. The IGIS's proactive oversight work includes the risk-based inspection programs delivered each year in accordance with section 9A of the IGIS Act, as well as inquiries (both preliminary and substantive). Reactive oversight work is where the IGIS is responding to notifications or engagement from the agencies or the general public. It includes assessment of compliance matters identified by the agencies and disclosed to the IGIS, and receipt and assessment of complaints and PIDs under the IGIS Act.

IGIS inspection work incorporates initial engagement with and briefings from the intelligence agencies (including relevant operational staff), review of material related to the subject of the inspection, follow-up engagement with the agency to seek clarification or responses based on the material reviewed, and preparation of inspection findings that outline the conclusions and any recommendations of the IGIS.

Given the complex operating environment of the intelligence agencies, the IGIS has continued to incorporate and focus on inspection areas where there is significant work being undertaken jointly by agencies. These cross-agency inspections allow inspection teams to review and assess work being undertaken from multiple points of view and provide additional assurance to relevant ministers.

Our complaints and PID work requires us to work with those who have made a complaint or PID, as well as with the relevant intelligence agencies to which the complaint or PID relates.

In relation to both complaints and PIDs, the intelligence agencies provide information and documents to the IGIS in response to preliminary inquiries, inquiries and investigations. At the conclusion of each preliminary inquiry, inquiry and investigation, the intelligence agencies are 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. Where required, formal reports are issued and provided to agency heads and responsible ministers.

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. No concerns in relation to systems or facilities access were identified in 2024–25.

Intelligence agencies

Australian Security Intelligence Organisation

Key statistics



22

Inspections commenced



21

Inspections completed



30

Compliance incidents reported



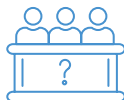
2

Ministerial letters sent to relevant minister



2

Senior-level meetings held



3

Inquiries commenced



42

Complaints received



21

Complaints closed

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*

*The Attorney-General was the responsible minister until May 2025. ASIO was subsequently moved to the Home Affairs portfolio.

Australian Security Intelligence Organisation

In 2024–25, the IGIS's oversight of ASIO consisted of:

- progressing 4 inquiries pursuant to section 17 of the IGIS Act
- inspections of ASIO's activities pursuant to section 9A of the IGIS Act
- one own-motion preliminary inquiry relating to ASIO, which is reported on in 'Cross-agency activities' later in this section
- independent reviews of 30 compliance incident reports received from ASIO
- consideration of 42 complaints
- 2 scheduled meetings between the Inspector-General, the Director-General of Security, the IGIS's senior leadership team and ASIO senior executives (in October 2024 and February 2025).

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 made the following findings with respect to its oversight of ASIO in 2024–25:

- a legality finding with respect to one inspection
- a propriety finding with respect to one inspection

In reviewing ASIO's own assessment of its compliance incidents, the IGIS agreed with ASIO's findings of:

- legislative non-compliance, as identified in 13 compliance incident reports
- non-compliance with Minister's Guidelines, as identified in 8 compliance incident reports
- non-compliance with internal policy and procedure, as identified in 2 compliance incident reports
- non-compliance with an instrument of delegation, as identified in one compliance report
- no non-compliance identified in the investigation of the incident, as identified in 4 compliance incident reports.

The IGIS also made recommendations within a section 25B report that was provided to ASIO.

These findings and recommendations are detailed below under the relevant headings.

Inquiries

Three inquiries were commenced in 2024–25 into specific matters identified through the IGIS's oversight activities. One was initiated in relation to complaints made to the IGIS, and 2 were own-motion inquiries. None of these inquiries were finalised at the end of the reporting period. In addition, there remains an inquiry that was commenced in 2023–24 relating to a complaint that was close to being finalised at the end of the reporting period. The outcomes of these inquiries will be reported on in the 2025–26 annual report.

Inspections

The IGIS commenced 22 inspections of ASIO activities in 2024–25.

Of these 22 inspections, 4 remained underway at the end of the financial year. These relate to:

- non-warranted surveillance devices
- minors
- the TOP SECRET-Privileged Access vetting capability
- a cross-agency examination of warranted collection activity.

The IGIS's findings on these inspections will be reported in 2025–26.

The IGIS completed 21 inspections in 2024–25. In addition to the 18 inspections commenced and completed in 2024–25, the IGIS completed 3 inspections commenced in 2023–24.

Of the 21 inspections completed in 2024–25, 19 did not identify any issues of legality or propriety. These inspections looked into the following matters:

- warrants (4 inspections)
- case inspection (4 inspections)
- human source management (2 inspections)
- security assessments
- covert online operations and SIOs
- cooperation under section 19A of the ASIO Act
- compliance remediation (2 inspections)
- preservation notices
- visa and citizenship referrals
- internal investigations
- foreign liaison and exchange of information.

The IGIS identified issues relating to legality (see 'Industry assistance and access' below) and propriety (see *Respect@Work* on page 91) in 2 of the 21 completed inspections. High-level descriptions of the findings and recommendations appear further below.

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 with regard to the quality of record keeping.

Industry assistance and access

The scope of this inspection included ASIO's use of device access orders under section 34AAD of the ASIO Act, notices provided under section 313 of the *Telecommunications Act 1997* and industry assistance requests issued under Part 15 of that Act. The inspection is conducted annually, and the IGIS has reported concerns in previous annual reports. The IGIS did not identify any legality or propriety concerns which fell within the outlined scope of this inspection. The IGIS did make one legality finding in parallel to the inspection regarding non-compliance with section 24(3A) of the ASIO Act. This legality finding was made following review of material

related to, but not within, the formal scope of the inspection. Section 24(3A) requires the Director-General, as soon as practicable, to cause one or more written records to be made identifying each person who exercised the authority conferred by a relevant warrant. The IGIS identified one instance where the required record did not identify each person who exercised the authority of the warrant. The IGIS will conduct an inspection of ASIO's compliance with these obligations in 2025–26.

Respect@Work

The IGIS conducted a cross-agency inspection focusing on compliance by the 6 agencies in our jurisdiction with the positive duty obligations introduced by the *Anti-Discrimination and Human Rights Legislation Amendment (Respect at Work) Act 2022* (Respect@Work legislation).

The IGIS identified that ASIO had a strong commitment to ensuring a diverse and inclusive workforce, had committed to complying with the Australian Human Rights Commission (AHRC) Good Practice Indicators Framework for Preventing and Responding to Workplace Sexual Harassment (Good Practice Framework), and had implemented additional measures to address the positive duty. The IGIS made a propriety finding about the extent to which ASIO has met the AHRC's key expectations in 4 of the 7 standards identified in the Good Practice Framework. The IGIS made recommendations relating to development of a comprehensive action plan, training and education, policy development, evaluation and assessment, and risk management. The IGIS will revisit the positive duty obligations of Respect@Work in future inspections.

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 2024–25, in all instances the Inspector-General was notified within 24 hours of the Attorney-General granting approval for an SIO.

The ASIO Act also requires the Director-General of Security 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.

In June 2025, the Inspector-General commenced an own-motion inquiry into matters relating to an SIO. This inquiry is ongoing and will be reported in 2025–26.

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 2024–25.

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 2024–25.

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 2024–25, ASIO reported 30 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 one incident outside its control, arising from the actions of another Australian intelligence agency as it exercised the authority conferred by warrants under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) managed by ASIO.

In addition, ASIO reported one matter to the IGIS on propriety grounds where ASIO inadvertently provided a security clearance vetting candidate with information relating to another vetting candidate. The IGIS was satisfied the incident was an error and did not reflect systemic issues with ASIO's processes.

The IGIS reviewed matters of legislative non-compliance reported by ASIO. These incidents and the IGIS's findings, where the matter has been finalised in the reporting period, are outlined below. Two incidents remained under assessment by the IGIS at the end of 2024–25 and will be reported in 2025–26.

Telecommunications (Interception and Access) Act 1979

Non-compliance with section 11B(2)(b) of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) – error in warrant documentation: ASIO notified the IGIS of an incident relating to a warrant issued under section 11B of the TIA Act where the warrant request contained an error in one of the listed telecommunication services. The service was correctly identified in the warrant instrument. The error was not identified until after the Attorney-General had authorised the warrant. Upon identifying the error, ASIO ensured that data was not collected against the service. ASIO assessed that this matter was non-compliant with section 11B(2)(b) of the TIA Act, which requires a warrant request to include details (to the extent known to the Director-General) sufficient to identify the telecommunications service the subject of the warrant is using or likely to use. In this incident, ASIO did not include details that were

known to the Director-General. The IGIS agreed with ASIO's assessment that the incident was non-compliant with section 11B(2)(b) of the TIA Act.

Potential non-compliance with the TIA Act – omission of a telecommunications service from a warrant instrument: ASIO notified the IGIS of an incident relating to a warrant issued under section 11B of the TIA Act where a telecommunications service was omitted from the warrant instrument despite being correctly identified in the warrant request. Following legal advice, ASIO assessed that the matter did not result in non-compliance with the TIA Act. The IGIS agreed with ASIO's assessment.

Non-compliance with section 175 of the TIA Act – error in telecommunications data authorisation: Section 175 of the TIA Act empowers 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 as an eligible person. ASIO notified the IGIS of an incident where an error in the authorisation given by an eligible person resulted in data being requested for a future date. The error was identified by the carrier before it took action, following which ASIO cancelled the request. The IGIS agreed with ASIO's assessment that the incident was non-compliant with section 175 of the TIA Act.

Non-compliance with section 184 of the TIA Act – error in notifications to carriers: Section 184 of the TIA Act provides that where a person makes an authorisation under Division 3 of Part 4-1 of the TIA Act, an ASIO employee or ASIO affiliate must notify the person from whom the disclosure is sought. ASIO notified the IGIS of 3 incidents where the notification of an authorisation made under section 175 of the TIA Act contained an error. In all instances, the error occurred due to manual processes for transcribing information between different IT systems. ASIO assessed each incident to be non-compliant with section 184 of the TIA Act, and the relevant data was deleted. The IGIS agreed with this assessment and ASIO's remediation.

Australian Security Intelligence Organisation Act 1979

Potential non-compliance with the conditions of a warrant issued under section 25A of the ASIO Act: Section 25A of the ASIO Act enables ASIO to obtain a computer access warrant. ASIO notified the IGIS of an incident where the inclusion of incorrect information in the facts and grounds seeking approval to add selectors to a warrant may have resulted in non-compliance with the warrant conditions. ASIO obtained legal advice, following which it assessed that the matter did not result in non-compliance with the warrant conditions or section 3.7 of the Minister's Guidelines. The IGIS agreed with this assessment.

Non-compliance with the Director-General's Instrument of Delegation – security clearance suitability assessments furnished without authority: ASIO notified the IGIS of an incident where an ASIO officer continued to finalise non-prejudicial security clearance suitability assessments after a period of acting at a higher level had expired. The incident occurred because of an oversight in extending the officer's acting arrangement. The officer did not have authorisation under the then Director-General's Instrument of Delegation to make the approvals at their substantive level. On identifying the issue, the security clearance suitability assessments were approved at the correct level and refurnished to relevant agencies. The IGIS agreed with ASIO's assessment that the incident did not result in legislative non-compliance, but was non-compliant with the Director-General's Instrument of Delegation. The IGIS considered ASIO's remediation to be appropriate.

Non-compliance with section 27G(5) of the ASIO Act – failure to notify postal authorisations:

Section 27G of the ASIO Act enables ASIO, where an identified person warrant is in place, to access postal items while the articles are in the course of the post. Section 27G(5) requires ASIO to notify Australia Post of a postal authorisation as soon as practicable and to provide Australia Post with a certified copy of the authorisation. ASIO notified the IGIS that it had failed to notify Australia Post of 2 postal authorisations. ASIO subsequently identified that a total of 10 postal authorisations had not been notified to Australia Post since 2014, when the relevant provisions relating to identified person warrants were enacted. None of the 10 authorisations were executed. ASIO assessed that it was non-compliant with section 27G(5) of the ASIO Act. The IGIS agreed with this assessment and with ASIO's proposed remediation, which included changes to internal policies and procedures, additional reporting to the Attorney-General, advice to Australia Post and an internal review of ASIO's arrangements with Australia Post. The IGIS will review the remediation as part of the regular inspection program.

Potential non-compliance with section 18 of the ASIO Act – errors in communication of intelligence:

Section 18 of the ASIO Act provides that the communication of intelligence on behalf of the Director-General may only be done within the limits of the authority conferred by the Director-General. ASIO notified the IGIS of 2 incidents where intelligence was inadvertently shared with individuals in another agency in error. This occurred due to a technical error and outdated processes. Upon identifying the errors, ASIO undertook remediation, which included ensuring that the intelligence was deleted from other agency systems, and introduced processes to mitigate future incidents. Following legal advice, ASIO assessed that neither matter had resulted in non-compliance with section 18 of the ASIO Act. ASIO also considered whether the incidents were non-compliant with section 63 of the TIA Act as the relevant intelligence had been obtained under a TIA Act warrant. ASIO assessed that neither incident had resulted in non-compliance with section 63. The IGIS agreed with ASIO's assessment and remediation action, which will be reviewed through the regular inspection program.

Minister's Guidelines to ASIO

The Minister's Guidelines are issued under section 8A of the ASIO Act and are to be observed by ASIO in the performance of its functions. On 4 March 2025, the then Attorney-General issued updated Minister's Guidelines, which replaced those that had been issued in August 2020.

Non-compliance with section 2.5 or section 2.6 of the Minister's Guidelines – case reviews:

Section 2.5 of the 2020 Minister's Guidelines and section 2.6 of the 2025 Minister's Guidelines require ASIO to review ongoing investigations no less than annually. ASIO notified the IGIS of 3 incidents where the required review occurred outside the 12-month timeframe. ASIO considered all incidents to be non-compliant with either section 2.5 or section 2.6 of the Minister's Guidelines, and the IGIS agreed with this assessment.

Non-compliance with section 3.7 of the Minister's Guidelines – personal information: Section 3.7 of the 2020 Minister's Guidelines requires ASIO to take all reasonable steps to ensure that personal information used or disclosed by ASIO is relevant, accurate and not misleading. ASIO notified the IGIS of 4 incidents that were non-compliant with section 3.7.

In the first incident, a phone number that was not relevant to security was inadvertently included in a request for subscriber service activity. The error occurred because ASIO's checking processes did not identify that the phone number belonged to an individual who had the same name and lived in the same state as the intended subject. The IGIS agreed with ASIO's assessment that the incident was non-compliant with section 3.7 and will verify deletion of the relevant data through its regular inspection program.

The second incident occurred when a passenger movement alert was raised against an individual who had the same name as, but a different birthdate to, the intended subject of the alert. When the error was identified, the alert was deactivated and relevant data removed from ASIO systems. The IGIS agreed with ASIO's assessment that the incident was non-compliant with section 3.7.

The third incident occurred as the result of 2 separate errors in the attachment to a warrant issued under section 11C of the TIA Act. In the attachment, the name of one of the subjects was spelt incorrectly. Separately, the attachment did not correctly identify the affiliation of another subject. ASIO initially considered that the second error could be non-compliant with section 11C(3A)(a) of the TIA Act. ASIO concluded that the first error was non-compliant with section 3.7 of the Minister's Guidelines and that the second error did not result in non-compliance with the TIA Act. The IGIS agreed with this assessment and ASIO's proposed remediation, which included notifying the Attorney-General of the error in the warrant report.

In the fourth incident, a request for subscriber information contained incorrect information, resulting in a check being undertaken against a phone number that was not relevant to security. The IGIS agreed with ASIO's assessment that the incident was non-compliant with section 3.7, and will verify deletion of the relevant data through its regular inspection program.

Non-compliance with section 2.2b of the Minister's Guidelines – authorisation of investigations: Section 2.2b of the 2020 Minister's Guidelines requires the initiation and continuation of investigations to be authorised by officers at a certain level. ASIO notified the IGIS of an incident where the investigation of 3 entities was approved by an officer who was not authorised to do so. When the error was identified, the rationale for the investigation against the entities was reviewed and approvals made at the correct level. The IGIS agreed with ASIO's assessment that this incident was non-compliant with section 2.2b and considered ASIO's remediation to be appropriate.



Case Study: Minister's Guidelines to ASIO

The Minister's Guidelines are given to the Director-General of Security under section 8A of the ASIO Act and are to be observed by ASIO in the performance of its functions or the exercise of its powers.

Among other things, the stated purpose of the Minister's Guidelines is to support the accountability of the Director-General to the minister and of the minister to the parliament and the people of Australia, the minister's power to direct and guide ASIO, and the IGIS's oversight role.

On 4 March 2025, the Attorney-General issued new Minister's Guidelines to the Director-General. These guidelines were the outcome of an independent review conducted during 2023. The 2025 guidelines replaced a 2020 version, as well as older guidelines relating to foreign intelligence collection and sections 85 and 86 of the ASIO Act.

During the independent review, the IGIS shared with the independent reviewer areas where it considered amendments could be made to the Minister's Guidelines to improve clarity and the effectiveness of IGIS oversight.

From the IGIS's oversight perspective, notable amendments to the Minister's Guidelines include:

- additional reporting requirements for warrants obtained under the ASIO Act and TIA Act, in circumstances where force is authorised and used against a person; and for special intelligence operations, including reporting to the IGIS
- expanded information collection principles in section 3.4, including explicit requirements for children and investigative subjects more generally, and around the sensitivity of information
- new parts relating to foreign interference, foreign intelligence, security vetting and security clearance related activities.

The IGIS reviews ASIO's compliance with the Minister's Guidelines through our regular inspection program. The IGIS's inspections may include any aspect of the guidelines; however, some of the areas on which our inspections have focused or will do so in the future are:

- that ASIO's inquiries and investigations are authorised, conducted and reviewed in accordance with the guidelines
- that there are records of considerations of proportionality and of the information collection principles set out in section 3.4
- that considerations relating to conferral of immunity are documented
- the application of Part 4 relating to the treatment of personal information
- compliance with reporting requirements under Parts 2 and 8
- whether any use of vetting information for ASIO's other functions is consistent with the requirements set out in Part 9
- that ASIO maintains up-to-date policies as required by the guidelines.

On occasion, ASIO reports non-compliance with the Minister's Guidelines to the IGIS. The IGIS's consideration of these incidents is reported in our annual report.

Crimes Act 1914

Non-compliance with the Crimes Act – assumed identities: Part IAC of the *Crimes Act 1914* (Crimes Act) enables ASIO officers to create and use assumed identities for the purpose of performing ASIO's functions. ASIO notified the IGIS of 7 incidents relating to non-compliance with Part IAC of the Crimes Act.

Five incidents related to errors in requests for assumed identity evidence. In the first incident, an historical transcription error in an application for assumed identity evidence was identified when evidence for that assumed identity was renewed. In the second incident, the inclusion of incorrect information in an application for assumed identity evidence was identified when a subsequent request for evidence was made. In the third incident, a spelling error in the name provided in an application for assumed identity information was identified when the evidence was renewed. Upon identifying the errors, ASIO took steps to correct the evidence with the relevant authorities. The fourth incident also related to an historical transcription error in a request for assumed identity evidence. ASIO's investigation of the matter found that the error had been identified several years earlier but not fully remediated. Following this investigation, the assumed identity was cancelled. In the fifth incident, an historical error was identified in assumed identity evidence, arising from a name being recorded incorrectly in ASIO's assumed identity records. Upon identifying the error, ASIO took steps to remediate its records and the relevant evidence. ASIO assessed these incidents to be non-compliant with section 15K(4)(b) of the Crimes Act. The IGIS agreed with this assessment and ASIO's remediation for each incident.

Subsection 15K(2)(b) of the Crimes Act requires assumed identities for non-ASIO officers to be reviewed every 12 months. In the sixth incident, ASIO decided, based on the circumstances of the matter, that an assumed identity for a non-ASIO officer should be recorded as being for an ASIO officer in ASIO's assumed identity management system. This resulted in the deadline for review being set at 3 years rather than 12 months. ASIO was aware of this discrepancy and, although it implemented a manual tracking process, the 12-month deadline for the review was not met. On identifying the issue, ASIO completed the review, which resulted in a decision to cancel the assumed identity. The IGIS agreed with ASIO's assessment that this matter was non-compliant with section 15K(2)(b) of the Crimes Act.

The seventh incident arose from the use of an assumed identity and a piece of evidence that was not registered in ASIO's records to undertake a certain activity. ASIO sought legal advice to determine if any legislative or regulatory non-compliance had occurred. ASIO determined that the matter had not resulted in non-compliance with any legislative or regulatory requirements but that the use of the assumed identity was non-compliant with ASIO's internal policies and procedures. The lack of records relating to the relevant activities was also assessed to be non-compliant with ASIO's internal policies and procedures. The IGIS agreed with ASIO's assessment and proposed remediation action, and will review the remediation as part of the regular inspection program.

Criminal Code Act 1995

Potential non-compliance with section 478.1 of the *Criminal Code Act 1995* (Criminal Code) – access to restricted data: Section 478.1 of the Criminal Code contains offences for accessing or modifying restricted data, which is data held in a computer to which access is restricted by an access control system. ASIO notified the IGIS of potential non-compliance with section 478.1 of the Criminal Code and ASIO's internal procedures arising from an incident where an ASIO staff member conducted online research that may have constituted access to restricted data. Following legal advice, ASIO assessed that there was no legislative non-compliance, but considered that the staff member's actions were non-compliant with ASIO's internal procedures. The IGIS agreed with this assessment and ASIO's proposed remediation action, and will review the remediation as part of the regular inspection program.

State surveillance legislation

Non-compliance with specific state legislation governing the use of surveillance devices – use of surveillance capabilities without warrant: ASIO notified the IGIS that it had identified concerns that relevant legislation in an Australian state prohibits the use of certain surveillance capabilities without a warrant. On identifying the issue, ASIO immediately ceased all relevant operations in the state and in an additional state which has similar legislative provisions, and sought legal advice for all Australian jurisdictions. ASIO assessed that it had conducted a number of operations in the state since the legislation commenced that were non-compliant with the legislation. ASIO's remediation included suspending certain activities and imposing limitations on other activities while it takes action to ensure these capabilities can be used lawfully. ASIO also updated its internal procedures and staff training. The IGIS agreed with ASIO's assessment and will review the remediation as part of the regular inspection program.

Finalisation of 2023–24 compliance incidents

Four compliance incidents that were reported during 2023–24 were finalised by ASIO during 2024–25. Two incidents were determined on further investigation to be compliant, and the IGIS agreed with this assessment. The other 2 incidents remain under consideration by the IGIS – one incident will be considered in the SIO inquiry reported above, and the other has been paused while additional information is obtained from ASIO.

Complaints

The IGIS received 42 complaints about ASIO in 2024–25. This is broadly consistent with the number of complaints received in 2023–24 (41).

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

- commenced 21 preliminary inquiries
- commenced one inquiry which encompasses 8 related complaints
- did not undertake preliminary inquiries or inquiries in relation to 13 complaints during the reporting period.

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

- agency misconduct and surveillance
- processes for conducting security assessments for government functions
- public comment and publications
- data breaches or information sharing
- employment grievances
- recruitment and organisational suitability assessments.

In addition, in this reporting period the Inspector-General:

- prepared one report to ASIO under section 25B of the IGIS Act at the conclusion of the preliminary inquiry (see below)
- progressed an inquiry in response to a complaint received in the previous reporting period. This inquiry was ongoing as at 30 June 2025
- closed 21 complaints, including 6 complaints from the previous reporting period.

At the conclusion of the reporting period 30 complaints about ASIO remained open, which includes 3 from the previous reporting period.



Case Study: Preliminary inquiries with reports made under section 25B of the IGIS Act

After making a preliminary inquiry the Inspector-General may prepare a report to an agency, including conclusions and recommendations, under section 25B of the IGIS Act. During this reporting period, at the conclusion of a preliminary inquiry the Inspector-General issued a report to ASIO which made 3 recommendations.

The preliminary inquiry came about as a result of a complaint that included allegations related to ASIO having acted in a way that negatively affected the complainant's ability to travel to a number of foreign countries. Following receipt of information obtained from ASIO as a result of its preliminary inquiry, the IGIS determined that a formal inquiry was not warranted and that the complaint should be closed under section 11(2)(a), (2)(c) and (3) of the IGIS Act.

The recommendations contained in the preliminary inquiry report provided to ASIO included that ASIO liaise with foreign partners it has shared information with in relation to assessments about a person where those assessments subsequently change. The IGIS's recommendations accepted that ASIO would necessarily take security considerations into account when giving effect to this recommendation.

By the end of this reporting period, ASIO had accepted and actioned, or had undertaken to action, each of these recommendations in the preliminary inquiry report, including the recommendation outlined above.

Australian Secret Intelligence Service

Key statistics



18

Inspections commenced



17

Inspections completed



2

Compliance incidents reported



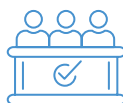
2

Ministerial letters sent to relevant minister



3

Senior-level meetings held



1

Inquiries completed



10

Complaints received



10

Complaints closed

Agency overview

As Australia's foreign intelligence collection agency, ASIS's primary function is to obtain and communicate intelligence – not readily available by other means – about the capabilities, intentions and activities of individuals or organisations outside Australia. ASIS communicates secret intelligence in accordance with government requirements, conducts counter-intelligence activities and liaises with foreign intelligence and security services. Under legislation, ASIS's activities are regulated by a series of ministerial directions, ministerial authorisations, and rules to protect the privacy of Australians.

Relevant Act: *Intelligence Services Act 2001*

Responsible minister: Minister for Foreign Affairs

Australian Secret Intelligence Service

In 2024–25, the IGIS's oversight of ASIS consisted of:

- progressing 2 inquiries, including the completion of one
- inspections of ASIS's activities pursuant to section 9A of the IGIS Act
- one own-motion preliminary inquiry relating to ASIS, which is reported on in 'Cross-agency activities' later in this section
- independent review of 5 compliance incident reports received from ASIS

- consideration of 10 complaints
- 3 scheduled meetings between the Inspector-General, the IGIS's senior leadership team and ASIS senior executives.

The IGIS made the following findings with respect to its oversight of ASIS in 2024–25:

- 3 propriety findings with respect to 3 inspections
- in relation to the IGIS's independent review of compliance incidents reported by ASIS:
 - 4 legality findings
 - 5 propriety findings
- one legality finding related to ASIS's reporting obligations under Schedule 3 of the *Intelligence Services Act 2001* (IS Act)
- one legality finding related to ASIS's historical engagement with section 63 of the TIA Act.

The IGIS also made recommendations within a section 25B report that was provided to ASIS.

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

Inquiries

During this reporting period, the IGIS continued to progress 2 inquiries that had commenced in the 2023–24 reporting period. One of these 2 inquiries was commenced as a result of a complaint made to the IGIS, and the other as a result of a PID. One of these inquiries was completed in 2024–25 and is reported on further below.

Inquiry completed during the reporting period

During the reporting period, the Inspector-General completed an inquiry into a PID made by a former public official in relation to ASIS. This matter was allocated to the IGIS during the 2023–24 reporting period, and it was decided to further investigate the disclosure under the inquiry provisions of the IGIS Act. There were 2 elements to the disclosure. In relation to the first of the 2 elements, the Inspector-General found that there had been no disclosable conduct as alleged by the discloser. Under the second element of the disclosure, the Inspector-General decided not to further inquire into this element pursuant to paragraph 11(2)(c) of the IGIS Act because the first element of the disclosure was not substantiated.

Inspections

Eighteen inspections of ASIS activities were commenced in 2024–25. Of these, 14 are complete, 3 remain underway, and one was rescheduled for 2025–26. These ongoing inspections include inspections of specific intelligence activities in a geographic location, specified operations, and a cross-agency inspection involving ASIS, ASD and ASIO. Findings on these inspections will be reported in the 2025–26 Annual Report.

In one inspection of ASIS's activities in relation to section 13A of the IS Act, the IGIS was not able to access sufficient information, due to technical limitations, to provide reasonable assurance of ASIS's activities. Therefore, the IGIS concluded that it was not possible to conduct the inspection as planned and it has been rescheduled for 2025–26.

The IGIS completed 17 inspections in 2024–25. This includes completion of 3 inspections that commenced in 2023–24. Of the 17 completed inspections, the IGIS did not identify any legality or propriety concerns in 14 inspections that looked into the following matters:

- ministerial submissions (6 inspections)
- activities under Schedules 2 and 3 of the IS Act
- operational files related to ASIS's activities overseas (3 inspections)
- ASIS's automated report publishing program
- ASIS's management of assumed identities
- 2 cross-agency inspections which are reported on in 'Cross-agency activities' later in this section.

The IGIS identified matters relating to propriety in the remaining 3 completed inspections (ministerial directions under section 6(1)(e) of the IS Act), a specific operational intelligence program, and activities in relation to section 13B of the IS Act). High-level summaries of the findings and recommendations of these inspections are provided below.

A summary of the IGIS's inspection of ASIS's activities under Schedules 2 and 3 of the IS Act is also included. The IGIS made one legality finding related to Schedule 3, which was identified independently of the inspection.

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.

Ministerial directions under section 6(1)(e) of the IS Act

The IGIS reviewed ASIS's activities directed by the Foreign Minister under section 6(1)(e) and correlating governance directions under section 8(2)(a) of the IS Act. Under these legislative provisions, the Foreign Minister may direct ASIS to undertake activities relating to the capabilities, intentions or activities of people or organisations outside Australia.

In 2022–23, the IGIS reviewed ASIS's activities under section 6(1)(e) and the supporting legal framework. The IGIS found that ASIS was conducting activities under the Foreign Minister's direction that amounted to an impermissible attempt to delegate the function entrusted to the Foreign Minister. Since that inspection, legislative amendments of section 6(1)(e) have occurred and ASIS has implemented new arrangements for activities conducted under a ministerial direction.

The 2024–25 inspection reviewed ASIS's internal arrangements and activities for a specified period, following the legislative changes. The IGIS identified one propriety finding in relation to non-compliance with the governance directions under section 8(2)(a) of the IS Act; the IGIS was satisfied that this non-compliance was administrative in nature. The IGIS also made one compliance observation on ASIS's governance frameworks relating to the ministerial directions and governance directions. ASIS has accepted these findings.

ASIS's activities and supporting governance framework will be reviewed regularly by the IGIS, including in 2025–26.

Operational intelligence program

This inspection was prompted by a complaint made to the IGIS in 2022–23. In the IGIS's review of the complaint, the IGIS undertook to inspect ASIS's broader operational program as part of the 2023–24 oversight schedule. In this inspection, the IGIS reviewed ASIS's governance and supporting frameworks involved in the delivery of the specified program, as well as a sample of operational activities.

This IGIS found no non-compliance with legislation and was satisfied with the overall management of the program. Nonetheless, this inspection identified one propriety concern and generated a number of compliance observations to improve the governance of the program and related activities. The IGIS provided ASIS with a number of recommendations to strengthen its management of the program. ASIS has implemented a number of changes based on these findings and will brief the IGIS on these efforts at the next senior engagement meeting.

ASIS's activities in relation to section 13B of the IS Act

This inspection is undertaken annually and reviews ASIS's activities conducted under section 13B of the IS Act. Specifically, the IGIS considers if ASIS is operating in line with its legislated functions, with policy requirements, and with regard to human rights. In the course of this inspection, the IGIS identified one propriety concern relating to compliance with internal ASIS policy. The IGIS also identified one compliance error/omission relating to record keeping that did not amount to a propriety concern. ASIS has since rectified the error/omission and the IGIS is satisfied it is not indicative of a systemic issue. ASIS has undertaken to review internal processes to provide clearer guidance to staff.

ASIS's activities under Schedules 2 and 3 of the IS Act

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 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.

The IGIS did not identify any instances of non-compliance with legislation, or any propriety concerns at the time of the inspection. Separately to this inspection, the Director-General of ASIS is required to provide a report to the IGIS in accordance with Schedule 3, clause 1(11) of the IS Act, outlining the actions taken in the Foreign Minister's annual review of approvals made under Schedule 3. While the Director-General has provided the 2024 report to the IGIS, the report for 2023 was not provided, amounting to one instance of non-compliance with legislation. ASIS acknowledged this non-compliance and has implemented internal processes to avoid future incidents.

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.

Compliance incidents

The IGIS independently reviews all compliance incidents reported by ASIS relating to non-compliance with legislation, the Privacy Rules, or internal policies and procedures. 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 2024–25, ASIS provided 2 compliance incident notifications to the IGIS, one of which remains under assessment. The IGIS's review of 4 compliance incident notifications provided in 2023–24 also concluded in 2024–25. All 5 of the finalised compliance incidents identified legislative or propriety concerns.

Themes, findings and recommendations relating to these 5 incidents are outlined below, as well as a legal matter that arose from an inspection activity.

Section 41 of the IS Act

In March 2024, ASIS notified the IGIS of a practice of historical non-compliance with section 41 of the IS Act. Section 41 makes it an offence to identify a person as being, or having been, an agent or staff member of ASIS, where that identification is not of the Director-General of ASIS or such other persons as the Director-General determines, or to make public any information from which the identity of such a person could reasonably be inferred or established (without the Director-General's or Foreign Minister's consent or prior publication by parliament).

ASIS reported to the IGIS an historical practice wherein, prior to November 2022, ASIS did not have policies or procedures in place to ensure compliance with section 41, and identified at least one incident where ASIS disclosed information to a liaison partner without approval from the Director-General in accordance with section 41.

Since November 2022, ASIS's internal practices and policies have changed and, in combination with the remediation action taken following the identification of the legislative non-compliance, the IGIS is satisfied ASIS's extant processes are effective.

Legal Services Directions 2017

The IGIS found one instance of non-compliance with the *Legal Services Directions 2017* (LSDs); specifically, ASIS was non-compliant with Schedule 1, section 2.1 and Appendix A. The specified sections of the LSDs direct that certain types of international law advice can only be provided by specific and identified government providers of legal advice; ASIS is not one of these providers. ASIS self-identified that it was not acting in accordance with these requirements.

ASIS also reported this matter to the Office of Legal Services Coordination (OLSC) and remediation efforts were organised in conjunction with OLSC. The IGIS made no recommendations in relation to this incident.

Section 10A(2) of the IS Act

The IGIS found one instance of non-compliance with section 10A(2) of the IS Act. ASIS failed to report to the Foreign Minister on the operational activity conducted under a ministerial authorisation, issued under section 9 of the IS Act, within 3 months of the day on which the authorisation ceased to have effect.

The IGIS made 2 additional propriety findings relating to this incident. Firstly, it found that ASIS staff failed to ensure the Director-General was informed that the grounds for the authorisation had ceased to exist, which thereby prevented the Director-General from performing their legislative obligations under section 10(2A) of the IS Act. Secondly, it found that ASIS did not report to the Foreign Minister every 6 months as was agreed in the ministerial authorisation. This incident related to ASIS de-prioritising a specific authorised operational activity without following the steps required under sections 10(2A) or 10A(2) of the IS Act or complying with the reporting requirements nominated under the authorisation.

The IGIS provided recommendations to ASIS relevant to the specific circumstances of the incident, which ASIS has accepted and is implementing.

Section 15(1A) of the IS Act

ASIS notified the IGIS of a matter relating to an error that had occurred during its auto-publishing process. In this incident, ASIS inadvertently and incorrectly referenced Australian persons in 4 intelligence reports, due to a technical error in its auto-publishing system.

Under section 15(1A), ASIS must apply its Privacy Rules when communicating intelligence information concerning Australian persons. ASIS had failed to apply the Privacy Rules when it communicated intelligence information concerning Australian persons, amounting to one instance of non-compliance with section 15(1A). The IGIS is satisfied with ASIS's remediation of this incident, which included withdrawing and republishing the affected reports, as well as internal technical updates to avoid future incidents.

Non-recording of the Privacy Rules

The IGIS found 2 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, which ASIS has accepted.

Section 63 of the TIA Act

Following the IGIS's cross-agency inspection of the use of foreign intelligence collection data by the AGO, ASD, ASIO and ASIS, the IGIS identified that ASIS's engagement with section 63 of the TIA Act differed from that of the other relevant agencies, resulting in different compliance incident notifications to the IGIS. Noting the scope of the cross-agency inspection, this issue was reviewed as a separate ASIS compliance matter. The IGIS concluded that ASIS was not notifying the IGIS of non-compliance with section 63(1) of the TIA Act, amounting to non-compliance with the legislation.

Upon receipt of advice from the Australian Government Solicitor, ASIS has accepted that this historical practice was not compliant and has implemented procedural changes to ensure future legislative compliance. These new processes have been reviewed by the IGIS.

Complaints

The IGIS received 10 complaints about ASIS in 2024–25. This is broadly consistent with the number of complaints received in 2023–24 (7).

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

- commenced 5 preliminary inquiries
- commenced no inquiries
- did not undertake preliminary inquiries or inquiries in relation to 5 complaints during the reporting period.

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

- employment grievances
- agency misconduct and surveillance
- recruitment and organisational suitability assessments.

In addition, in this reporting period the Inspector-General:

- completed one inquiry (see the above section on inquiries)
- progressed an inquiry in response to a complaint received in the previous reporting period; this inquiry was ongoing as at 30 June 2025
- prepared one report to ASIS under section 25B of the IGIS Act at the conclusion of a preliminary inquiry (see below)
- closed 10 complaints, including 5 complaints from the previous reporting period.

At the conclusion of the reporting period, 8 complaints about ASIS remained open, which includes 3 from the previous reporting period.

Preliminary inquiry report made under section 25B of the IGIS Act

After making a preliminary inquiry the IGIS may prepare a report to an agency, including conclusions and recommendations, under section 25B of the IGIS Act.

At the conclusion of a preliminary inquiry into a complaint, the IGIS issued a section 25B report to ASIS which made 5 recommendations. The complaint included allegations regarding processes around a code of conduct investigation. The IGIS made recommendations in relation to the specific matter as well as more general recommendations regarding how ASIS could improve its record keeping and administration in relation to such processes. By the end of this reporting period, ASIS had committed to either action, or consider, the 5 recommendations made in the section 25B report.

Australian Signals Directorate

Key statistics



19

Inspections commenced



17

Inspections completed



8

Compliance incidents reported



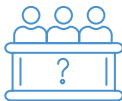
2

Ministerial letters sent to relevant minister



3

Senior-level meetings held



1

Inquiries commenced



10

Complaints received



8

Complaints closed

Agency overview

ASD, which encompasses the Australian Cyber Security Centre, is the Australian Government agency responsible for foreign signals intelligence and cyber security. ASD collects and analyses electronic signals in order to inform Australian Government stakeholders; protect and ensure the security of Australian networks and information; and disrupt threats against Australia's interests. ASD's activities are regulated by a series of ministerial directions, ministerial authorisations and Privacy Rules.

Since 2022, ASD has been progressing REDSPICE (Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers) to expand and develop its capabilities in response to the deteriorating strategic situation in Australia's region. As the types and scale of ASD's activities develop, the IGIS is adapting its oversight activities to ensure they are targeted towards the activities that utilise the most intrusive powers; are new or novel capabilities; and are in areas where issues have previously been identified.

Relevant Act: *Intelligence Services Act 2001*

Responsible minister: Minister for Defence

Australian Signals Directorate

In 2024–25, the IGIS's oversight of ASD consisted of:

- progressing one inquiry pursuant to section 17 of the IGIS Act
- inspections of ASD activities pursuant to section 9A of the IGIS Act
- one own-motion preliminary inquiry relating to ASD, which is reported on in 'Cross-agency activities' later in this section
- finalising the independent review of 11 compliance incident reports received from ASD
- consideration of 10 complaints
- 3 scheduled meetings between the Inspector-General, the IGIS's senior leadership team, the Director-General of ASD and ASD senior executives during the financial year.

With respect to its oversight of ASD in 2024–25, the IGIS made potential legality and propriety findings in respect of one inspection.

In reviewing ASD's own assessments of its compliance incidents, the IGIS agreed with ASD's findings that:

- there was legislative non-compliance, as identified in 8 compliance incident reports
- the investigation of the incident did not result in any non-compliance, as identified in 3 compliance incident reports.

The IGIS also made recommendations within 3 separate section 25B IGIS Act reports that were provided to ASD.

These findings and recommendations are detailed further below.

Inquiries

One inquiry was commenced in 2024–25 on an own-motion basis. This inquiry was not finalised at the end of the reporting period, and its outcomes will be reported on in the 2025–26 annual report.

Inspections

The IGIS commenced 19 inspections of ASD's activities in 2024–25.

Of these 19 inspections, 5 remain underway, including a cross-agency inspection relating to warranted collection activity. The IGIS will report on these inspections in 2025–26.

The IGIS completed 17 inspections in 2024–25. This includes completion of 3 inspections that commenced in 2023–24. In 16 of the 17 inspections completed, the IGIS did not identify any legality or propriety concerns. These inspections covered the following matters:

- the accuracy of information communicated by ASD in ministerial submissions and the legality and propriety of activities undertaken in reliance on a ministerial authorisation (3 inspections)
- ASD's application of the Privacy Rules made under section 15 of the IS Act (3 inspections)
- targeted inspections of ASD's compliance with its obligations under ministerial directions made under section 8 of the IS Act, relevant sections of the TIA Act, and previous IGIS inspection findings (2 inspections)

- a specified foreign intelligence collection capability conducted by ASD with foreign partners
- examination of warranted collection activity (cross-agency inspection)
- ASD's conduct and management of organisational suitability assessments
- ASD's management of a specific operational activity conducted under ministerial authorisation
- ASD's implementation of full knowledge and concurrence requirements
- ASD's management of a program connected to its cyber security function
- ASD's management of assumed identities in accordance with Part IAC of the Crimes Act
- ASD's implementation of the Respect@Work legislation.

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 with regard to improving the quality of record keeping.

The IGIS identified matters relating to potential legality and propriety in one inspection relating to ASD's human rights assessments conducted in support of international relationships and foreign release of intelligence. A high-level summary of the findings and recommendations is provided below.

Additionally, a summary is included below of the IGIS's inspection of ASD's reporting requirements under the Privacy Rules in relation to overturning a presumption of nationality.

Human rights assessments

The IGIS undertook an inspection of ASD's human rights assessments (HRAs) conducted in support of international relationships, including HRAs produced prior to releasing intelligence to foreign partners. ASD's policies and procedures relating to the conduct of HRAs were reviewed, together with the records produced to support the consideration of human rights risks for specific relationships.

The IGIS reviewed ASD's release of intelligence to foreign partners, focusing on how ASD considered the risk of human rights violations occurring as a result of the disclosure. The IGIS noted that ASD had recently updated policies and procedures guiding this process in response to an internal audit. Accordingly, the IGIS made no findings regarding this process.

The IGIS also reviewed ASD's HRAs conducted in support of international relationships outside of releasing intelligence. In this review, the IGIS identified propriety concerns based on ASD's inability to demonstrate consistent and adequate consideration of the human rights risks posed by engaging with specific international partners. The IGIS also observed one instance of potential non-compliance with paragraph 13(1)(c) of the IS Act by cooperating with an authority of another country without the required ministerial approval, and a number of instances of non-compliance with internal procedural and record-keeping policies.

The resulting IGIS recommendations included the need for ASD to review and update its policies and procedures to make clear ASD's expectations as to when an HRA is required outside of the foreign release process. This included a specific recommendation that ASD clarify via policy when it is appropriate to adopt another Australian Government agency's HRA.

Other recommendations included ensuring HRAs are more accessible to staff and that a responsible officer or team is identified to ensure the currency of each HRA. The IGIS will review ASD's HRAs conducted in support of international relationships in a future inspection.

The IGIS notes that since receiving these findings, ASD has sought legal advice concerning the issue of potential legality, and has also obtained approval from the relevant minister pursuant to paragraph 13(1)(c) of the IS Act to cooperate with the relevant authority. The IGIS also notes that despite the identified areas of concern in ASD's consideration of human rights risks, it did not observe any instances where ASD's deficient administrative practices resulted in ASD causing, contributing to or condoning a human rights contravention.

Rules to Protect the Privacy of Australians

The Minister for Defence issues Privacy Rules to regulate the communication and retention by ASD of intelligence information about Australian persons. In 2024–25, the IGIS undertook 3 inspections of ASD's application of the Privacy Rules, and identified no legality or propriety concerns. Each inspection involved the review of a sample of disseminations of intelligence concerning Australian persons in a period. The inspection confirmed that ASD had 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 2025–26.

Overtaken presumptions of nationality

Under the Privacy Rules, ASD must 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. The Privacy Rules include principles for making reasonable assumptions about nationality. If the initial presumption was reasonable based on the information available at the time, and appropriate steps were taken to manage information related to that individual, such incidents do not represent non-compliance with legislation or the Privacy Rules.

In 2024–25, ASD provided 16 reports in which the application of the Privacy Rules resulted in a presumption of nationality being overturned. The IGIS reviewed the circumstances surrounding 14 of these reports. The reviews of 2 reports remain underway and will be reported on in 2025–26.

In each of the 14 reports 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. ASD reported one incident relating to an OPN, which is detailed in 'Compliance incidents' below.

Compliance incidents

The IGIS independently reviews all potential and actual compliance incidents reported by ASD. In conducting this review, the IGIS considers ASD's remediation action in response to the incident and may seek additional information, including capability briefings.

The IGIS's review of potential compliance incidents takes place at the end of ASD's internal investigation and includes reviewing incidents ASD has assessed to be compliant and those it has assessed to be non-compliant with legislation.

In 2024–25, ASD provided:

- 8 notifications of potential compliance incidents at the start of ASD's internal investigation
- 16 reports at the conclusion of ASD's investigation of an incident. These reports included potential incidents initially notified to the IGIS in previous years, where the investigation was concluded in the reporting period.

In 2024–25, the IGIS completed its review of 11 reports: 6 from the reporting period and 5 provided from previous reporting periods. Of the 11 reports reviewed, 8 were assessed by ASD and confirmed by the IGIS to be matters of legislative non-compliance. An overview of these incidents and the IGIS's findings is provided below. The remaining 3 reports were assessed by ASD and confirmed by the IGIS to be compliant with legislation.

At the end of the reporting period, 10 reports of which ASD had concluded its investigation remained under review by the IGIS, and 12 potential compliance incidents continued to be assessed by ASD. These matters will be reported on in subsequent annual reports.

Telecommunications (Interception and Access) Act 1979

Non-compliance with section 108 and section 133 of the TIA Act: ASD notified the IGIS of 2 separate incidents resulting in legislative non-compliance concerning its access to stored communications. The first incident constituted non-compliance with subparagraph 108(1)(a)(i) of the TIA Act by accessing a stored communication, and also non-compliance with subsection 133(1) by making a record of the relevant communication. The second incident constituted non-compliance with subparagraph 108(1)(a)(i) of the TIA Act by accessing a stored communication, non-compliance with subsection 133(1) by making a record of the relevant communication, and non-compliance with subparagraph 108(1)(a)(iii) by enabling access to a stored communication. In both these incidents, ASD incorrectly believed that it had a legal authorisation in place which authorised access to these communications.

Once the errors were identified, ASD took appropriate action, purged all information and updated relevant training material to provide clarity to ASD staff regarding how access to stored communications is authorised. ASD has now obtained an appropriate instrument to authorise access to the relevant communications.

Non-compliance with section 7 and section 63 of the TIA Act: ASD notified the IGIS of 3 separate incidents where ASD was non-compliant with subsection 7(1) and subsection 63(1) of the TIA Act.

The first incident resulted in 4 instances of legislative non-compliance with paragraph 7(1)(c) of the TIA Act by enabling the interception of a communication passing over a telecommunications system, and 4 corresponding instances of non-compliance with subsection 63(1) by communicating or making a record of information intercepted in contravention of subsection 7(1). This incident was initially identified by the IGIS during inspection activity in 2022–23.

The second incident resulted in one instance of legislative non-compliance with paragraph 7(1)(a) of the TIA Act by intercepting a communication passing over a telecommunications system, one instance of non-compliance with subsection 63(1) by communicating or making a record of information intercepted in contravention of subsection 7(1), and one instance of legislative non-compliance with paragraph 7(1)(c) by enabling the interception of a communication passing over a telecommunications system. This incident was identified by ASD staff during an internal audit.

The third incident resulted in one instance of legislative non-compliance with paragraph 7(1)(c) by enabling the interception of a communication passing over a telecommunications system. This incident was also identified by ASD staff during an internal audit.

ASD assessed that all 3 of the incidents occurred due to a misunderstanding regarding applicable exceptions available under the TIA Act, combined with human error when conducting the activities. In response, ASD undertook to review and update relevant procedures that guide the interception activities and to investigate options to integrate automatic system checks.

Noting the repeated nature of the incidents, for completeness the IGIS reviewed all 3 incidents at the same time to identify any systemic weaknesses. The IGIS noted that while each incident may have occurred due to human error, the repeated nature reinforced the need for ASD's processes and systems to be further developed. The IGIS noted that actions are being undertaken by ASD to address the incidents, and will monitor ASD's progress against these and additional recommendations made by the IGIS.

Non-compliance with a provision of the TIA Act: ASD reported one additional incident that constituted a breach of a provision of the TIA Act. The IGIS reviewed the incident and agreed with ASD's assessment, and noted that ASD took reasonable steps to prevent similar instances occurring.

Other legislation

Non-compliance with subsection 8(3) of the IS Act: ASD notified the IGIS of 2 separate incidents when ASD did not comply with subsection 8(3) of the IS Act, which requires an agency head to ensure the agency complies with ministerial directions.

The first incident involved ASD not obtaining a ministerial authorisation prior to conducting activities to obtain intelligence on an Australian person. In this incident, ASD did not conduct appropriate checks, which resulted in ASD not identifying information that would have overturned the presumption of nationality. In response, ASD updated relevant policies and procedures to clearly articulate the required processes to mitigate future recurrence. The IGIS considered the action taken by ASD following the incident to be appropriate in the circumstances.

The second incident involved ASD conducting activities to obtain intelligence on an Australian person beyond the period that was authorised by the ministerial authorisation. In this incident, ASD staff misinterpreted the wording contained in an authorisation concerning its expiration. In response, ASD reviewed and updated its standard operating procedures to clarify expiration dates for authorisations. The IGIS considered the action taken by ASD to be appropriate in the circumstances.

Other reviews

Section 9D of the IS Act authorisation

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

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

Complaints

The IGIS received 10 complaints about ASD in 2024–25. This is lower than the number of complaints received in 2023–24 (15).

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

- commenced 7 preliminary inquiries
- commenced no inquiries
- did not undertake preliminary inquiries or inquiries in relation to 3 complaints during the reporting period.

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

- agency misconduct and surveillance
- employment grievances
- recruitment and organisational suitability assessments
- data breaches or information sharing
- public comment and publications.

In addition, in this reporting period the Inspector-General:

- prepared 3 reports to ASD under section 25B of the IGIS Act at the conclusion of 3 preliminary inquiries, including one own-motion preliminary inquiry (see below)
- closed 8 complaints, including 3 complaints from the previous reporting period.

At the conclusion of the reporting period 5 complaints about ASD remained open, all of which were received during this reporting period.

Preliminary inquiries with reports made under section 25B of the IGIS Act

After making a preliminary inquiry the IGIS may prepare a report to an agency, including conclusions and recommendations, under section 25B of the IGIS Act.

During this reporting period, at the conclusion of a preliminary inquiry into 2 separate complaints, the Inspector-General issued a report to ASD which made 4 recommendations. The complaints included allegations regarding organisational suitability assessments. The Inspector-General made recommendations in relation to the specific matters, as well as more general recommendations regarding ASD conducting a review of certain organisational suitability assessment processes. By the end of this reporting period, ASD had accepted and actioned each of these recommendations.

At the conclusion of another preliminary inquiry into a complaint, the Inspector-General issued a report to ASD which made 3 recommendations. This complaint also included allegations regarding an organisational suitability assessment. The Inspector-General made general recommendations in relation to improvements in communication and administration regarding certain organisational suitability assessment processes. By the end of this reporting period, ASD had accepted and actioned each of these recommendations.

At the conclusion of an own-motion preliminary inquiry, the Inspector-General issued a report to ASD which made 5 recommendations. The own-motion preliminary inquiry examined ASD's administration of PIDs under the PID Act between 2021 and January 2023. The Inspector-General found that ASD had suitable PID procedures and policies and that its actions in handling PIDs were timely and appropriate. The Inspector-General made recommendations in relation to ASD clarifying or amending certain policies and procedures. By the end of this reporting period, ASD had accepted each recommendation, actioned 2 of the recommendations and was on track to complete the remaining 3 recommendations.

Australian Geospatial-Intelligence Organisation

Key statistics



8

Inspections commenced



7

Inspections completed



0

Compliance incidents reported



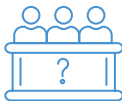
2

Ministerial letters sent to relevant minister



2

Senior-level meetings held



0

Inquiries commenced



1

Complaints received



1

Complaints closed

Agency overview

AGO is Australia's national geospatial-intelligence agency, producing geospatial intelligence derived from fusing the analysis of imagery and geospatial data. Located within the Department of Defence, AGO supports the Australian Government's decision-making and assists with the planning and conduct of Australian Defence Force (ADF) operations. AGO also directly assists Commonwealth and state bodies responding to security threats and natural disasters. A series of ministerial directions, ministerial authorisations and Privacy Rules regulate AGO's activities.

Relevant Act: *Intelligence Services Act 2001*

Responsible minister: Minister for Defence

Australian Geospatial-Intelligence Organisation

In 2024–25, the IGIS's oversight of AGO consisted of:

- inspections of AGO's activities pursuant to section 9A of the IGIS Act
- one own-motion preliminary inquiry relating to AGO, which is reported on in 'Cross-agency activities' later in this section
- review of AGO's use of an emergency authorisation in relation to circumstances which involved an imminent risk to the safety of an Australian person who was outside Australia

- 2 scheduled meetings between the Inspector-General, the IGIS's senior leadership team, the Director of AGO and AGO senior executives.

The IGIS made the following findings with respect to its oversight of AGO in 2024–25:

- 2 legality findings in relation to one inspection
- a propriety finding in relation to one inspection
- one legality finding related to AGO's use of an emergency authorisation.

The IGIS implemented a risk-based approach to its inspections of AGO, given the breadth of AGO's functions under section 6B of the IS Act. In 2024–25, the IGIS focused on areas of higher risk or sensitivity or areas that had not previously been inspected for thematic inspections.

Inspections

Eight inspections of AGO activities were commenced in 2024–25. Of these, 6 are complete and 2 remained underway at the end of 2024–25. One inspection commenced in 2023–24 was also completed. The ongoing inspections include a cross-agency inspection of the compliance of AGO and the DIO with the Respect@Work requirements and an inspection of AGO's governance and use of specified data. Findings on these inspections will be reported in the 2025–26 Annual Report.

Five of the 7 completed inspections did not identify any legality or propriety concerns. The focus of these inspections was:

- one cross-agency inspection, reported on in 'Cross-agency activities' later in this section
- application of AGO's Privacy Rules made under the IS Act
- ministerial authorisations to undertake certain activities and Director of AGO approvals
- provision of geospatial-intelligence products to foreign partners
- assessment of human rights considerations.

The IGIS identified issues relating to legality (AGO's cooperation with foreign authorities) and propriety (adherence to policy on full knowledge and concurrence) in 2 of the 7 completed inspections. A high-level summary of the findings and recommendations is provided below.

More generally, the IGIS provided findings and recommendations, based on compliance observations, from some of the above inspections. Recommendations directed improvements to the clarity of, and compliance with, AGO's internal policies and procedures, or to promote stronger compliance practices.

AGO's cooperation with foreign authorities under section 13(1)(c) of the IS Act

Section 13(1)(c) of the IS Act permits AGO, subject to ministerial arrangement or direction, to cooperate with authorities of other countries that are capable of assisting AGO in the performance of its functions. Section 13(3B) of the IS Act requires the Director of AGO to, as soon as practicable after each year ending on 30 June, give to the Minister for Defence and the IGIS a report about any significant cooperation conducted under section 13(3A). This requirement was introduced in the legislation in 2022 and the Director of AGO was required to report AGO's activities under section 13(3A) as of financial year 2021–22.

The Director of AGO provided the IGIS a report on AGO's section 13(3A) activities for 2023–24 in May 2025. However, the Director of AGO did not provide reports to the IGIS for the previous 2 financial years' activities until requested by the IGIS in May 2025. Accordingly, the IGIS found 2 instances of non-compliance with section 13(3B) of the IS Act: one relating to the failure to give the IGIS a report on these activities for 2021–22 and 2022–23, and one for not providing the reports on activities as soon as practicable after 30 June.

AGO's adherence to the Department of Defence's full knowledge and concurrence policy

Australia's policy of full knowledge and concurrence requires AGO to have a full and detailed understanding of any relevant capability or activity with a presence on Australian territory or making use of Australian assets.

The IGIS identified one propriety finding regarding the mechanisms in place to assure adherence to the full knowledge and concurrence principles relating to one low-risk capability. The IGIS recommended that AGO review the assurance mechanism for this capability and advise the IGIS once this had occurred.

Rules to Protect the Privacy of Australians

AGO's communication and retention of intelligence information about Australian persons is regulated by the Privacy Rules as issued by the Minister for Defence. In 2024–25, the IGIS inspected AGO's application of the Privacy Rules and identified no legality or propriety concerns. The IGIS made 2 recommendations focused on improving guidance for analysts relating to record keeping. As this is an annual inspection, AGO's application of the Privacy Rules will next be inspected in 2025–26.

Compliance incidents

AGO did not report any compliance incidents in 2024–25.

Other reviews

9D authorisation

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

The Inspector-General concluded that the Director of AGO complied with all requirements of section 9D of the IS Act when exercising this power, with one exception, and informed the responsible minister and the PJCIS as required. The one instance of non-compliance with legislation related to AGO not notifying the Minister for Defence and the IGIS of the cancellation as soon as practicable as required by section 9D(13) of the IS Act. AGO accepted this finding and adjusted its processes to prevent a recurrence of this incident.

Complaints

The IGIS received one complaint about AGO in 2024–25. This is broadly consistent with the number of complaints received in 2023–24 (0).

The complaint received related to alleged employment grievances, including the conduct of organisational suitability assessments. This was the subject of a preliminary inquiry. The complaint was closed during the reporting period under section 11(2)(c) of the IGIS Act.

In this reporting period the Inspector-General did not prepare any reports to AGO under section 25B of the IGIS Act.

At the conclusion of the reporting period no complaints about AGO remained open.

Defence Intelligence Organisation

Key statistics



7

Inspections commenced



4

Inspections completed



0

Compliance incidents reported



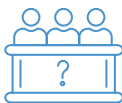
2

Ministerial letters sent to relevant minister



2

Senior-level meetings held



0

Inquiries commenced



0

Complaints received



0

Complaints closed

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 Minister for Defence.

Relevant Act: *Intelligence Services Act 2001*

Responsible minister: Minister for Defence

Defence Intelligence Organisation

In 2024–25, the IGIS's oversight of DIO consisted of:

- inspections of DIO's activities pursuant to section 9A of the IGIS Act
- one own-motion preliminary inquiry relating to DIO, which is reported on in 'Cross-agency activities' later in this section
- 2 scheduled meetings between the Inspector-General, the IGIS's senior leadership team, the Chief of Defence Intelligence and DIO senior executives.

The IGIS implemented a risk-based approach to its inspections of DIO.

The IGIS's oversight of DIO in 2024–25 did not identify any issues of legality or propriety.

Inspections

The IGIS commenced 7 inspections of DIO's activities in 2024–25.

Of these 7 inspections, 4 were completed during the reporting period and 3 remained underway and will be reported on in the 2025–26 Annual Report. In all 4 completed inspections, the IGIS did not identify any issues of legality or propriety.

The completed inspections covered the following activities:

- application of DIO's Privacy Rules made under the IS Act
- the accuracy of information communicated in ministerial submissions
- a specified program
- a specific program that DIO undertakes with partners.

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

Below is a summary of DIO's application of the Privacy Rules, along with an overview of the inspection of a DIO specified program, though no issues were identified.

Compliance with Rules to Protect the Privacy of Australians

The Minister for Defence issues Privacy Rules to regulate the communication and retention by DIO of intelligence information about Australian persons.

In 2024–25, the IGIS undertook one inspection of DIO's application of the Privacy Rules and identified no legality or propriety concerns. The inspection confirmed that DIO continued to have a strong culture of compliance with the Privacy Rules. This culture was evidenced during the reporting period when DIO staff reported one incident of non-compliance with DIO's Privacy Rules policy. The IGIS reviewed the incident and confirmed that while DIO was non-compliant with its governing policy, DIO officers had considered the privacy of Australians at the time the information was being disseminated. The IGIS will continue its regular review of DIO's implementation of the Privacy Rules in 2025–26.

Specified program

The IGIS conducted an inspection of a program of specified activities, which was the subject of 2 prior IGIS inspections, reported in 2021–22 and 2023–24. In the earlier inspections, propriety and procedural concerns were identified, including that those activities conducted within the program may be beyond DIO's mandate.

This inspection reviewed how DIO had addressed earlier inspection findings and involved reviewing policies, supporting procedures and forms, and records associated with the program. The inspection found that DIO had implemented significant changes to the program to address the earlier recommendations. This included amending the DIO mandate to include activities conducted within the program, issuing a new policy, and providing supporting documentation to guide the conduct of the program.

Noting that DIO has addressed concerns raised in earlier IGIS inspections, further inspection work relating to the program will be considered as part of the IGIS's broader risk-based approach to inspections.

Complaints

There were no complaints received about DIO in 2024–25. This was broadly consistent with the number of complaints received in 2023–24 (1).

In this reporting period:

- the Inspector-General did not commence any preliminary inquiry or any inquiry
- the Inspector-General did not prepare any reports to DIO under section 25B of the IGIS Act.

At the conclusion of the reporting period no complaints about DIO remained open.

Office of National Intelligence

Key statistics



4

Inspections
commenced



4

Inspections
completed



2

Compliance
incidents reported



2

Ministerial letters
sent to relevant
minister



2

Senior-level
meetings held



0

Inquiries
commenced



1

Complaints
received



1

Complaints
closed

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 2024–25, the IGIS's oversight of ONI consisted of:

- inspections of ONI's activities pursuant to section 9A of the IGIS Act
- one own-motion preliminary inquiry relating to ONI, which is reported on in 'Cross-agency activities' later in this section
- receiving one compliance incident report
- consideration of one complaint
- 2 scheduled meetings between the Inspector-General, the IGIS's executive team and ONI senior executives in November 2024 and June 2025.

The IGIS made the following findings with respect to its oversight of ONI in 2024–25:

- a propriety finding with respect to one inspection
- a legality finding with respect to a compliance incident report received from ONI.

These findings are detailed further below.

Inspections

The IGIS commenced 4 inspections of ONI activities in 2024–25. Of these, one inspection remains underway and will be reported on in 2025–26.

The IGIS finalised one inspection that commenced in 2023–24.

The IGIS identified propriety-related issues in one of the completed inspections (see ‘Respect@ Work’ below). No issues of legality were identified. A high-level summary of the findings and recommendations of each inspection appears below.

Open-source intelligence functions

The IGIS undertook an inspection of ONI’s open-source intelligence functions, reviewing policies and procedures regarding the collection and use of open-source intelligence and the use and management of online personae.

The inspection found no instances of non-compliance with legislation or propriety concerns; however, minor concerns about aspects of ONI’s persona-related policies and procedures were identified. The IGIS made recommendations to improve record keeping, develop procedures, update policies, and include use and maintenance of online personae in mandatory training.

Rules to Protect the Privacy of 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 personal information of Australian persons in specific circumstances where needed to properly perform its functions. Records of instances where ONI has collected or communicated such 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.

While the IGIS made no findings with respect to legality or propriety, the IGIS found 18 instances of minor administrative non-compliance with the Privacy Rules policy and had minor concerns regarding ONI’s inability to demonstrate consistent application of the Privacy Rules when communicating unpublished or informal products. The IGIS also identified minor concerns relating to incorrectly completed privacy disclosure forms. Despite the number of minor non-compliance matters identified, the IGIS was satisfied that ONI had put in place sufficient mitigation to prevent further error, and noted that the non-compliance was predominantly caused by human error.

The IGIS made recommendations for ONI to consider the development of a centralised database of Australian persons, update the Privacy Rules policy and ensure privacy disclosure forms are completed as per the Privacy Rules policy requirements.

The IGIS will continue to review ONI’s compliance with the Privacy Rules in 2025–26.

Assumed identities

The IGIS reviewed management practices enabling ONI's use of assumed identities under section 15K of the Crimes Act and section 7(1)(g) of the ONI Act.

While the inspection found no instances of non-compliance with legislation or propriety concerns, the IGIS had minor concerns related to ONI failing to comply with the terms of a memorandum of understanding with a partner agency. Specifically, notification in writing did not take place regarding reviews undertaken pursuant to section 15KF of the Crimes Act. Such notification was required under Part 5 of the memorandum of understanding. The IGIS noted that verbal notification did take place and that ONI has undertaken to make future notifications in writing.

Respect@Work

The IGIS undertook a cross-agency inspection of each agency's (including ONI's) compliance with the positive duty obligations introduced by the Respect@Work legislation to eliminate unlawful conduct as described by the *Sex Discrimination Act 1984*. The IGIS has not conducted an inspection on this topic previously.

The inspection identified no non-compliance by ONI with legislation. However, the inspection had one propriety finding relating to ONI's implementation of its positive duty in relation to the broad availability of training resources for staff. The IGIS also had moderate concerns about ONI's lack of communication to staff regarding the Respect@Work changes and an outdated definition within ONI's workplace behaviour policy. The IGIS made recommendations for developing mandatory Respect@Work training, implementing dedicated Respect@Work resources and updating ONI's workplace behaviour policy to include the current definition.

During the course of the inspection and immediately following its conclusion, ONI undertook mitigation steps including the provision of bespoke workplace behaviour training, creating a dedicated Respect@Work intranet page and updating the relevant policy definition such that the IGIS's concerns have been effectively ameliorated.

Compliance incidents

ONI reported one compliance incident to the IGIS which had a legality finding. This incident related to ONI's disclosure to a foreign entity, as governed by the ONI Act under section 13(1). The IGIS found that ONI failed to comply with section 13(1) of the ONI Act, disclosing sensitive information to a foreign entity where that entity had not been approved. A second incident was reported and is included in 'Cross-agency activities' below.

Complaints

The IGIS received one complaint about ONI in 2024–25. This is broadly consistent with the number of complaints received in 2023–24 (0).

The complaint alleged ONI's job advertisements and expressions of interest utilised artificial intelligence and contained numerous errors. The complaint was not the subject of preliminary inquiry or inquiry, and was closed during the reporting period under section 11(2)(b) of the IGIS Act.

In this reporting period the IGIS did not prepare any reports relating to ONI under section 25B of the IGIS Act. At the conclusion of the reporting period no complaints about ONI remained open.



Case Study: Day in the life of an IGIS Oversight Officer

I recently joined the IGIS after a number of years working in the broader Australian Public Service. I was always interested in national security, and I was attracted to the role of Intelligence Oversight Officer (IOO) because it offered me a unique and rewarding opportunity for the next phase of my career.

Most of my team's work is spent on our annual agency inspection program. In a typical inspection, my team will begin by arranging a pre-inspection brief with the relevant team within the agency, which provides important background and context for the upcoming inspection. If the inspection topic is particularly sensitive, security briefings will be provided for inspection staff. In order to conduct our work, IOOs are provided agency access for oversight work. On a typical day of inspection work, I will carefully review agency records, documenting my observations. The types of records and information we review include policies, procedures, IT systems, and operational files.

During an inspection, IOOs review records looking at:

- whether agency activities are conducted in accordance with the law
- whether agency activities are conducted with respect for human rights
- whether agency activities are conducted with propriety
- the completeness of records
- whether agencies have complied with relevant record-keeping requirements
- whether agencies have followed their internal policies and procedures.

Inspection staff develop tools or guides for every inspection. These provide a framework for recording their observations, assessing legality and propriety, and eventually formulating inspection findings and recommendations.

The role is truly unique. It is an opportunity to work across multiple agencies with unparalleled exposure and access. I have reviewed records, files, programs and reports across a wide variety of agency activities. My experience has been much more varied than if I had spent the same amount of time working inside a single agency. I take great satisfaction in being able to draft findings and provide recommendations that help agencies improve their practices to better accord with legislation, policies and procedures, as well as providing assurance to the minister and the community that Australia's intelligence agencies are acting within the bounds of the law, with propriety and with respect for human rights.

Australian Criminal Intelligence Commission and Australian Federal Police

Key statistics



4

Inspections
commenced



4

Inspections
completed



0

Compliance
incidents reported



4

Ministerial letters
sent to relevant
minister



0

Senior-level
meetings held



0

Inquiries
commenced



0

Complaints
received



0

Complaints
closed

Agency overview

The IGIS has oversight responsibility for the network activity warrant (NAW) regime for ACIC and the AFP under the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*. The IGIS 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:

Responsible minister:

Relevant Act: *Surveillance Devices Act 2004*

Responsible minister: Minister for Home Affairs*

*The Attorney-General was the minister responsible for the ACIC and AFP until May 2025. The ACIC and AFP were subsequently moved to the Home Affairs portfolio.

Australian Criminal Intelligence Commission and Australian Federal Police

In 2024–25, the IGIS undertook inspections of ACIC's and the AFP's activities in relation to their use and management of NAWs. No issues of legality or propriety were found through these inspections.

ACIC inspections and compliance incidents

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

The ACIC did not report any compliance incidents to the IGIS in 2024–25.

AFP inspections and compliance incidents

Inspections

In the reporting period, the IGIS undertook 2 inspections regarding the AFP'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

The AFP did not report any compliance incidents to the IGIS in 2024–25.

Complaints

There were no complaints received in relation to either ACIC or the AFP in relation to NAWs in 2024–25. This was the same as the number of complaints received in 2023–24 (0 for ACIC and 0 for the AFP) in relation to NAWs.

During the reporting period, no preliminary inquiries or inquiries commenced. The Inspector-General did not prepare any reports to ACIC or the AFP under section 25B of the IGIS Act.

At the conclusion of the reporting period, no complaints about ACIC or the AFP in relation to NAWs remained open.

Cross-agency activities

Key statistics



2

Inspections
commenced



1

Inspections
completed



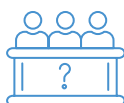
1

Own-motion
preliminary inquiries
commenced



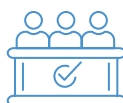
0

Own-motion
preliminary inquiries
completed



1

Inquiries
commenced



0

Inquiries
completed

Overview

In 2024–25, the IGIS commenced one inquiry and one own-motion preliminary inquiry reviewing the activities of multiple agencies. While other inspections relating to multiple agencies were also conducted, the statistics and details relating to these are reported against each agency independently. These related to the agencies' compliance with their obligations under the Respect@Work legislation and the management of compliance incidents related to a particular warrant type.

Cross-agency inspections and inquiry activities

Inquiries

During 2024–25, the IGIS conducted one cross-agency inquiry.

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

In October 2024, the Inspector-General informed the relevant ministers and heads of agencies of his intention to conduct an inquiry into activities undertaken under a warrant issued by the Attorney-General under section 11C of the TIA Act. This inquiry complements the inquiry on the same topic conducted by the IGIS in 2022–23, and concerns the implementation of specific elements of the mandatory procedure issued under subsection 11C(6) of the TIA Act. These elements could not be examined in the previous inquiry, due to relevant timeframes for certain requirements not having elapsed.

This inquiry remains underway and will be reported on in 2025–26.

Own-motion preliminary inquiry

During 2024–25, the IGIS commenced one own-motion preliminary inquiry, which is being conducted across all 6 intelligence agencies. The own-motion preliminary inquiry is focused on the agencies' use and management of exceptionally controlled information (ECI) to compartmentalise particularly sensitive matters. The own-motion preliminary inquiry is considering the accountability, transparency and ability to effectively oversee material and activities which have been placed under an ECI. The IGIS has received responses to this own-motion preliminary inquiry from all agencies, and as at the end of 2024–25 was finalising the preliminary report for consultation.

The outcome of this own-motion preliminary inquiry will be reported on in the 2025–26 annual report.

Inspections

During 2024–25, the IGIS undertook 2 cross-agency inspection activities, looking into agency activities relating to:

- practices and procedures for managing compliance incidents relating to a particular intelligence collection warrant issued by the Attorney-General. This activity remains underway and will be completed in 2025–26
- each agency's compliance with the positive duty obligations introduced by the Respect@Work legislation to eliminate unlawful conduct as described by the *Sex Discrimination Act 1984*. Inspections related to ONI, ASIO, ASIS and ASD were completed. The inspections of DIO and AGO remain underway and will be completed in 2025–26.

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. These inspections were concluded in 2024–25 and relevant findings and recommendations are reported in the individual agency sections.

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.

As agencies' reporting for 2024–25 will cover the creation and use of assumed identities up to 30 June 2025, this reporting is not available to the IGIS in the current reporting period and will be reported on in 2025–26.

Annual reporting by ONI identified that the audits conducted to cover the 2023–24 period were not completed within the statutory timeframes established by section 15LG of the Act. The required audits were completed by September 2024. ONI has implemented measures to prevent this from occurring again.

Annual reporting by ASIO made observations relevant to an assumed identities inspection conducted by IGIS in 2022–23 and reported on in last year's annual report.

Annual reporting by ASD, ASIO and ASIS did not identify any compliance concerns.

IGIS inspection programs that directly address the agencies' use and management of assumed identities have been identified in the individual agency sections of this report.

Complaints and public interest disclosures

Key statistics



64

Complaints received*



41

Complaints closed



5

PID Act disclosures about intelligence agencies which were allocated by the Inspector-General



1

PID Act disclosures allocated to the Inspector-General by an intelligence agency



358

Other correspondence handled^

*Includes 9 matters that are under assessment as at the end of the reporting period to determine whether they meet 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

General overview

This part of Section 6 provides a summary of the activities of the Inspector-General in relation to complaints received and disclosures investigated in total across all agencies within the Inspector-General's jurisdiction. Information about complaints and inquiries by agency can be found under agency-specific headings earlier in the section.

In addition to the complaints against each agency outlined earlier in the section, the Inspector-General receives complaints regarding the processing of visa and citizenship 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 also has key responsibilities under the PID Act. The Inspector-General has a broad jurisdiction to receive 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 NAWs.

The Inspector-General also receives a large number of complaints and other correspondence that do not fall within the jurisdiction of either the IGIS Act or the PID 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 the 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

	2024–25 FY (1 July 2024 – 30 June 2025)	2023–24 FY (1 July 2023 – 30 June 2024)	2022–23 FY (1 July 2022 – 30 June 2023)
Complaints within the jurisdiction of the IGIS Act	64	64	34
Visa and citizenship complaints	30	40	70
PID Act disclosures about intelligence agencies which were allocated by the Inspector-General*	5	1	6
Other correspondence not within the jurisdiction of the IGIS Act or PID Act**	358	655	599

*Does not include one matter which was allocated to the Inspector-General by an intelligence agency

**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 2024–25 was 64. This was consistent with the number of complaints in 2023–24 (64) and more than the number of complaints received in 2022–23 (34).

Table 6.2: Complaints received by agency

Agency	Number of complaints
ACIC (NAWs)	0
AFP (NAWs)	0
AGO	1
ASD	10
ASIO	42
ASIS	10
DIO	0
ONI	1

In response to the overall number of complaints received in this reporting period, the Inspector-General:

- commenced 34 preliminary inquiries
- commenced one inquiry in relation to 8 related complaints
- did not undertake any preliminary inquiries or inquiries in relation to 22 complaints during the reporting period (8 of which were closed without further action being required, with the remaining 14 remaining under active consideration at the end of the reporting period).

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

- employment grievances
- agency misconduct and surveillance
- processes for conducting security assessments for government functions
- public comment and publications
- data breaches or information sharing
- recruitment and organisational suitability assessments.

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. Staff are committed to resolving complaints in a timely manner having regard to the nature and complexity of each matter.

In addition, in this reporting period the Inspector-General:

- prepared 5 reports under section 25B of the IGIS Act at the conclusion of the relevant preliminary inquiry, making a total of 20 recommendations
- commenced 3 preliminary inquiries in response to complaints received during the previous reporting period
- did not commence any inquiries in response to complaints received during the previous reporting period.

In the reporting period, the Inspector-General closed 41 complaint matters. Of these, 27 were received in this reporting period and 14 were received in a previous reporting period. The matters were closed on the following grounds:

- section 11(2)(b) of the IGIS Act – one matter
- section 11(2)(c) of the IGIS Act – 38 matters
- section 11(3) of the IGIS Act – one matter
- multiple sections (11(2)(a), 11(2)(c), and 11(3)) – one matter.

The number of complaints closed in this reporting period (41) is lower than in the previous reporting period (64), while the number of complaints is consistent (64). This decrease in the number of cases closed reflects the increased complexity of complaints received. Complaints are often requiring significantly more resources and expertise to investigate than has previously been the case.

At the conclusion of the reporting period, 43 complaints remained open. This comprised 37 complaints received in this reporting period and 6 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 IGIS also receives complaints concerning the processing of visa and citizenship applications, particularly regarding the length of time taken to finalise applications. However, the IGIS's jurisdiction only extends to cases where the delays are a result of processes or practices within the intelligence agencies over which the IGIS has jurisdiction. As identified in Table 6.1, the number of complaints regarding visa and citizenship applications decreased in 2023–24. The IGIS did not identify any systemic compliance issues in the visa and citizenship complaints investigated in 2024–25.

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.

Disclosures handled by the Inspector-General

During the reporting period, the Inspector-General assessed 20 matters that resulted in a decision not to allocate the disclosure. This is broadly consistent with the number of matters (16) assessed in 2023–24 which resulted in a decision not to allocate. In relation to these matters a decision not to allocate was made in:

- 9 matters because the conduct was not disclosable conduct (personal work-related grievances)
- 4 matters because the conduct was not disclosable conduct (conduct other than personal work-related grievances)
- 7 matters because the conduct was considered more appropriately investigated as a complaint under the IGIS Act.

During the reporting period, the Inspector-General allocated the following disclosures relating to intelligence agencies:

- one disclosure to the IGIS. This matter was received in the previous reporting period and related to 3 instances of suspected disclosable conduct. The investigation of this matter was ongoing as at 30 June 2025
- 4 disclosures to intelligence agencies. These disclosures related to a total of 10 instances of alleged disclosable conduct.

The total number of instances of disclosable conduct (13) allocated by the Inspector-General during the reporting period related to different kinds of suspected disclosable conduct (see Table 6.3).

Table 6.3: Kinds of suspected disclosable conduct

Suspected disclosable conduct	Number of instances
Maladministration	4
Contravention of a law of the Commonwealth or of a state or territory	3
Danger to health or safety	2
Conduct that involves or is engaged in for the purpose of a public official abusing their position as a public official	2
Conduct that could lead to disciplinary action against a public official	2

One disclosure was allocated to the Inspector-General by an intelligence agency after the Inspector-General consented to its allocation. This disclosure concerned one instance of suspected disclosable conduct with allegations related to conduct that involves corruption. The investigation of this matter was ongoing as at 30 June 2025.

Overall, as at 30 June 2025, the IGIS was investigating 2 disclosures which had been allocated to the Inspector-General during this reporting period. No disclosures allocated to the IGIS from the previous reporting periods were still under investigation.

During the reporting period, 2 investigations of alleged disclosable conduct were completed, both of which related to the same intelligence agency. These matters were allocated to the IGIS for investigation by the Inspector-General in the 2022–23 reporting period. Of these investigations:

- one investigation was completed with a finding of 4 instances of maladministration. This investigation resulted in 2 recommendations regarding administrative practices, which were accepted and actioned by the agency
- one investigation was completed with a finding of 3 instances of maladministration, with no recommendations made.

Both investigations were completed in more than 180 days.

As at 30 June 2025, 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.

Overseeing the operation of the PID scheme in the intelligence agencies

In accordance with section 44(1A)(b) of the PID Act, intelligence agencies (which includes the 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 for investigation and when an investigation is completed.

The Inspector-General was notified of 3 disclosures received by the intelligence agencies during the reporting period. Of these 3 disclosures:

- a decision not to allocate was made in relation to one disclosure
- a decision to allocate to their own agency was made in relation to one disclosure. This matter related to one instance of disclosable conduct. The alleged conduct was conduct that resulted in a wastage of relevant money or property, or money or property of a prescribed authority
- a decision to allocate to the Inspector-General was made in relation to one disclosure as noted earlier.

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

During the reporting period 6 investigations of alleged disclosable conduct were completed by the intelligence agencies:

- 2 were received and allocated in 2024–25
- 2 were received in 2023–24 and allocated in 2024–25
- 2 were received and allocated 2023–24.

In relation to the findings of the 6 investigations, only one investigation found instances of disclosable conduct. This investigation found 3 instances of disclosable conduct, which included maladministration; conduct that results in wastage of relevant money or property, or money or property of a prescribed authority; and conduct that involves or is engaged in for the purpose of a public official abusing their position as a public official. The findings included 6 recommendations, all of which were actioned. This included a recommendation for state or federal police to be notified of information in accordance with section 56 of the PID Act.

No instances of disclosable conduct were found in relation to the other 5 investigations. Of these 5 investigations:

- one investigation related to 3 instances of disclosable conduct: conduct that involves or is engaged in for the purpose of a public official abusing their position as a public official; conduct that could lead to disciplinary action against a public official; and conduct that contravenes a law of the Commonwealth, a state or a territory. There were no findings of disclosable conduct or recommendations made
- one investigation related to 2 instances of disclosable conduct: maladministration; and unreasonable endangerment to health and safety. The investigation also considered additional allegations that did not reach the threshold of disclosable conduct but were deemed serious enough to be included in the scope of the investigation. While no findings of disclosable conduct were made, 7 recommendations were made. As at 30 June 2025, 3 recommendations had been actioned and finalised and 4 recommendations had actions which were ongoing

- one investigation related to 3 instances of disclosable conduct: maladministration; unreasonable endangerment to health and safety; and conduct that contravenes a law of the Commonwealth, a state or a territory. While no findings of disclosable conduct were made, further consideration of relevant internal processes was recommended and relevant action was undertaken by the agency
- one investigation related to one instance of disclosable conduct regarding allegations of maladministration. While no findings of disclosable conduct were made, the agency undertook a review of the relevant framework and associated business processes
- one investigation related to one instance of disclosable conduct regarding allegations of conduct that results in wastage of relevant money or property, or money or property of a prescribed authority. No findings of disclosable conduct or recommendations were made.

In relation to the duration of the 6 investigations:

- one was completed within 90 days
- 4 were completed in 91 to 180 days
- one exceeded 180 days.

For all 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.

Regarding the PIDs which were investigated during the reporting period, the agencies identified no claims or evidence of detrimental action taken against the discloser in their section 51 reports (final reports).

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 IGIS provided assistance and guidance to officials within the intelligence agencies about the operation of the scheme. This included the IGIS hosting a PID community of practice forum for officials within the intelligence agencies to facilitate sharing of expertise. In the context of a broad range of education and engagement activities, the Inspector-General's staff also discussed IGIS's role in the PID scheme and alerted agencies to PID-related training courses and relevant fora that may be of interest to their officials.

The Inspector-General's staff engaged with staff from the Office of the Commonwealth Ombudsman about the PID scheme and assisted the Ombudsman in relation to its functions under the PID Act throughout the reporting period. Staff assisting the Inspector-General coordinated intelligence agencies' input to the Ombudsman for their 6-monthly and annual reports about the operation of the PID Act.

When collecting information in support of the Ombudsman's annual report, the IGIS obtained information from intelligence agencies regarding their support for potential and actual disclosers and their assessment and management of possible reprisal actions. The IGIS anticipates that this will inform oversight activities during the next reporting period.

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:

- 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 2024–25 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 measure its electricity and natural gas usage separately 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 2024–25

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	–	–
Refrigerants	–	n/a	n/a	–
Fleet and other vehicles	0.22	n/a	0.06	0.28
Domestic commercial flights	n/a	n/a	11.10	11.10
Domestic hire car	n/a	n/a	0.10	0.10
Domestic travel accommodation	n/a	n/a	2.82	2.82
Other energy	–	n/a	–	–
Total kg CO₂-e	0.22	–	14.07	14.30

Note: the table above presents emissions related to electricity usage using the location-based accounting method.
CO₂-e = carbon dioxide equivalent.

n/a = not applicable

Table 7.2: Electricity greenhouse gas emissions 2024–25

Emission source	Scope 12 t CO ₂ -e	Scope 3 t CO ₂ -e	Total t CO ₂ -e	Electricity kWh
Electricity (location-based approach)	–	–	–	–
Market-based electricity emissions	–	–	–	–
Total renewable electricity consumed	n/a	n/a	n/a	–
Renewable power percentage ¹	n/a	n/a	n/a	–
Jurisdictional renewable power percentage ^{2, 3}	n/a	n/a	n/a	–
GreenPower ²	n/a	n/a	n/a	–
Large-scale generation certificates ²	n/a	n/a	n/a	–
Behind the meter solar ⁴	n/a	n/a	n/a	–
Total renewable electricity produced	n/a	n/a	n/a	–
Large-scale generation certificates ²	n/a	n/a	n/a	–
Behind the meter solar ⁴	n/a	n/a	n/a	–

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. Electricity usage is measured in kilowatt hours (kWh).

- 1 Listed as mandatory renewables in 2023–24 annual reports. The renewable power percentage accounts for the portion of electricity used, from the grid, that falls within the Renewable Energy Target.
- 2 Listed as voluntary renewables in 2023–24 annual reports.
- 3 The Australian Capital Territory is currently the only state with a jurisdictional renewable power percentage.
- 4 Reporting behind the meter solar consumption and/or production is optional. The quality of data is expected to improve over time as emissions reporting matures.

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	158–165
17AJ(c)	Annexures	Glossary of abbreviations and acronyms.	Mandatory	156–157
17AJ(d)	Annexures	List of requirements.	Mandatory	145–155
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	2–4
17AD(b)	Overview of the entity			
17AE(1)(a)(i)	Section 2	A description of the role and functions of the entity.	Mandatory	8

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AE(1)(a)(ii)	Section 2	A description of the organisational structure of the entity.	Mandatory	13
17AE(1)(a)(iii)	Section 3	A description of the outcomes and programmes administered by the entity.	Mandatory	19, 83
17AE(1)(a)(iv)	Section 2	A description of the purposes of the entity as included in corporate plan.	Mandatory	9
17AE(1)(aa)(i)	Section 3	Name of the accountable authority or each member of the accountable authority.	Mandatory	18
17AE(1)(aa)(ii)	Section 3	Position title of the accountable authority or each member of the accountable authority.	Mandatory	18
17AE(1)(aa)(iii)	Section 4	Period as the accountable authority or member of the accountable authority within the reporting period.	Mandatory	40
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			
	<i>Annual Performance Statements</i>			
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	18–30

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AD(c)(ii)	Report on Financial Performance			
17AF(1)(a)	Section 5	A discussion and analysis of the entity's financial performance.	Mandatory	56–81
17AF(1)(b)	Annexures	A table summarising the total resources and total payments of the entity.	Mandatory	82–83
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	49
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

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(2)(b) (iii)	Preliminaries	A certification by accountable authority that all reasonable measures have been taken to deal appropriately with fraud 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	42-44
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	43
17AG(2A)(b)	Section 4	The name of each member of the entity's audit committee.	Mandatory	43-44
17AG(2A)(c)	Section 4	The qualifications, knowledge, skills or experience of each member of the entity's audit committee.	Mandatory	43-44
17AG(2A)(d)	Section 4	Information about the attendance of each member of the entity's audit committee at committee meetings.	Mandatory	43-44
17AG(2A)(e)	Section 4	The remuneration of each member of the entity's audit committee.	Mandatory	43-44
External Scrutiny				
17AG(3)	Section 4	Information on the most significant developments in external scrutiny and the entity's response to the scrutiny.	Mandatory	50-54

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(3)(a)	n/a	Information on judicial decisions and decisions of administrative tribunals and by the Australian Information Commissioner that may have a significant effect on the operations of the entity.	If applicable, mandatory	n/a
17AG(3)(b)	Section 4	Information on any reports on operations of the entity by the Auditor- General (other than report under section 43 of the Act), a Parliamentary Committee, or the Commonwealth Ombudsman.	If applicable, mandatory	50
17AG(3)(c)	n/a	Information on any capability reviews on the entity that were released during the period.	If applicable, mandatory	n/a
Management of Human Resources				
17AG(4)(a)	Section 4	An assessment of the entity's effectiveness in managing and developing employees to achieve entity objectives.	Mandatory	32-34
17AG(4)(aa)	Section 4	Statistics on the entity's employees on an ongoing and non-ongoing basis, including the following: (a) statistics on full-time employees; (b) statistics on part-time employees; (c) statistics on gender (d) statistics on staff location	Mandatory	5, 35, 38

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(4)(b)	Section 4	Statistics on the entity's APS employees on an ongoing and non-ongoing basis; including the following: • 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	5, 35, 38
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	39
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	39
17AG(4)(c)(ii)	Section 4	The salary ranges available for APS employees by classification level.	Mandatory	38
17AG(4)(c)(iii)	Section 4	A description of non-salary benefits provided to employees.	Mandatory	39
17AG(4)(d)(i)	n/a	Information on the number of employees at each classification level who received performance pay.	If applicable, mandatory	n/a
17AG(4)(d)(ii)	n/a	Information on aggregate amounts of performance pay at each classification level.	If applicable, mandatory	n/a
17AG(4)(d)(iii)	n/a	Information on the average amount of performance payment, and range of such payments, at each classification level.	If applicable, mandatory	n/a

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(4)(d) (iv)	n/a	Information on aggregate amount of performance payments.	If applicable, mandatory	n/a
Assets Management				
17AG(5)	Section 4	An assessment of effectiveness of assets management where asset management is a significant part of the entity's activities.	If applicable, mandatory	50
Purchasing				
17AG(6)	Section 4	An assessment of entity performance against the <i>Commonwealth Procurement Rules</i> .	Mandatory	51
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	51
17AG(7)(d)	Section 4	A statement that <i>"Annual reports contain information about actual expenditure on reportable consultancy contracts. Information on the value of reportable consultancy contracts is available on the AusTender website."</i>	Mandatory	51
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	53

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(7A)(b)	Section 4	A statement that “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.”	Mandatory	52
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	52–53
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	54

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	54
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	51
17AG(10)(b)	Section 4	An outline of the ways in which the procurement practices of the entity support small and medium enterprises.	Mandatory	51
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

PGPA Rule Reference	Part of Report	Description	Requirement	Page
<i>Financial Statements</i>				
17AD(e)	Section 5	Inclusion of the annual financial statements in accordance with subsection 43(4) of the Act.	Mandatory	58–81
<i>Executive Remuneration</i>				
17AD(da)	Section 4	Information about executive remuneration in accordance with Subdivision C of Division 3A of Part 23 of the Rule.	Mandatory	40
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	142
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	41

PGPA Rule Reference	Part of Report	Description	Requirement	Page
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	50
17AH(1)(e)	n/a	Correction of material errors in previous annual report	If applicable, mandatory	n/a
17AH(2)		Information required by other legislation	Mandatory	41, 86-139, 142-144

Glossary

ACIC	Australian Criminal Intelligence Commission
ACT	Australian Capital Territory
ADF	Australian Defence Force
AFP	Australian Federal Police
AGD	Attorney-General's Department
AGO	Australian Geospatial-Intelligence Organisation
AHRC	Australian Human Rights Commission
ANAO	Australian National Audit Office
APS	Australian Public Service
Archives Act	<i>Archives Act 1983</i>
ARC	Audit and Risk Committee
ART	Administrative Review Tribunal
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
Crimes Act	<i>Crimes Act 1914</i>
Criminal Code	<i>Criminal Code Act 1995</i>
D&I	Diversity and inclusion
DIO	Defence Intelligence Organisation
ECI	Exceptionally controlled information
EL	Executive Level
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>
HR	Human resources
HRA	Human rights assessment
ICT	Information and communications technology
IGIS	The statutory agency of the Inspector-General of Intelligence and Security

IGIS Act	<i>Inspector-General of Intelligence and Security Act 1986</i>
IOO	Intelligence Oversight Officer
IPS	Information Publication Scheme
IS Act	<i>Intelligence Services Act 2001</i>
NACC	National Anti-Corruption Commission
NAW	Network activity warrant
NIC	National intelligence community
NSIRA	National Security and Intelligence Review Agency
OLSC	Office of Legal Services Coordination
ONI	Office of National Intelligence
ONI Act	<i>Office of National Intelligence Act 2018</i>
OPN	Overturning a presumption of nationality
PBS	Portfolio Budget Statements
PGPA Act	<i>Public Governance, Performance and Accountability Act 2013</i>
PGPA Rule	Public Governance, Performance and Accountability Rule 2014
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>
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>

Index

A

- abbreviations, 156–157
- Aboriginal and Torres Strait Islander people, 33
- accountable authority, 18, 42
 - statements by, 18, 59
- Accountable Authority Instructions, 51
- ACIC see Australian Criminal Intelligence Commission (ACIC)
- acknowledgement of Country, ii
- address and contact information, ii
- Administrative Appeals Tribunal (AAT), 15
- advertising and market research, 142
- AFP see Australian Federal Police (AFP)
- Agency Oversight section, 13
- AGO see Australian Geospatial-Intelligence Organisation (AGO)
- ANAO see Australian National Audit Office (ANAO)
- annual performance statement
 - accountable authority statement, 18
 - reporting framework, 19
 - results:
 - Objective 1: Inquiries, 20–21
 - Objective 2, Inspections, 22–23
 - Objective 3, Complaints, 24–25
 - Objective 4, Public interest disclosures, 26–28
 - Objective 5, Assurance, 29–30
- anti-corruption initiatives see fraud control;
National Anti-Corruption Commission
- Anti-Discrimination and Human Rights Legislation
Amendment (Respect at Work) Act 2022*
(Respect@Work), 91, 117, 125, 129, 130
- APS see Australian Public Service (APS)
- Archives Act 1983*, 15
- ASD see Australian Signals Directorate (ASD)
- ASIO see Australian Security Intelligence
Organisation (ASIO)
- ASIS see Australian Secret Intelligence Service
(ASIS)
- asset management, 50
- Assistant Inspectors-General, 13, 40
- assumed identities, 97, 125, 131
- assurance
 - assuring ministers and parliament, 11, 14–15,
19, 29–30
 - expert evidence to AAT or OAIC, 15
 - informing the public, 11, 14, 19, 29–30
 - performance results and analysis, 29–30
 - see also ministers; parliamentary committees
- Attorney-General, 14, 30, 88, 91
- Attorney-General's Department
 - IGIS engagement with, 4, 44
 - IGIS office co-location with, 45, 142, 143
 - portfolio department, 3
- Audit and Risk Committee, 41, 42, 43–44
- Auditor-General, 21, 54, see also Australian
National Audit Office (ANAO)
- audits
 - financial statements audit report, 50, 56–57
 - internal, 44
- AusTender, 51, 52, 54
- Australia Day awards, 34
- Australian Criminal Intelligence Commission
(ACIC), 2, 8, 11, 127–128
- Australian Cyber Security Centre, 108
- Australian Federal Police (AFP), 2, 8, 11, 127–128
- Australian Geospatial-Intelligence Organisation
(AGO), 116–119
 - agency overview, 116
 - complaints about, 119
 - compliance incidents, 118
 - IGIS engagement with, 3–4, 117
 - IGIS role in respect of, 8, 116–117
 - inspections, 117–118
 - key statistics, 116
 - legislation and responsible minister, 116
 - privacy rules compliance, 118
 - record keeping, 118
- Australian Human Rights Commission, 46
 - Good Practice Framework, 91
- Australian Human Rights Commission Act 1986*, 46
- Australian Information Commissioner, 15, 46
- Australian National Audit Office (ANAO)
 - access clauses in contracts, 54
 - financial statements audit report, 50, 56–57
- Australian National University, National Security
College, 34, 45
- Australian persons
 - obtaining intelligence on, 113
 - privacy protections see Privacy Rules
 - risk to safety of, outside Australia, 113–114, 118
- Australian Public Service (APS)
 - Census Action Plan, 4, 34
 - Graduate Development Program, 34

- Net Zero 2030 emissions reporting, 143–144
 - values and code of conduct, 32, 49
 - see also Public Service Act 1999*
 - Australian Public Service Commission, 34
 - Australian Public Service Commissioner, 4
 - Australian Secret Intelligence Service (ASIS), 101–107
 - agency overview, 101
 - assumed identities, 131
 - complaints about, 107
 - compliance incidents, 105–107
 - IGIS engagement with, 3, 102
 - IGIS role in respect of, 8, 101–102
 - inquiries, 102
 - inspections, 102–104
 - key statistics, 101
 - legislation and responsible minister, 101
 - ministerial directions, 101, 103
 - preliminary inquiry reports, 14, 107
 - Privacy Rules compliance, 105
 - record keeping, 103, 104, 107
 - weapons management, 104
 - Australian Security Intelligence Organisation (ASIO), 88–100
 - agency overview, 88
 - assumed identities, 97, 131
 - complaints about, 99
 - compliance incidents, 89, 92–98
 - compulsory questioning powers, 91
 - device access orders, 90–91
 - IGIS engagement with, 3, 89
 - IGIS role in respect of, 8, 89
 - inquiries, 89, 99
 - inspections, 90–91, 96
 - key statistics, 88
 - legislation and responsible minister, 88
 - Minister's Guidelines, 88, 96
 - non-compliance with Minister's Guidelines, 94–95
 - preliminary inquiries, 14, 99, 100
 - record keeping, 90
 - special intelligence operations, 88, 91
 - use of force, 92
 - warrants, 88, 90–91, 92–93
 - Australian Security Intelligence Organisation Act 1979* (ASIO Act), 88, 89, 90–94
 - Australian Signals Directorate (ASD), 108–115
 - agency overview, 108
 - assumed identities, 131
 - complaints about, 114
 - compliance incidents, 109, 111–113
 - human rights assessments, 110–111
 - ICT support for IGIS, 45
 - IGIS engagement with, 3, 109
 - IGIS role in respect of, 8, 109
 - inquiries, 109
 - inspections, 109–111
 - key statistics, 108
 - legislation and responsible minister, 108
 - ministerial authorisations, 113
 - overturned presumptions of nationality, 111, 113
 - preliminary inquiries, 14, 114, 115
 - privacy rules compliance, 111
 - public interest disclosure administration, 115
 - record keeping, 110
 - REDSPICE, 108
 - Australian Transaction Reports and Analysis Centre (AUSTRAC), 2
 - Australia's Disability Strategy 2021–2031, 41
- ## B
- bilateral engagement, 47
 - Bogaart, Karla, 43
 - Brookes, Chris, 40
 - business continuity plan, 44, 48
- ## C
- Cabinet
 - National Security Committee, 123
 - Canada
 - National Security and Intelligence Review Agency, 47
 - see also Five-Eyes Intelligence Oversight and Review Council*
 - capability reviews
 - Oversight Capability Review, 4, 20, 21, 22, 23
 - case studies
 - Day in the life of an IGIS Oversight Officer, 126
 - Employee Value Proposition, 37
 - Minister's Guidelines to ASIO, 96
 - Preliminary inquiries with reports made under section 25B of the IGIS Act, 100
 - citizenship application-related complaints, 5, 25, 135
 - code of conduct, 32
 - committees, 42

Commonwealth Contracting Suite, 51, 54
Commonwealth Electoral Act 1918, 142
 Commonwealth Fraud and Corruption Control Framework 2024, iii, 49
 Commonwealth Indigenous Procurement Policy, 51
 Commonwealth Ombudsman, 21, 46, 50, 139
 Commonwealth Procurement Rules, 51
 communications interception see *Telecommunications (Interception and Access) Act 1979* (TIA Act)
 complaints, 2, 86–87, 107, 132–135
 about ACIC and AFP, 128
 about AGO, 119
 about ASD, 114
 about ASIO, 99
 about ASIS, 107
 about DIO, 122
 about ONI, 125
 complaints-handling process improvements, 25
 IGIS function and powers, 11
 inquiries, 134–135
 non-visa related, 134–135
 performance results and analysis, 24–25
 statistics, 5, 132, 133
 visa or citizenship related, 5, 25, 133, 135
 compliance discipline, 2, 10, 87
 compliance incidents, 5, 23, 86
 ACIC and AFP, 128
 AGO, 118
 ASD, 111–113
 ASIO, 92–98
 ASIS, 105–107
 ONI, 125
 warranted collection activity, 130
 consultants, 51–52
 contact information, ii
 contracts, 51–54
 corporate governance, 4, 42–44
 Corporate Plan 2024–25, 18, 19
 corporate support, 45
 Corradin, Andrew, 13, 40
 correspondence handled, 132, 133, *see also* complaints
 corruption, 49, 137, *see also* ethical standards;
 fraud control; National Anti-Corruption Commission
Crimes Act 1914 non-compliance, 97

Criminal Code Act 1995 non-compliance, 98
 Cronan, Paul, 13, 40
 cross-agency inspection and inquiry activities, 10, 86, 91, 117, 129–131
 cyber security, 108

D

defence intelligence agencies *see* Australian Geospatial-Intelligence Organisation (AGO); Australian Signals Directorate (ASD); Defence Intelligence Organisation (DIO)
 Defence Intelligence Organisation (DIO), 120–122
 agency overview, 120–121
 complaints against, 122
 IGIS engagement with, 3, 120
 IGIS role in respect of, 8, 120–121
 inspections, 121–122
 key statistics, 120
 legislation and responsible minister, 120
 privacy rules compliance, 121
 record keeping, 121
 specified program, 122
 Department of Defence full knowledge and concurrence policy, 118, *see also* Minister for Defence
 Department of Foreign Affairs *see* Minister for Foreign Affairs
 Department of Home Affairs, 2, *see also* Minister for Home Affairs
 Deputy Inspector-General, 13, 40
 device access orders, 90–91
 DIO *see* Defence Intelligence Organisation (DIO)
 disability reporting, 41
 disclosures in the public interest *see* public interest disclosures
 Diversity and Inclusion Committee, 33, 42
 diversity and inclusion initiatives, 33

E

ecologically sustainable development and environmental performance, 142
 emissions reporting, 143–144
 Employee Value Proposition, 37, *see also* staff
 enabling legislation, 2, 8, *see also* *Inspector-General of Intelligence and Security Act 1986*
 energy-saving initiatives, 142
 enterprise agreement, 39
 Enterprise Management Unit, 13, 39
 entity resource statement, 82–83

Environment Protection and Biodiversity

Conservation Act 1999, 142

ethical standards, 49, *see also* fraud control;
values

Executive Board, 23, 41, 42

Executive Director, Enterprise Management Unit,
13, 39, 40

executives *see* senior executives

exempt contracts, 54

expenses for outcome, 82–83

expert evidence to AAT or OAIC, 15

external scrutiny of IGIS, 50–54

F

financial services, 45

financial statements, 56–81

audit report, 50, 56–57

entity resource statement, 82–83

statement by the accountable authority, 59

firearms *see* weapons management

Five-Eyes Intelligence Oversight and Review
Council, 4, 30, 46–47

flexible work, 32

force

use-of-force notifications, 92

foreign authorities

AGO cooperation with, 117–118

see also international engagement

foreign intelligence collection, 88, 96, 101, 106, *see*
also Australian Secret Intelligence Service
(ASIS); Australian Security Intelligence
Organisation (ASIO)

fraud control, iii, 48, 49

Freedom of Information Act 1982, 15

exemptions, 15, 50, 54

G

geospatial intelligence agency *see* Australian
Geospatial-Intelligence Organisation (AGO)

governance *see* corporate governance

greenhouse gas emissions reporting, 143–144

H

health *see* workplace health and safety

Home Affairs portfolio, 2, 88, 127

human resources management *see* staff

human rights assessments, 110–111

Indigenous businesses, commitment to, 51

individual flexibility arrangements, 39

information and communications technology
(ICT), 45

Information Publication Scheme, 50

information security authority *see* Australian
Signals Directorate (ASD)

inquiries, 2, 5, 10, 86–87

ASD, 109

ASIO, 89, 99

ASIS, 102

complaints inquiries, 2, 134–135

cross-agency, 129–130

no requests from Prime Minister or ministers,
14

own-motion, 89, 91, 109, 115, 129, 130

performance results and analysis, 20–21

preliminary inquiries, 10, 14

preliminary inquiries, reports made under
section 25B of the IGIS Act, 14, 100, 107,
115

inquiries by parliamentary committees *see*
parliamentary committees

inspections, 2, 5, 10, 86–87

ACIC and AFP, 128

AGO, 117–118

ASD, 109–111

ASIO, 90–91, 96

ASIS, 102–104

cross-agency, 10, 86, 91, 117, 130

day in the life of an IGIS Oversight Officer, 126

DIO, 121–122

ONI, 124–125

performance results and analysis, 22–23

risk-based annual inspection plans, 23

risk-based proactive inspections, 10, 86

section 25A inspection reports, 14

Inspector-General of Intelligence and Security
approach, 12

engagement with agencies, 3–4, 11, 29, 30, 45,
50, 87, 89, 102, 109, 117, 120, 123

key activities, 10–11

letter of transmittal, iii

organisation chart, 13

Oversight Capability Review, 4, 20, 21, 22, 23

purpose, 9, 19

remuneration, 39, 40

- review of year, 2–4
- role and functions, 2, 8
- statutory office holder, 35, 39
- Technical Advisor, 34
- Inspector-General of Intelligence and Security Act 1986*, iii, 2, 3, 8, 14, 19, 27–28, 86
 - complaints handling see complaints
 - inquiries see inquiries
 - inspections see inspections
- Inspectors-General Forum, 45
- Integrity Agencies Group, 3, 45
- intelligence agencies
 - human rights obligations, 110–111
 - IGIS engagement with, 3–4, 30, 45, 87, 89, 102, 109, 117, 120, 123
 - IGIS oversight of (list of agencies), 8, see also Inspector-General of Intelligence and Security
 - IGIS oversight of (overview), 86–87
 - public interest disclosure obligations, 139
 - record keeping see record keeping
 - 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 Oversight Officer, day in the life of, 126
- Intelligence Services Act 2001*, 101, 102–106, 109, 113–114, 117–118
 - non-compliance, 104, 105–106, 110–111, 113, 118
 - privacy rules see Privacy Rules
- Intelligence Services Legislation Amendment Bill 2023, 2
- internal audit, 44
- international engagement, 4, 30, 46–47
- investigations under PID Act, 2, 28, 86–87, 136–139

J

Jessup, Christopher, 13, 18, 40, see also Inspector-General of Intelligence and Security

K

- key activities, 10–11
- key management personnel, 39, 40

L

- labour market see recruitment
- leadership development, 34
- Leadership Group, 41
- learning and development, 34
- Legal & Assurance section, 13
- Legal Services Directions 2017*, 105–106
- legislation affecting the work of the IGIS, 2–3, 8, see also *Inspector-General of Intelligence and Security Act 1986*
- legislation governing intelligence agencies, 88, 101, 108, 116, 120, 123
- length-of-service recognition, 34
- letter of transmittal, iii

M

- maladministration, 137, 138–139
- market research, 142
- memoranda of understanding
 - IGIS, 45, 46
 - ONI, 125
- Menzies, Clare, 40
- Minister for Defence, 108, 111, 116, 120
- Minister for Foreign Affairs, 101, 103, 106
- Minister for Home Affairs, 88, 127
- ministerial authorisations, 101, 106, 108, 109, 110, 113, 116, 117
- ministerial directions, 101, 103, 108, 109, 113, 116
- ministerial letters, 5, 25, 88, 101, 108, 116, 120, 123, 127
- ministers
 - reporting to, 4, 8, 11, 14, 21, 22, 23, 29–30, 87
 - responsible for intelligence agencies, 88, 101, 108, 116, 120, 123
- Minister's Guidelines to ASIO, 88, 96
- Moore, Stephen, 43

N

- National Anti-Corruption Commission, 45
- National Intelligence Academy, 34
- national intelligence community see intelligence agencies
- National Security and Intelligence Review Agency (Canada), 47
- National Security College, Australian National University, 34, 45

National Security Committee of Cabinet, 123

nationality

- overturned presumptions of nationality, 111, 113

Net Zero 2030 emissions reporting, 143–144

network activity warrants (NAWS), 8, 127–128, 133, 134

non-compliance with law, standards or procedures *see* compliance incidents

non-consultancy contracts, 53

non-salary benefits, 39, *see also* remuneration

notifiable incidents, 41

O

office culture, 32–33

Office of National Intelligence (ONI), 123–125

- agency overview, 123–124
- assumed identities, 125, 131
- complaints, 125
- compliance incidents, 125
- IGIS engagement with, 3, 123
- IGIS role in respect of, 8, 123–124
- inspections, 124–125
- key statistics, 123
- legislation and responsible minister, 123
- open-source intelligence functions, 124
- privacy rules compliance, 124
- record keeping, 124

Office of National Intelligence Act 2018, 123, 124

Office of the Australian Information Commissioner, 15, 46

Office of the Commonwealth Ombudsman, 21, 46, 50, 139

Office of the Inspector-General of Intelligence and Security *see* Inspector-General of Intelligence and Security

ONI *see* Office of National Intelligence (ONI)

open-source intelligence functions, 124

organisation chart, 13

organisational profile, 35

outcome and program, 19, 83

- resources for outcome, 82–83
- see also* annual performance statement

Oversight Capability Review, 4, 20, 21, 22, 23

Oversight Legislation Amendment (Robodebt Royal Commission Response and Other Measures) Bill 2024, 15

overturning a presumption of nationality, 111, 113

own-motion inquiries, 89, 91, 109, 115, 129, 130

P

parliamentary committees

- IGIS submissions and appearances, 3, 11, 14–15, 29–30, 50

Parliamentary Joint Committee on Intelligence and Security (PJICIS), 2, 3, 15, 50, 113–114

People Capability Framework, 34

performance pay, 41

performance results and discussion *see* annual performance statement

personal information protection *see* Privacy Rules

Portfolio Budget Statements, 18

- Office of the Inspector-General of Intelligence and Security outcome, 19, 83

portfolio membership, 45

preliminary inquiries, 10, 14, 99, 100, 107, 114, 115

- complaints inquiries, 134–135
- own-motion, 115, 129, 130

Prime Minister, 14, 123

Privacy Rules, 105, 111, 118, 121

procurement *see* purchasing and procurement

Public Governance, Performance and Accountability Act 2013, iii, vi, 18, 42, 43, 51

Public Governance, Performance and Accountability (Financial Reporting) Rule 2015, iii, vi

Public Governance, Performance and Accountability Rule 2014, iii, vi, 51

public information, 11, 14, 19, 29–30

Public Interest Disclosure Act 2013, 2, 3, 11, 133, 136–139, 227–228

public interest disclosures, 132, 136–139

- authorised officers, 11
- disclosable conduct, 136–139
- IGIS function and powers, 3, 11, 28, 133, 136–137, 139
- inquiries, 102
- intelligence agency obligations, 139
- investigations, 2, 28, 86–87, 136–139
- performance results and analysis, 26–28
- statistics, 5, 132, 133, 136

Public Service Act 1999, 36, 39, *see also* Australian Public Service (APS)

purchasing and procurement, 51–54

purpose, 9, 19

Q

Quiggin, Peter, 44

R

Reconciliation Action Plan, 33

record keeping, 126

AGO, 118

ASD, 110

ASIO, 90

ASIS, 103, 104, 107

corporate record-keeping systems, 18

DIO, 121

Office, 18

ONI, 124

recruitment, 4, 35–36, *see also* staff

REDSPICE (Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers), 108

Reflect Reconciliation Action Plan, 33

regulation *see* ministerial authorisations;
ministerial directions; Privacy Rules

remuneration

allowances and non-salary benefits, 39

Audit and Risk Committee members, 43–44

executives, 39–40

Inspector-General of Intelligence and
Security, 39, 40

key management personnel, 40

performance pay, 41

reporting framework *see* annual performance
statement

resources for outcome, 82–83

Respect@Work legislation, 91, 117, 125, 129, 130

review of year, 2–4

rewards and recognition program, 34

risk management, 44, 48–49

risk-based annual inspection plans, 23

risk-based proactive inspections, 10, 86, *see also*
inspections

Royal Commission into the Robodebt Scheme, 15

Rules to Protect the Privacy of Australians *see*
Privacy Rules

S

security clearance processes, 4, 39, 49

security plan, 48, *see also* risk management

Senate Continuing Order for Indexed File Lists
(Harradine Order), 50

Senate Legal and Constitutional Affairs
Legislation Committee, 15, 50

senior executives

key management personnel, 39, 40

profile, 38

recruitment, 36

remuneration, 39–40

senior-level meetings held, 4, 5, 11, 14, 29, 30, 89,
102, 109, 117

Sex Discrimination Act 1984, 125, 130

shared services arrangements, 45

signals intelligence *see* Australian Signals
Directorate (ASD)

small business participation in procurement, 51

Social Club, 33

special intelligence operations, 88, 91

staff, 32–41

APS Census Action Plan, 4, 34

average staffing level, 32, 35, 83

diversity and inclusion, 33

Employee Value Proposition, 37

employment arrangements, 5, 35, 39

flexible work arrangements, 32, 39

key management personnel, 39, 40

learning and development, 34

non-salary benefits, 39

profile, 5, 35, 38

recruitment and retention, 4, 35–36

remuneration, 39–41

rewards and recognition, 34

values and code of conduct, 12, 32

workforce planning, 35, 36

workplace health and safety, 41

stakeholder engagement, 45–47, *see also*
international engagement

Stanbridge, Sarah, 13, 40

Strengthening Oversight of the National
Intelligence Community Bill 2025, 2

study assistance, 39

surveillance devices, 98

Surveillance Devices Act 2004, 127

*Surveillance Legislation Amendment (Identify and
Disrupt) Act 2021*, 8, 127

T

Technical Advisor role, 34

Telecommunications Act 1997, 90

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

ASD non-compliance, 112–113

ASIO non-compliance, 92–93

training, 34

U

United Nations Convention on the Rights of
Persons with Disabilities, 41

use-of-force notifications, 92

V

values, 12, 32, *see also* ethical standards

visa-related complaints, 5, 25, 133

W

warrants, 88, 130

network activity warrants (NAWS), 8, 127–128,
133, 134

weapons management, 104

website, ii

whistleblower protection scheme *see* public
interest disclosures

Work Health and Safety Act 2011, 41

workforce *see* staff

workplace health and safety, 41

workplace sexual harassment Good Practice
Framework compliance, 91, *see also*
Respect@Work legislation

Y

year at a glance, 5

