



**IGIS**

INSPECTOR-GENERAL OF  
INTELLIGENCE AND SECURITY

# 2021–2022

## ANNUAL REPORT

## 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](mailto:info@igis.gov.au)  
Website: [www.igis.gov.au](http://www.igis.gov.au)

## COMPLAINTS

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

## NON-ENGLISH SPEAKERS

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

## ACKNOWLEDGEMENT

Design and Typesetting: Typeyard Design & Advertising  
Printing: Elect Printing

ISSN: 1030-4657

© Commonwealth of Australia 2022



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](http://www.creativecommons.org.au)

## ACKNOWLEDGEMENT OF COUNTRY

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



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

## **Office of the Inspector-General of Intelligence and Security Annual Report 2021–2022**

I am pleased to present the Inspector-General of Intelligence and Security annual report for the period 1 July 2021 to 30 June 2022.

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

Each of the intelligence agencies within my jurisdiction has confirmed that the components of the report that relate to them will not prejudice security, the defence of Australia, Australia's relations with other countries, law enforcement operations or the privacy of individuals. The report is therefore suitable to be laid before each House of Parliament.

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

As required by s10 of the Public Governance, Performance and Accountability Rule 2014 I certify that my Office has undertaken a fraud risk assessment and has a fraud control plan, both of which are reviewed periodically. I further certify that appropriate fraud prevention, detection, investigation and reporting mechanisms are in place that meet the specific needs of my agency and that I have taken all reasonable measures to deal appropriately with fraud relating to the agency.

Yours sincerely

The Hon Christopher Jessup KC  
Inspector-General of Intelligence and Security  
27 September 2022

# CONTENTS

Contact information	inside cover
Letter of transmittal	iii
About this report	vi
Glossary	vii

## SECTION ONE

<b>REVIEW BY THE INSPECTOR-GENERAL</b>	<b>1</b>
Inspector-General's review	2

## SECTION TWO

<b>OVERVIEW</b>	<b>5</b>
Purpose	6
Our approach	7
About us	8
Key activities	9
Organisation chart	10
Providing assurance	11

## SECTION THREE

<b>ANNUAL PERFORMANCE STATEMENT</b>	<b>15</b>
2021–22 Annual Performance Statement	16
Reporting framework	17
2021–22 Performance Review	19

## SECTION FOUR

### **MANAGEMENT AND ACCOUNTABILITY** **25**

---

Our staff and culture	26
Organisational profile	29
Corporate governance	35
Stakeholders	38
Risk oversight and management	40
External scrutiny	42

## SECTION FIVE

### **FINANCIAL STATEMENTS** **45**

---

Financial statements	46
<b>Appendix A:</b> Entity Resource Statements and Resource for Outcomes	71

## SECTION SIX

### **REVIEW OF INTELLIGENCE AGENCIES** **73**

---

The intelligence agencies	74
Agency oversight activities 2021–22	80
Complaints and Public Interest Disclosures	102

## SECTION SEVEN

### **ANNEXURES** **107**

---

Annexure 7.1	108
Annexure 7.2	109
Index	119

# ABOUT THIS REPORT

This report provides information on the activities, achievements and performance of the Office of the Inspector-General of Intelligence and Security (IGIS/the Office) for the 2021–22 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), s 35 of the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) and other legislation.

## GUIDE TO THE REPORT

**Section One** contains the Inspector-General’s review of the reporting period and outlook for 2021–22.

**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 2021–22.

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

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

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

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

# GLOSSARY

<b>AAT</b>	Administrative Appeals Tribunal
<b>ACIC</b>	Australian Criminal Intelligence Commission
<b>ACSC</b>	Australian Cyber Security Centre
<b>ACLEI</b>	Australian Commission for Law Enforcement Integrity
<b>ACT</b>	Australian Capital Territory
<b>ADF</b>	Australian Defence Force
<b>AFP</b>	Australian Federal Police
<b>AGD</b>	Attorney-General's Department
<b>AGO</b>	Australian Geospatial-Intelligence Organisation
<b>AHRC Act</b>	<i>Australian Human Rights Commission Act 1986</i>
<b>AMLCTF Act</b>	<i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i>
<b>ANAO</b>	Australian National Audit Office
<b>APS</b>	Australian Public Service
<b>Archives Act</b>	<i>Archives Act 1983</i>
<b>ASD</b>	Australian Signals Directorate
<b>ASIO</b>	Australian Security Intelligence Organisation
<b>ASIO Act</b>	<i>Australian Security Intelligence Organisation Act 1979</i>
<b>ASIS</b>	Australian Secret Intelligence Service
<b>ASL</b>	Average Staffing Level
<b>AUSTRAC</b>	Australian Transaction Reports and Analysis Centre
<b>CCSSC</b>	Cultural and Corporate Shared Services Centre
<b>Comprehensive Review</b>	Comprehensive Review of the Legal Framework of the National Intelligence Community
<b>CPRs</b>	The Commonwealth Procurement Rules
<b>Crimes Act</b>	<i>Crimes Act 1914</i>
<b>Criminal Code</b>	<i>Criminal Code Act 1995</i>
<b>CT(TEO) Act</b>	<i>Counter-Terrorism (Temporary Exclusion Orders) Act 2019</i>
<b>D&amp;I</b>	Diversity and Inclusion
<b>DIO</b>	Defence Intelligence Organisation
<b>FIORC</b>	Five Eyes Intelligence Oversight and Review Council

<b>The Five Eyes</b>	The Five Eyes countries comprising an intelligence partnership of Australia, Canada, New Zealand, the United Kingdom and the United States
<b>FOI Act</b>	<i>Freedom of Information Act 1982</i>
<b>KMP</b>	Key Management Personnel
<b>ICT</b>	Information and Communications Technology
<b>IGIS/The Office</b>	The statutory agency of the Inspector-General of Intelligence and Security
<b>IGIS Act</b>	<i>Inspector-General of Intelligence and Security Act 1986</i>
<b>IPS</b>	Information Publication Scheme
<b>IS Act</b>	<i>Intelligence Services Act 2001</i>
<b>MA</b>	Ministerial Authorisation
<b>NAWs</b>	Network Activity Warrants
<b>NIC</b>	National Intelligence Community
<b>ONI</b>	Office of National Intelligence
<b>ONI Act</b>	<i>Office of National Intelligence Act 2018</i>
<b>PBS</b>	Portfolio Budget Statements
<b>PGPA Act</b>	<i>Public Governance, Performance and Accountability Act 2013</i>
<b>PGPA Rule</b>	<i>Public Governance, Performance and Accountability Rule 2014</i>
<b>PID Act</b>	<i>Public Interest Disclosure Act 2013</i>
<b>PID</b>	Public Interest Disclosure
<b>PJCIS</b>	Parliamentary Joint Committee on Intelligence and Security
<b>Privacy Act</b>	<i>Privacy Act 1988</i>
<b>Public Service Act</b>	<i>Public Service Act 1999</i>
<b>REDSPICE</b>	Resilience - Effects - Defence - Space - Intelligence - Cyber - Enablers
<b>SES</b>	Senior Executive Service
<b>SIO</b>	Special intelligence operations
<b>Surveillance Legislation (Identify and Disrupt) Act</b>	<i>Surveillance Legislation Amendment (Identify and Disrupt) Act 2021</i>
<b>The intelligence agencies</b>	ONI, ASIO, ASIS, ASD, AGO and DIO
<b>TIA Act</b>	<i>Telecommunications (Interception and Access) Act 1979</i>
<b>Telecommunications Act</b>	<i>Telecommunications Act 1997</i>
<b>WHS Act</b>	<i>Work Health and Safety Act 2011</i>



# **SECTION ONE**

## REVIEW BY THE INSPECTOR-GENERAL

# INSPECTOR-GENERAL'S REVIEW



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

As is apparent from this report, the conduct of inquiries, the making of regular inspections and the investigation of complaints are core functions of the Office. Regular inspection work is a daily, fundamental activity for the Office. During the year under review, one inquiry (which had been commenced in a previous year) was completed. Further particulars of this inquiry are set out in the relevant section of this report. The complaints practice of the Office continues to grow and evolve, and details of this practice can be found in this report.

Our inspection teams regularly encounter material in the files of agencies (some more so than others) which provide evidence of non-compliance, either with the law or with appropriate standards of propriety. In the great majority of such instances, the matters are towards the less serious end of the spectrum, and are readily put to rights upon being drawn to the attention of the agencies concerned. Indeed, in many cases the matters of concern are drawn to the Office's attention by the relevant agencies themselves.

In general terms, the agencies overseen by the Office did, in the year under review, treat compliance as a matter of importance, both organisationally and in their ongoing protocols and practices. Further, they treated regular inspection and oversight by the Office as a conventional feature of their ongoing operations. Here it is important to stress that this disposition on the part of the agencies implied no compromise of the independence of the Office or of the rigour of its oversight: rather, the assumption implied by it was that the agencies welcomed the impact upon their own compliance discipline which that oversight involved. This state of affairs – and the generally high level of compliance produced by it – made its own contribution to the activity of the Office.

Responding to change has been, over the year under review and more broadly, an ever-present challenge for the Office.

First, as noted in last year's Annual Report, the COVID-19 pandemic continued to have an impact on work in this reporting year. In particular, lockdowns within the ACT during the period August – October, together with ongoing isolation rules, resulted in unavoidable disruptions to operational activity. The Office activated its COVID-19 working arrangements that were previously implemented in 2020. While some of the Office's enabling services were able to continue largely without interruption, other work was affected because the security classifications of material relevant to IGIS's core inspection, complaint and inquiry activities mean that this work cannot be done remotely.

Over the past year, this Office has ensured that the work that needed to be delayed over the last reporting year because of COVID-19 was resumed and completed as restrictions eased in the ACT and other jurisdictions. However, interstate travel to undertake the work of the Office continued to be affected over the course of this year, as restrictions were implemented and lifted in various jurisdictions across Australia. No international travel occurred during the year. Despite these challenges, the Office continued to meet critical deadlines.

Secondly, since the publication of the 2017 Independent Intelligence Review, an increase in the number of agencies for which the Office has oversight responsibilities has been a strong likelihood, but, over time, the extent and detail of that proposal have been subject to adjustment.

The *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*, which came into force in September 2021, gave the Office oversight over the use of network activity warrants by an additional two agencies (the Australian Federal Police (AFP) and Australian Criminal Intelligence Commission (ACIC)).

The Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020, introduced on 9 December 2020, also sought to expand the oversight of the Office to include the intelligence functions of the Australian Transaction Reports and Analysis Centre and of the ACIC. This Bill, however, lapsed on dissolution of the 46th Parliament.

As was the case last year, in this reporting year there were changes to the legislative framework affecting agencies within the IGIS's jurisdiction. The Office was consulted on the development of these proposals for change, and continues to contribute significantly to the consultation processes regarding further proposed change. Often the legislation governing intelligence work can be legally and technically complex; this consultation is an important feature of legislative design and development as it assists in ensuring that structures supporting effective oversight are recognised and included in legislation.

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

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

The Office continued to work with the Office of the Australian Information Commissioner (OAIC) on a project related to the COVIDSafe App, and provided two reports on the project to the Information Commissioner which were published on the OAIC website.

The Office's international engagement with other Five Eyes oversight bodies was maintained throughout the year, although the annual Five Eyes Intelligence Oversight and Review Council conference was held virtually in November 2021 due to restrictions on travel. Meeting virtually enabled this important dialogue to continue, but underscored the importance of discussions in person, when possible, in maintaining our professional relationships and supporting an open exchange of ideas and approaches.

This year also provided the Office with the opportunity to refine further the flexible and innovative ways of working that have been developed in response to the challenges of the COVID-19 lockdown and isolation rules. The Office's corporate governance framework continued to be strengthened, and several key projects were completed over the year particularly in the information governance space. The work of further embedding corporate and information governance systems and processes will continue into the next reporting year, as the Office continues to grow.

More generally, although the Office had many new staff join it over the year, the planned expansion to the Office's full complement of staff has not yet been reached for a number of reasons, including those related to the necessary but lengthy security clearance process. The Office, like many public sector agencies, continues to feel the challenges of recruiting and retaining subject matter experts across a range of skillsets. These challenges continue across ICT, information governance and HR within the corporate streams, and other agency specific roles required in intelligence oversight.

In the coming year, the Office will continue its focus on strategic HR initiatives and strategies to continue to attract talent, retain high quality staff and provide a rewarding and intellectually stimulating work environment.

Finally, this year marked the 35th anniversary of the establishment of the Office of the Inspector-General of Intelligence and Security. This is an auspicious moment, both for what has been achieved and for what the future holds for this Office. The work of this Office is important, and it is critical to independent and credible oversight of the intelligence community. I thank all staff of my Office for their professionalism and dedication over the year.

# SECTION TWO

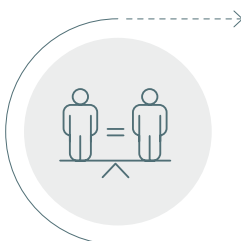
## OVERVIEW

# PURPOSE

The purposes of IGIS reflect the objects contained in section 4 of the IGIS Act, including:

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

# OUR APPROACH



## Independent and impartial

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



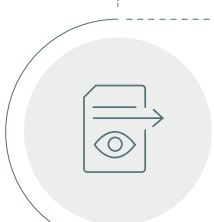
## Astute and informed

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



## Measured

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



## Open

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



## Influential

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

# ABOUT US

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

The Office does this by inspecting, inquiring into and reporting on agency activities. As set out in the IGIS Act, the intelligence agencies IGIS oversees are:

- Office of National Intelligence
- Australian Security Intelligence Organisation
- Australian Secret Intelligence Service
- Australian Signals Directorate
- Australian Geospatial-Intelligence Organisation
- Defence Intelligence Organisation

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

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

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

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



# KEY ACTIVITIES

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

## INQUIRIES AND PRELIMINARY INQUIRIES

Conducting inquiries is a core function of IGIS. An inquiry may be initiated by the Inspector-General by their own motion (which may in some cases be in response to a complaint) or at the request of the Attorney-General, the relevant responsible minister and the Prime Minister. Although it is customary for the intelligence agencies to cooperate fully with IGIS, the Inspector-General is granted Royal Commission-like powers under the IGIS Act to undertake inquiries. The provision of these powers is an important element in the authority of the Inspector-General and the oversight of agencies. A preliminary inquiry may be initiated by the Inspector-General into the action of an intelligence agency, either in connection with a complaint or of the Inspector-General's own motion. This process provides the means for the Inspector-General to make preliminary investigations and to determine whether a formal inquiry into the action is within their authority and warranted in the circumstances.

## REGULAR INSPECTIONS

The conduct of regular inspections on a day-to-day basis is an important activity of IGIS. This is carried out by inspection teams, each specialising in the oversight of one or more of the intelligence agencies. IGIS receives a high degree of cooperation from the agencies in the conduct of these inspections including, in many cases, self-reporting of instances of potential non-compliance. Biannual reports of key inspections and other activities are provided to each relevant responsible minister.

## COMPLAINTS

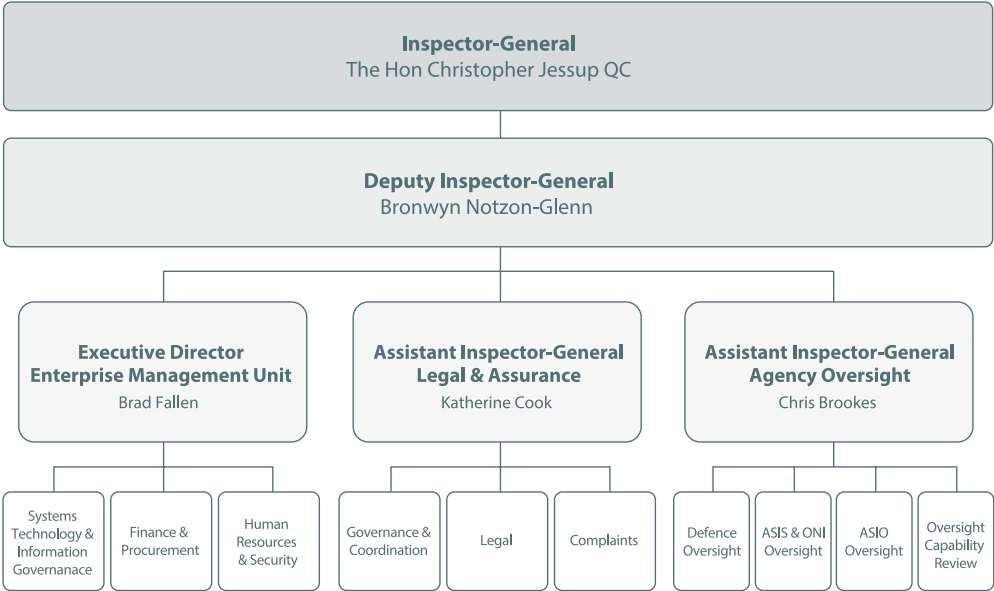
The Office receives contacts from a range of people – including current or former staff of the intelligence agencies, people who have had dealings with the agencies, and others. These contacts are mostly initiated through the general complaint form on the IGIS website. Once a contact is assessed as a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

## PUBLIC INTEREST DISCLOSURES

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

# ORGANISATION CHART

Figure 2.1: IGIS organisational structure at 30 June 2022



# 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 2021–22, no occasion arose for a report on inadequate action.

Under s 25A of the IGIS Act, the Inspector-General may report to the responsible minister on a completed inspection of an intelligence agency. In 2021–22, the Inspector-General wrote to responsible ministers to provide updates regarding the Office’s inspection and review activities.

The Inspector-General also wrote to the responsible Minister concerning the COVIDSafe app report, disclosures and complaints, and legislative developments. The Inspector-General and IGIS officers also met with staff of responsible ministers to discuss how IGIS conducts inspection and review activities.

During 2021–22, no requests were made by the Prime Minister or ministers for the Inspector-General to conduct an inquiry under the IGIS Act.

## PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY (PJCIS)

During 2021–22 the Inspector-General and senior staff appeared before the PJCIS in a public hearing into the review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Bill 2021.

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 remarks in the context of the Office’s oversight and review role, but do not comment on the policies underpinning the bills.

**Table 2.1: 2021–22 Inspector-General submissions to PJCIS****Inspector-General Submissions to PJCIS**

Submission 10 to the *Review of Administration and Expenditure No. 20 (2020–2021)* by the Parliamentary Joint Committee on Intelligence and Security.

Submission to the *Review of the Migration and Citizenship Legislation Amendment (Strengthening Information Provisions) Bill 2020* by the Parliamentary Joint Committee on Intelligence and Security.

Submission 7 to the *Review of the Counter-Terrorism (Temporary Exclusion Orders) Act 2019* by the Parliamentary Joint Committee on Intelligence and Security.

Submission 10 to the *Review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Bill 2021* by the Parliamentary Joint Committee on Intelligence and Security.

Submission 25 to the *Review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* by the Parliamentary Joint Committee on Intelligence and Security.

## EVIDENCE TO THE AAT AND THE AUSTRALIAN INFORMATION COMMISSIONER

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

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

During the reporting period, the Inspector-General received 3 requests for evidence from the Australian Information Commissioner.

## INFORMING THE PUBLIC

A purpose of the Inspector-General under the IGIS Act is to assist the Government in assuring the public that intelligence and security matters relating to Commonwealth agencies are open to scrutiny, in particular the activities and procedures of intelligence agencies. The Office does this, among other things, by making unclassified information about its activities publicly available where possible, and through other activities such as its engagement program.

The Office conducts a program of presentations to the broader community. This includes presentations to groups who have an interest in national security and intelligence matters, such as those who study and research in the area.

The ongoing effects of COVID-19 lockdowns and travel restrictions made it more challenging for the Office to conduct an effective outreach program; however, the Office took proactive steps to increase its engagement in 2022 as soon as it was possible. Senior staff presented at a number of public forums, including university lectures, on the role of the Office and effective oversight of the intelligence agencies.



# **SECTION THREE**

## ANNUAL PERFORMANCE STATEMENT

# 2021–22 ANNUAL PERFORMANCE STATEMENT

## STATEMENT BY THE ACCOUNTABLE AUTHORITY

As the Inspector-General and accountable authority for the Office of the Inspector-General of Intelligence and Security, I present IGIS's annual performance statement for the financial year 2021–22, 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

IGIS's performance framework is set out in its Corporate Plan 2021–22 and the Portfolio Budget Statements (PBS). In preparing the annual performance statement, IGIS draws data from its corporate recordkeeping systems.



# REPORTING FRAMEWORK

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

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

Independent assurance for the Prime Minister, senior 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.

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

Figure 3.1: IGIS Reporting Framework



# 2021–22 PERFORMANCE REVIEW

During 2021–22, the Office performed strongly against its four objectives and achieved or partially achieved its targets on all 5 performance measures due to be measured in 2021–22. For the majority of measures, the target for this reporting period was to establish a baseline to provide a benchmark for future performance assessment. However, in the process of establishing baseline metrics it was identified that a 'baseline' statistic would not provide meaningful data to measure the Office's performance, due to the highly varied and complex nature of the inquiry, inspection, complaints and PID work undertaken by this Office. As a result of this finding, all performance measures and targets have been adjusted in the 2022–23 Corporate Plan to allow the Office to better measure and record its performance.

Due to the changes made to the IGIS performance framework for the 2022–23 reporting period, the Office elected to assess 2021–22 performance against the 'baseline measures' based on the overall intent of the measure. This involves looking at a range of data and outcomes to assess whether the work of the Office was efficient, effective and compliant with governing legislation.



## Objective 1: Inquiries

Provide ministers, and to the extent possible the public, with independent information by conducting inquiries relating to legality, propriety and consistency with human rights.

No.	Measure	Target	Result
1.1	The percentage of inquiries where, before the commencement thereof, the responsible minister and/or the head of the relevant agency and/ or the Secretary of Defence (as required) were informed [IGIS Act, s 15].	100%	100%
1.2	The percentage of inquiries where, before the commencement thereof, the responsible minister and/or the head of the relevant agency and/ or the Secretary of Defence (as required) were informed [IGIS Act, s 15].	100%	100%
1.3	The percentage of inquiries where, before the commencement thereof, the responsible minister and/or the head of the relevant agency and/ or the Secretary of Defence (as required) were informed [IGIS Act, s 15].	Baseline to be established	Intent achieved
1.4	The percentage of inquiries where, before the commencement thereof, the responsible minister and/or the head of the relevant agency and/ or the Secretary of Defence (as required) were informed [IGIS Act, s 15].	Baseline to be established	Intent achieved

## Analysis

During 2021–22, the Office achieved its objective to provide ministers, and to the extent possible the public, with independent information by conducting inquiries relating to legality, propriety and consistency with human rights. One inquiry which commenced 7 May 2021 was undertaken and completed in 2021–22. The inquiry was completed despite challenges in conducting interviews with key individuals due to COVID-19. Once interviews were completed, draft and final reports were produced in a timely manner and shared with agency leadership, the responsible Minister and with the complainant. Chapter 6 provides a detailed overview of the Office's inquiry work during the reporting period.



## Objective 2: Inspections

Provide ministers, and to the extent possible the public, with independent information by conducting regular inspection of a range of operational activities to monitor the legality, propriety and consistency with human rights of intelligence agencies.

No.	Measure	Target	Result
2.1	The number of intelligence agencies in respect of which an inspection plan has been prepared by September in the relevant year.	6	Partially achieved
2.2	The number of intelligence agencies in respect of which the responsible ministers have been provided with reports about key inspection activities at least every six months in the relevant year. [IGIS Act, s 25A]	6	Partially achieved
2.3	The number of intelligence agencies with whose senior officers the IGIS Executive conferred at least every six months in the relevant year.	6	Achieved
2.4	In relation to compliance incidents coming to the attention of inspection teams, the average number of days taken by the teams to complete their investigations and, where required, their reports.	Baseline to be established	Intent achieved

### Analysis

During 2021–22, the Office achieved its objective to provide ministers, and to the extent possible the public, with independent information by conducting regular inspection of a range of operational activities to monitor the legality, propriety and consistency with human rights of intelligence agencies. Measures 2.1 and 2.2 were partially achieved due to COVID 19 restrictions. The ACT lockdowns resulted in staff working a roster system which reduced the number of staff in the office during that time. As a result, work had to be prioritised which resulted in slight delays to some inspection activity.

In relation to performance 2.4, all compliance incidents were investigated and feedback provided to agencies. A valid baseline was unable to be developed due to the highly varied nature of the compliance incidents and the level of review required, the diverse functions of the intelligence agencies, and the impact of COVID-19 on resourcing.

Chapter 6 provides a detailed overview of the Office's inspection activity during the reporting period.



### Objective 3: Complaints

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

No.	Measure	Target	Result
3.1	The average number of days, after receipt of a complaint, within which an acknowledgement is sent to the complainant.	Baseline to be established	Intent achieved
3.2	The average number of days, after receipt of an oral complaint, within which the complaint is put, or the complainant is required to put the complaint, in writing. [IGIS Act, s 10(2)]	Baseline to be established	Intent achieved
3.3	<p>The average number of days, after receipt of a complaint, within which it is decided that:</p> <ul style="list-style-type: none"> <li>the complaint is not within authority; or the complaint is within authority, but there will be no inquiry; or</li> <li>there will be an inquiry; or</li> </ul> <p>a preliminary inquiry is necessary. [IGIS Act, ss 11, 14]</p>	Baseline to be established	Intent achieved
3.4	The average number of days, after completion of a preliminary inquiry, within which it is decided whether the complaint is within authority, and if so, whether there will be an inquiry. [IGIS Act, s 14]	Baseline to be established	Intent achieved
3.5	Where there has been no, or no further, inquiry, the average number of days within which the complainant has been informed accordingly. [IGIS Act, s 12]	Baseline to be established	Intent achieved
3.6	The number of intelligence agencies in respect of which the agency head, and the responsible minister, have been informed, at least once in the relevant year, of the complaints where there were no, or no further, inquiries. [IGIS Act, s 12]	Baseline to be established	Intent achieved
3.7	The average number of days, after the required agreement with the head of the relevant agency, within which a response relating to the inquiry is given to the complainant and to the responsible minister. [IGIS Act, s 23]	Baseline to be established	Intent achieved

**Analysis**

During 2021–22, the Office achieved its objective to investigate complaints made by the public, or by a current or former staff of an intelligence agency, about the activities of an intelligence agency.

The Office received 80 complaints during the year that fell within the jurisdiction of the IGIS Act. In addition, the Office received 141 complaints about visa and citizenship matters which are reported separately. The Office also considered more than 400 additional pieces of correspondence to determine whether they fell within the Inspector-General's jurisdiction.

The Office continues to streamline and strengthen its complaints processes to ensure that it deals with complaints under the IGIS Act in an efficient and effective manner.



#### Objective 4: Public Interest Disclosures

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

No.	Measure	Target	Result
4.1	The average number of days, after receipt of a disclosure, within which an acknowledgement is sent to the complainant.	Baseline to be established	Intent achieved
4.2	The average number of days, after receipt of a disclosure, within which to decide whether there is a reasonable basis on which to consider the disclosure to be an internal disclosure. [PID Act, s 43(2)]	Baseline to be established	Intent achieved
4.3	The average number of days, after receipt of a disclosure, within which to allocate the handling of the disclosure. [PID Act, s 43(1)]	Baseline to be established	Intent achieved
4.4	<p>The average number of days, after allocation of a disclosure to the Inspector-General, within which the discloser is informed that:</p> <ul style="list-style-type: none"><li>the disclosure will be investigated, and whether under the PID Act or the IGIS Act; or</li><li>the disclosure will not be investigated. [PID Act, ss 48, 49, 50]</li></ul>	Baseline to be established	Intent achieved
4.5	The average number of days, after allocation of a disclosure to the Inspector-General, within which the investigation is completed. [PID Act, s 52]	Baseline to be established	Intent achieved
4.6	The average number of days, after completion of an investigation, within which a report of the investigation is prepared. [PID Act, s 51(1)]	Baseline to be established	Intent achieved
4.7	The average number of days, after preparation of the report, within which a copy is given to the discloser. [PID Act, s 51(4)]	Baseline to be established	Intent achieved

## Analysis

During 2021–22, the Office achieved its objective to receive and, where appropriate, investigate authorised disclosures about suspected wrongdoing within an intelligence agency.

In 2021–22, the Office received a total of 10 disclosures relating to intelligence agencies under the PID Act:

- The Office received 9 disclosures directly, 5 of which it allocated to itself, and 4 it allocated to other agencies.
- The Office received 1 disclosure indirectly when it was allocated the disclosure by another agency.

The Office commenced two investigations under the PID Act during 2021–22. At the end of the reporting period, one of the two investigations was complete and the other was ongoing.

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

The Office continues to streamline and strengthen its processes in relation to PIDs.



# **SECTION FOUR**

## MANAGEMENT AND ACCOUNTABILITY

# OUR STAFF AND CULTURE

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

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

## DIVERSITY AND INCLUSION

IGIS's commitment to diversity and inclusion reflects the importance we place on our people and on creating a workplace culture in which every employee is valued and respected for their contribution.

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

The Committee works closely with the IGIS Women's Network as well as partners in the Attorney-General's Department and across the National Intelligence Community, drawing on these larger networks to support, enable, and add to our existing efforts.

During 2021–22, the Committee focused on developing a Reconciliation Action Plan, working to embed D&I into office culture and planning, and extending outreach through events, resource packs, and raising awareness. A key outcome was the development and endorsement of the IGIS D&I Statement, now published on the IGIS website and included in recruitment packs. It is a visible commitment by the Office to build a diverse and inclusive work environment, as well as a reminder of the goals and values it strives toward.

In early 2022, staff participated in a voluntary Health Check regarding D&I at IGIS. It highlighted positives for the Office as well as identifying areas for continuing improvement. The results are being used to inform and prioritise organisational change and efforts from the Committee and beyond. Key findings include:

**Figure 4.1: Diversity and Inclusion Health Check Results**

## LEARNING AND DEVELOPMENT

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

Particular importance is placed on the retention of staff, flexible working arrangements, and workplace training to promote leadership skills and capability development. The Office's human resources and learning and development function continues to mature and work continues to further strengthen professional development. A range of opportunities are available for staff, including management and leadership courses, the APS Academy, National Centre for Intelligence Training and Education programs and courses with the Australian National University's National Security College.

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

## OVERSIGHT CAPABILITY REVIEW

In the second half of 2021–22, the Office allocated one staff member to undertake an Oversight Capability Review (the Review) to examine the current practices, procedures and capabilities of the proactive oversight area of IGIS, and to provide recommendations on how it can remain fit-for-purpose to provide strong oversight, in particular in the context of:

- the NIC's current and likely future activities
- any expansion or increased investment in the NIC and resulting capability changes
- the future technology environment and the increasing technological complexity of NIC operations in delivering against its various missions.

The Review has developed an executive agreed scope and outcomes, and internal consultation has commenced. This has included workshops and individual discussions, to understand the current practices, processes and capabilities and to collect initial thoughts on areas for enhancement.

The Review will continue into 2022–23 and final findings and recommendations will be delivered to the Executive Board for consideration.

# ORGANISATIONAL PROFILE

IGIS had an average staffing level (ASL) of 42 for 2021–22, having recruited against a target ASL of 56. The gap between the actual and target ASL is due to a number of contributing factors, including: a slow-down of recruitment activity during COVID-19 lockdowns; timeframes for new starters to progress through the clearance pipeline; and ongoing separation of staff either retiring or moving into other roles.

The Office continues to experience the impact of labour market shortages across a range of critical skill sets in both corporate and operational areas. The changing nature of work, digital transformation and increasing demand for skills has contributed to this and the competition for talent is further complicated by the clearance process which subsequently lengthens the recruitment processes.

The Office continues to explore opportunities to source and attract talent, including creative approaches to job design, employee referral programs and promotion of flexible working arrangements. Reporting and workforce planning activities across the Office ensures forecasting of critical roles and ongoing recruitment activities to meet these challenges. These functions will enable the Office to further grow in capability to meet organisational requirements into the future.

## RECRUITMENT

During 2021–22, the Office conducted a number of recruitment campaigns to strengthen its workforce of specialist oversight and corporate officers. Several successful campaigns were completed across the APS, Executive Levels and SES for a variety of roles. In addition, operational roles were also prioritised and campaigns completed resulting in the commencement of a number of new employees.

The Office, alongside other APS agencies, faced significant challenges to recruitment during this period. This has led to innovation in our attraction and development strategies such as temporary employment register for vacancies and secondments across the NIC. The use of a multiclassification workforce is being explored, with the view to expand further the potential workforce. This will be evaluated into 2022–23.

At 30 June 2022, the Office had a total of 49 ongoing employees. This included 5 staff (10 per cent) on long-term leave arrangements and 7 staff (14 per cent) on part-time work arrangements. There were no staff employed on a non-ongoing basis, and no IGIS staff working at locations outside of Canberra; however, the Office is exploring and where possible strengthening opportunities for flexible based work. No employees identified as Indigenous in 2021–22.

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

**Table 4.1: Overview of substantive IGIS staffing profile**

APS classification (salary range 2021–22)	At 30 June 2022			At 30 June 2021		
	Ongoing	Non-ongoing	Total	Ongoing	Non-ongoing	Total
<b>APS Classification</b>						
APS 4 (\$70,966 - \$ 77,213)	2	0	2	1	0	1
APS 5 (\$78,999 - \$ 85,694)	1	0	1	1	0	1
APS 6 (\$90,155 - \$ 101,315)	11	0	11	7	0	7
Executive Level 1 (\$108,902 - \$ 121,401)	23	0	23	16	0	16
Executive Level 2 (\$126,753 - \$ 150,854)	7	0	7	7	0	7
SES Band 1	3	0	3	2	0	2
Deputy Inspector-General (SES Band 2)	2	0	2	2	0	2

**Table 4.2 Gender balance as at 30 June 2022**

Level	Male	Female
APS 4-6	3	11
EL1	11	12
EL2	3	4
SES Band 1	2	1
SES Band 2	1	1

## EMPLOYMENT FRAMEWORKS

All IGIS officers are employed under the Public Service Act. Since 6 May 2020, all non-SES officer salaries and conditions were made under the *OIGIS Enterprise Agreement 2020–2023*. There are currently 5 SES officers employed in accordance with individual determinations under subs 24(1) of the Public Service Act.

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 \$1,229.

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

## EXECUTIVE REMUNERATION

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

The terms and conditions of all SES officer employment, including salary, are set out in individual determinations. Each determination is reviewed annually with the Inspector-General, with general performance discussions occurring during the year. The Inspector-General's remuneration is determined by the Remuneration Tribunal.

## KEY MANAGEMENT PERSONNEL (KMP) EXECUTIVE REMUNERATION

**Table 4.3: Information about remuneration for key management personnel**

Key management personnel (KMP)		Short-term benefits employment benefits		Post-employment benefits		Other long-term benefits		Termination benefits	Total
Name	Position title	Base salary <sup>1</sup>	Other benefits and allowances <sup>2</sup>	Superannuation contributions	Long service leave <sup>3</sup>	Other long-term benefits	Termination benefits	remuneration	
<b>Christopher Jessup</b>	Inspector-General (1 July 2021 to 30 June 2022)	481,980	59,892	23,568	–	–	–	–	565,440
<b>Bronwyn Notzon-Glenn</b>	Acting / Deputy Inspector-General (1 July 2021 to 30 June 2022)	259,853	28,034	43,515	6,510	–	–	–	337,912
<b>Steve McFarlane</b>	Assistant Inspector-General (1 July 2021 to 30 June 2022)	113,184	25,917	48,899	4,867	–	–	–	192,867
<b>Chris Brookes</b>	Assistant Inspector-General (7 March 2022 to 30 June 2022)	56,226	8,821	10,686	1,511	–	–	–	77,244
<b>Katherine Cook</b>	Assistant Inspector-General (9 May 2022 to 30 June 2022)	31,078	3,734	6,530	808	–	–	–	42,150
<b>Brad Fallen</b>	Acting / Assistant Inspector-General and Executive Director (1 July 2021 to 30 June 2022)	192,072	11,911	28,955	4,192	–	–	–	237,130
<b>Nathan Kenney</b>	Acting / Assistant Inspector-General (7 February 2022 to 6 May 2022)	41,383	300	5,115	1,070	–	–	–	47,868
<b>Julia Searle</b>	Acting / Assistant Inspector-General (10 January 2022 to 4 March 2022)	28,261	185	3,932	626	–	–	–	33,004

<sup>1</sup> Base salary includes leave taken and the movement in annual leave provision—i.e. four weeks accrued annual leave less annual leave taken.

<sup>2</sup> Other benefits and allowances includes motor vehicle, housing and reunion allowances as part of SES remuneration packages.

<sup>3</sup> Long service leave represents the movement in long service leave provision—i.e. nine days accrued per annum less long service leave taken.

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

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



## PERFORMANCE PAY

The Office does not have a performance pay scheme.

## WORKPLACE HEALTH AND SAFETY

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

Throughout 2021–22, the additional WHS measures implemented in response to the COVID-19 pandemic were continued, including the development and constant review of the Office COVID-19 Risk Assessment. The Office monitored and provided regular updates to advise staff of the evolving conditions presented by the pandemic to put the safety of our staff at the forefront. Our actions were informed by ACT Health advice and Safe Work Australia guidelines and closely aligned with AGD procedures through engagement as tenants in the AGD building. Since the end of lockdown in the ACT in October 2021, the Office has maintained a flexible approach to working locations and hours where possible.

Throughout 2021–22, the Office continued a range of other WHS initiatives, including:

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

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

## DISABILITY REPORTING MECHANISM

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

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

## SYSTEMS TECHNOLOGY AND INFORMATION GOVERNANCE

The Office is co-located with the Attorney-General's Department at 3-5 National Circuit, Barton. These premises and IGIS's ICT systems continue to be accredited and meet all applicable standards.

Following the updates to the Office's systems technology infrastructure reported in the 2020–21 Annual Report, the Office continues to refine and progress systems infrastructure improvements on the Local Area Network as appropriate. The Office has finalised its Information Governance Framework during the reporting period and continues to undertake enhancements to its governance and management of digital information assets on both the PROTECTED network and the classified Local Area Network. The adjustments will further align the Office with whole of government information management requirements, as outlined by the National Archives of Australia policy, *Building trust in the public record: managing information and data for government and community*.

# CORPORATE GOVERNANCE

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

The Office corporate governance framework guides good governance and sound business practices across the Office. During 2021–2022, the Office conducted a comprehensive review designed to drive efficient and effective business operations; identify and mitigate risk; and drive continuous improvement and innovation through corporate planning, performance monitoring and reporting. A new governance framework was implemented in May 2022 as a result of the review.

Key components of our corporate governance framework include:

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

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

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

In addition to the Executive Board, a number of committees have been established to support the Executive Board to meet their objectives and responsibilities. These committees are focused on core business areas like security governance and complaints, and enabling functions like staff consultation, leadership, audit and diversity and inclusion. The ongoing cooperation and coordination of these committees with the Executive Board enables the effective governance of the Office and efficient business operations.

## IGIS AUDIT COMMITTEE

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

The membership and functions of the IGIS Audit Committee are structured according to the PGPA Act. The IGIS Audit Committee charter is available at [https://www.igis.gov.au/sites/default/files/2022-07/IGIS\\_Audit\\_Committee\\_Charter\\_2021\\_0.pdf](https://www.igis.gov.au/sites/default/files/2022-07/IGIS_Audit_Committee_Charter_2021_0.pdf)

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

**Table 4.4: IGIS Audit Committee membership**

Audit Committee member	Qualifications, knowledge, skills and experience	Meetings attended <sup>1</sup>	Total annual remuneration
<b>Current members</b>			
<b>Ms Sarah Vandenbroek</b> (Chair) (External member)	Ms Vandenbroek holds a Bachelor of Information Management, a Graduate Diploma in Accounting and is a Fellow of CPA Australia. Ms Vandenbroek has held a range of senior roles in the Commonwealth Public Service including as a Chief Financial Officer and a Chief Operating Officer. Ms Vandenbroek is the First Assistant Secretary for the Territories Division in the Department of Infrastructure, Transport, Regional Development and Communications.	30 September 2021 14 December 2021 29 March 2022	Nil
<b>Mr Stephen Moore</b> (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.	30 September 2021 14 December 2021 29 March 2022	\$1,980

Audit Committee member	Qualifications, knowledge, skills and experience	Meetings attended <sup>1</sup>	Total annual remuneration
<b>Mr Peter Quiggin QC</b> (External member)	Mr Quiggin holds a Bachelor of Laws, a Graduate Diploma in Professional Accounting, a Bachelor of Science, Computing and Maths and is a fellow of the Australian Institute of Company Directors. Mr Quiggin is a highly experienced former Commonwealth agency head (First Parliamentary Counsel) with extensive senior board member experience across Government and not-for-profits.	30 September 2021 14 December 2021 29 March 2022  <b>Term commenced:</b> 23 September 2021	\$11,250
<b>Former members</b>			
<b>Ms Linda Waugh</b>	Ms Waugh holds a Bachelor of Arts, a Graduate Diploma in Psychology and a Master of Business Administration. Ms Waugh has held leadership roles within both state and federal integrity bodies, and is currently the Merit Protection Commissioner for the APS and the Parliamentary Service.	<b>Term ended:</b> 23 August 2021	Nil

1. The Audit Committee meeting scheduled for 28 June 2022 was rescheduled due to a number of COVID-19 related staff absences. The meeting was subsequently held on 29 July 2022.

## INTERNAL AUDIT

During the reporting period IGIS engaged an external contractor to prepare an Internal Audit Plan to guide IGIS's internal audit program. The plan formalises how the Office will conduct internal audits going forward, and prioritises 7 audits based on an assessment of risk in line with IGIS Risk Management Policy and Framework. The Internal Audit Plan is administered by the Governance Directorate and in 2021–22 one internal audit was completed, which considered the Memorandum of Understanding with the Attorney-General's Department (AGD) for shared corporate services.

The Internal Audit Plan will drive future internal audits throughout 2022–23 and, in consultation with the Audit Committee, the Office will continue to strengthen its internal audit program to respond to the changing risk profile as the Office expands.

# STAKEHOLDERS

We maintain strong and cooperative relationships with a range of agencies and entities both Domestic and International.

## DOMESTIC ENGAGEMENT

### ATTORNEY-GENERAL'S DEPARTMENT

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

### CORPORATE SUPPORT

In addition to the corporate support provided by AGD, ASD also provide some ICT system support. Additionally, IGIS accesses some financial services via the Cultural and Corporate Shared Services Centre (CCSSC) provided by the National Museum of Australia.

### ACCOUNTABILITY AND INTEGRITY AGENCIES

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

### AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

IGIS continued to liaise with the Australian Commission for Law Enforcement Integrity (ACLEI) regarding cooperative and complementary oversight arrangements in anticipation of any proposed changes to the Inspector-General's jurisdiction, as well as on general oversight issues.

### AUSTRALIAN HUMAN RIGHTS COMMISSION

The Australian Human Rights Commission is required by subs 11(3) of the AHRC Act to refer to the Inspector-General any human rights and discrimination matters relating to an act or practice of security agencies. During 2021–22, the Australian Human Rights Commission did not refer any such matters to the Office.

## OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER

IGIS provided 2 six-monthly reports to the Commissioner that covered the incidental collection, access, use and deletion of COVIDSafe app data by relevant intelligence agencies, and their policies and procedures in place relating to Part VIIIA of the Privacy Act. IGIS officers and Office of the Australian Information Commissioner discussed matters of mutual interest during the reporting period.

## OFFICE OF THE COMMONWEALTH OMBUDSMAN

IGIS continued to engage regularly with the Office of the Commonwealth Ombudsman. The responsibilities of the 2 offices are considered complementary and a memorandum of understanding exists to provide guidance on a wide range of legislative issues and the handling of complaints that may fall within the jurisdiction of both offices.

## INTERNATIONAL ENGAGEMENT

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

In 2021–22, the Inspector-General and IGIS officers continued to engage with the Five Eyes Intelligence Oversight and Review Council (FIORC). FIORC is comprised of the following intelligence oversight, review and security entities of the Five Eyes countries:

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

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

Council members usually meet in person at least once each year. Due to COVID-19 travel restrictions, a virtual conference was held over 3 days in November 2021 hosted by the Office of the Inspector-General of Intelligence and Security of New Zealand. Sessions were held on topics including:

- technical expertise requirements for oversight
- experiences adapting to altered jurisdiction
- access to agency information.

Due to the conference being held virtually, a large number of IGIS staff were able to participate.

Council members continue to meet every few months via teleconference, and an in person annual conference in the United States is planned for late 2022.

# RISK OVERSIGHT AND MANAGEMENT

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

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

The Office's risk oversight and management tools include its Risk Management Framework, risk appetite and risk tolerance statements, Risk Register, Audit Committee reviews and the Fraud Control Plan, Business Continuity Plan, and Security Plan. The Risk Management Framework requires risk owners to be responsible for risks identified in the risk register, which includes responsibility for related controls and mitigation strategies. The Governance Directorate coordinates biannual reviews with risk owners which is considered by the Executive Board. In addition, the Audit Committee provides advice to the Inspector-General about IGIS's risk framework, governance, compliance and financial accountability. The Audit Committee is supported by an internal audit program that is supplied through externally contracted arrangements.

The Office monitors and reviews risk against the following categories:



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



## ETHICAL STANDARDS AND FRAUD CONTROL

During 2021–22, the Office continued its commitment to high ethical standards. High ethical standards across the Office are maintained through:

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

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

# EXTERNAL SCRUTINY

## REPORTS OF THE AUDITOR-GENERAL, PARLIAMENTARY COMMITTEES, THE COMMONWEALTH OMBUDSMAN OR AN AGENCY CAPABILITY REVIEW

The Australian National Audit Office completed an audit of the Office's financial statements for 2021–22. The independent auditor's report is presented in the financial statements section of this Annual Report.

During the reporting period, the Office was not subject to scrutiny by other external agencies, such as the courts, administrative tribunals, parliamentary committees or the Commonwealth Ombudsman.

## ASSET MANAGEMENT

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

## PURCHASING AND PROCUREMENT

### PURCHASING

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

The Office's purchasing framework seeks to ensure:

- procurement methods are efficient, cost-effective and take account of the Office's security needs, specialised role and size
- value for money is always the primary guiding principle
- participation in mandatory whole-of-government coordinated procurement, such as travel and property services
- support for small and medium enterprise participation
- use of the Commonwealth Contracting Suite for low-risk procurements valued under \$200,000
- use of corporate credit cards when possible and appropriate, to allow more timely payment to suppliers.

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

The Office supports small business participation in the Commonwealth Government procurement market. Small and Medium Enterprises (SME) and Small Enterprise participation statistics are available on the Department of Finance's website.

## CONSULTANTS

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

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

Details of the reportable new and ongoing consultancy contracts entered into during 2021–22 are shown in the following tables.

**Table 4.5: Reportable Consultancy contracts 2021–22**

Reportable consultancy contracts 2020–21	Number	Expenditure (GST inc.)
New contracts entered into during the reporting period	6	302,571.17
Ongoing contracts entered into during a previous reporting period	1	209,451.00
<b>Total</b>	<b>7</b>	<b>512,022.17</b>

**Table 4.6: Reportable consultancy contract expenditure 2021–22**

Name of organisation	Expenditure (GST inc.)
Yardstick Advisory Pty Ltd (ABN 38 158 309 150)	370,667.00
BellChambersBarrett (ABN 88 625 460 291)	76,307.47
Gillian Beaumont Recruitment Pty Ltd (ABN 58 107 780 683)	32,243.20
Synergy Group Australia Pty Ltd (ABN 65 119 369 827)	21,554.50
PQQC Consulting (ABN 94 484 818 597)	11,250.00

During 2021–22, 6 new reportable consultancy contracts were entered into involving total actual expenditure of \$302,571.17. In addition, one ongoing reportable consultancy contract was active during the period, involving total actual expenditure of \$209,451.

## 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 2021–22 are shown in the following tables.

**Table 4.7: Expenditure on Reportable Non-Consultancy contracts 2021–22**

Contract types	Number	Expenditure (GST inc.)
New contracts entered into during the reporting period	2	46,968.00
Ongoing contracts entered into during a previous reporting period	0	0
<b>Total</b>	<b>2</b>	<b>46,968.00</b>

**Table 4.8: Organisations receiving a share of Reportable Non-Consultancy contract expenditure 2021–22**

Name of organisation	Expenditure (GST inc.)
National Security College (ABN 52 234 063 906)	25,650.00
Workplace Research Associates Pty Ltd (ABN 11 083 481 298)	21,318.00

## AUSTRALIAN NATIONAL AUDIT OFFICE (ANAO) ACCESS CLAUSES

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

## EXEMPT CONTRACTS

During 2021–22, no IGIS contracts or standing offers were exempt from publication on AusTender on the basis that publication would disclose exempt matters under the FOI Act.

## INFORMATION PUBLICATION SCHEME

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

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

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

# **SECTION FIVE**

## FINANCIAL STATEMENTS



## INDEPENDENT AUDITOR'S REPORT

### To the Attorney-General

#### Opinion

In my opinion, the financial statements of the Office of the Inspector-General of Intelligence and Security ('the Entity') for the year ended 30 June 2022:

- (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 2022 and its financial performance and cash flows for the year then ended.

The financial statements of the Entity, which I have audited, comprise the following statements as at 30 June 2022 and for the year then ended:

- Statement by the Accountable Authority and Chief Financial Officer;
- Statement of Comprehensive Income;
- Statement of Financial Position;
- Statement of Changes in Equity;
- Cash Flow Statement;
- Notes to the forming part of the financial statements.

#### Basis for opinion

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

#### Other information

The Accountable Authority is responsible for the other information. The other information obtained at the date of this auditor's report, which was the draft annual report for the year ended 30 June 2022 did not include the financial statements and my auditor's report thereon.

My opinion on the financial statements does not cover the other information and accordingly I do not express any form of assurance conclusion thereon.

In connection with my audit of the financial statements, my responsibility is to read the other information and, in doing so, consider whether the other information is materially inconsistent with the financial statements or my knowledge obtained in the audit, or otherwise appears to be materially misstated.

If, based on the work I have performed, I conclude that there is a material misstatement of this other information, I am required to report that fact. I have nothing to report in this regard.

## Accountable Authority's responsibility for the financial statements

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

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

## Auditor's responsibilities for the audit of the financial statements

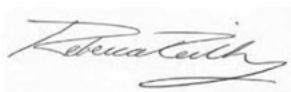
My objective is to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes my opinion. Reasonable assurance is a high level of assurance but is not a guarantee that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

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

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

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

Australian National Audit Office



Rebecca Reilly  
Executive Director

Delegate of the Auditor-General

Canberra  
29 July 2022

# CONTENTS

## Certification

### Primary financial statements

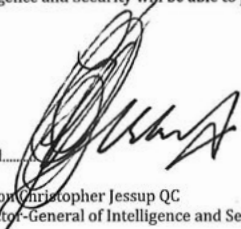

Statement of Comprehensive Income  
Statement of Financial Position  
Statement of Changes in Equity  
Cash Flow Statement

## 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



<b>STATEMENT BY THE ACCOUNTABLE AUTHORITY AND CHIEF FINANCIAL OFFICER</b>	
In our opinion, the attached financial statements for the year ended 30 June 2022 comply with subsection 42(2) of the <i>Public Governance, Performance and Accountability Act 2013</i> (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.....	Signed.....
The Hon Christopher Jessup QC Inspector-General of Intelligence and Security	Ms Jodie Hugel Chief Financial Officer
29 July 2022	29 July 2022

## Statement of Comprehensive Income

for the period ended 30 June 2022

	Notes	2022 \$	2021 \$	Original Budget \$
<b>NET COST OF SERVICES</b>				
<b>Expenses</b>				
Employee benefits	1.1A	6,653,156	5,241,113	9,323,000
Suppliers	1.1B	2,596,181	1,973,596	2,930,000
Depreciation and amortisation	2.2A	912,141	1,260,053	1,741,000
Finance costs		60	149	-
Write-down and impairment of assets		2,406	47,745	-
<b>Total expenses</b>		<b>10,163,944</b>	<b>8,522,656</b>	<b>13,994,000</b>
<b>Own-source revenue</b>				
Revenue from contracts with customers	1.2A	27,422	35,224	-
Other revenue	1.2B	40,000	40,000	40,000
<b>Total own-source revenue</b>		<b>67,422</b>	<b>75,224</b>	<b>40,000</b>
<b>Net (cost of)/contribution by services</b>		<b>(10,096,522)</b>	<b>(8,447,432)</b>	<b>(13,954,000)</b>
Revenue from Government	1.2C	12,220,000	11,908,000	12,220,000
<b>Surplus/(Deficit) after income tax on continuing operations</b>		<b>2,123,478</b>	<b>3,460,568</b>	<b>(1,734,000)</b>
<b>OTHER COMPREHENSIVE INCOME</b>				
<b>Items not subject to subsequent reclassification to net cost of services</b>				
Changes in asset revaluation reserve		-	(7,358)	-
<b>Total comprehensive income/(loss)</b>		<b>2,123,478</b>	<b>3,453,210</b>	<b>(1,734,000)</b>

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

### Budget Variances Commentary

#### Statement of Comprehensive Income

##### Employee Benefits

The variance between actual expense and the original budget is a decrease of \$2,669,844 (40%) is reflective of the difference in the associated cost of budgeted ASL (56) and actual ASL (42). Delays in on-boarding staff are linked to the extensive time to complete security related pre-employment processes. In 2022-23, ASL will increase significantly as recruitment efforts from 2021-22 materialise.

##### Suppliers

Expenses were \$331,819 (13%) lower than the original budget. This variance is consistent with employee benefits, associated supplier costs (based on number of ASL) such as security vetting, ICT and training are proportionally lower than budgeted. COVID-19 has also impacted budgeted travel expenditure.

##### Depreciation and amortisation

Actual expenditure was \$828,859 (91%) lower than the original budget. Prior and current year capital acquisitions did not materialise to the extent of that budgeted. The impact of the COVID-19 pandemic and lower ASL affected planned capital acquisition activities. Accordingly, the depreciation and amortisation of a lower asset base has driven the variance. In addition, the useful life of the Property, plant & equipment asset class was increased following regular review of depreciation rates and the Asset Valuation at 30 June 2021.

## Statement of Financial Position

as at 30 June 2022

		2022	2021	Original Budget
	Notes	\$	\$	\$
<b>ASSETS</b>				
<b>Financial assets</b>				
Cash and cash equivalents	2.1A	521,864	228,304	221,000
Trade and other receivables	2.1B	30,015,661	26,262,819	26,953,000
<b>Total financial assets</b>		<b>30,537,524</b>	<b>26,491,123</b>	<b>27,174,000</b>
<b>Non-financial assets</b>				
Leasehold Improvements	2.2A	1,481,770	1,852,212	2,099,000
Property, plant and equipment	2.2A	1,070,623	1,290,352	-
Right-of-use	2.2A	2,488	9,122	-
Intangibles	2.2A	369,240	652,029	460,000
Prepayments		170,056	149,298	32,000
<b>Total non-financial assets</b>		<b>3,094,177</b>	<b>3,953,013</b>	<b>2,591,000</b>
<b>Total assets</b>		<b>33,631,701</b>	<b>30,444,136</b>	<b>29,765,000</b>
<b>LIABILITIES</b>				
<b>Payables</b>				
Suppliers	2.3A	494,034	266,086	251,000
Other payables	2.3B	302,611	225,318	-
<b>Total payables</b>		<b>796,646</b>	<b>491,404</b>	<b>251,000</b>
<b>Interest bearing liabilities</b>				
Leases	2.4A	2,523	9,210	2,000
<b>Total interest bearing liabilities</b>		<b>2,523</b>	<b>9,210</b>	<b>2,000</b>
<b>Provisions</b>				
Employee provisions	4.1A	2,384,806	1,727,923	3,109,000
<b>Total provisions</b>		<b>2,384,806</b>	<b>1,727,923</b>	<b>3,109,000</b>
<b>Total liabilities</b>		<b>3,183,975</b>	<b>2,228,537</b>	<b>3,362,000</b>
<b>Net assets</b>		<b>30,447,726</b>	<b>28,215,599</b>	<b>26,403,000</b>
<b>EQUITY</b>				
Contributed equity		10,554,949	10,446,301	10,357,000
Reserves		14,265	14,265	22,000
Retained surplus/(Accumulated deficit)		19,878,511	17,755,033	16,024,000
<b>Total equity</b>		<b>30,447,726</b>	<b>28,215,599</b>	<b>26,403,000</b>

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

### Budget Variances Commentary

#### Statement of Financial Position

##### Non-Financial Assets

Assets recognised are \$503,177 (16%) higher than the original budget. The variance relates predominantly to the increase in the useful life of Property, plant & equipment following regular review of depreciation rates and the Asset Valuation at 30 June 2021.

##### Supplier Payables

The actual amount reported is \$243,035 (49%) higher than the original budget and relates to the timing of supplier invoices received and accrued at 30 June 2022.

##### Employee Provisions

The actual provision is \$724,194 (30%) lower than original budgeted which is reflective of the difference in the provision for a budgeted ASL (56) compared to actual ASL (42) at 30 June 2022.

## Statement of Changes in Equity

for the period ended 30 June 2022

	Notes	2022 \$	2021 \$	Original Budget \$
<b>CONTRIBUTED EQUITY</b>				
Opening balance		10,446,301	14,854,167	10,083,000
Transactions with owners				
Distributions to owners				
Returns of capital		(165,352)	(5,408,866)	-
Contributions by owners				
Departmental capital budget		274,000	1,001,000	274,000
Closing balance as at 30 June		10,554,949	10,446,301	10,357,000
<b>RETAINED EARNINGS</b>				
Opening balance		17,755,033	14,294,465	17,758,000
Comprehensive income				
Surplus/(Deficit) for the period		2,123,478	3,460,568	(1,734,000)
Closing balance as at 30 June		19,878,511	17,755,033	16,024,000
<b>ASSET REVALUATION RESERVE</b>				
Opening balance		14,265	21,623	22,000
Comprehensive income				
Other comprehensive income		-	(7,358)	-
Closing balance as at 30 June		14,265	14,265	22,000
<b>TOTAL EQUITY</b>				
Opening balance		28,215,599	29,170,255	27,863,000
Surplus/(Deficit) for the period		2,123,478	3,460,568	(1,734,000)
Other comprehensive income		-	(7,358)	-
Transactions with owners		108,648	(4,407,866)	274,000
Closing balance as at 30 June		30,447,726	28,215,599	26,403,000

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

**Accounting Policy**Equity Injections

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

Other Distributions to Owners

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

**Budget Variances Commentary****Statement of Changes in Equity**Return of unspent appropriation

Unspent prior year Appropriation Act (No. 1) 2018-19 - DCB of \$165,352 was quarantined under sunset clauses and returned to the Official Public Account on 1 July 2021.

## Cash Flow Statement

for the period ended 30 June 2022

		2022	2021	Original Budget
	Notes	\$	\$	\$
<b>OPERATING ACTIVITIES</b>				
<b>Cash received</b>				
Appropriations		9,283,186	7,485,852	10,867,000
Net GST received		103,356	101,405	-
Other		27,422	35,224	40,000
<b>Total cash received</b>		<b>9,413,964</b>	<b>7,622,481</b>	<b>10,907,000</b>
<b>Cash used</b>				
Employees		6,085,893	5,274,406	7,970,000
Suppliers		2,454,750	2,175,220	2,930,000
Interest payments on lease liabilities		60	149	-
Section 74 receipts transferred to OPA		573,013	204,205	-
<b>Total cash used</b>		<b>9,113,716</b>	<b>7,653,980</b>	<b>10,900,000</b>
<b>Net cash from/(used by) operating activities</b>		<b>300,248</b>	<b>(31,499)</b>	<b>7,000</b>
<b>INVESTING ACTIVITIES</b>				
<b>Cash used</b>				
Purchase of property, plant and equipment		5,376	3,578	274,000
Purchase of intangibles		29,578	60,657	-
<b>Total cash used</b>		<b>34,954</b>	<b>64,235</b>	<b>274,000</b>
<b>Net cash (used by) investing activities</b>		<b>(34,954)</b>	<b>(64,235)</b>	<b>(274,000)</b>
<b>FINANCING ACTIVITIES</b>				
<b>Cash received</b>				
Contributed equity		34,953	109,648	274,000
<b>Total cash received</b>		<b>34,953</b>	<b>109,648</b>	<b>274,000</b>
<b>Cash used</b>				
Principal payments of lease liabilities		6,687	6,622	7,000
<b>Total cash used</b>		<b>6,687</b>	<b>6,622</b>	<b>7,000</b>
<b>Net cash from financing activities</b>		<b>28,266</b>	<b>103,026</b>	<b>267,000</b>
<b>Net increase in cash held</b>		<b>293,560</b>	<b>7,292</b>	<b>-</b>
Cash and cash equivalents at the beginning of the reporting period		228,304	221,012	221,000
<b>Cash and cash equivalents at the end of the reporting period</b>	2.1A	<b>521,864</b>	<b>228,304</b>	<b>221,000</b>

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

### Budget Variances Commentary

#### Cash Flow Statement

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

Standard/ Interpretation	Nature of change in accounting policy, transitional provisions, and adjustment to financial statements
AASB 1060 <i>General Purpose Financial Statements – Simplified Disclosures for For-Profit and Not-for-Profit Tier 2 Entities</i>	AASB 1060 applies to annual reporting periods beginning on or after 1 July 2021 and replaces the reduced disclosure requirements (RDR) framework. The application of AASB 1060 involves some reduction in disclosure compared to the RDR with no impact on the reported financial position, financial performance and cash flows of OIGIS.

### 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 2022.

### 1.1 Expenses

	2022	2021
	\$	\$
<b>1.1A: Employee benefits</b>		
Wages and salaries	4,869,590	4,298,549
Superannuation		
Defined contribution plans	563,152	396,713
Defined benefit plans	339,182	288,236
Leave and other entitlements	881,232	257,615
<b>Total employee benefits</b>	<b>6,653,156</b>	<b>5,241,113</b>

#### Accounting Policy

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

	2022	2021
	\$	\$
<b>1.1B: Suppliers</b>		
<b>Goods and services supplied or rendered</b>		
Audit Fees	35,000	35,000
Consultants	345,480	335,545
Contractors	332,843	99,623
ICT and Communication	675,456	525,556
Insurance	17,632	18,941
Legal	15,329	19,329
Property	667,596	598,497
Recruitment and HR	124,978	144,948
Security Vetting	160,491	56,618
Training	108,339	63,395
Travel	20,979	20,978
Other	77,178	47,602
<b>Total goods and services supplied or rendered</b>	<b>2,581,301</b>	<b>1,966,032</b>
<b>Other suppliers</b>		
Workers compensation expenses	14,880	7,564
<b>Total other suppliers</b>	<b>14,880</b>	<b>7,564</b>
<b>Total suppliers</b>	<b>2,596,181</b>	<b>1,973,596</b>

**1.2 Own-Source Revenue and gains**

	2022	2021
	\$	\$

**Own-Source Revenue****1.2A: Revenue from contracts with customers**

Rendering of services - onsite car staff parking	27,422	35,224
<b>Total revenue from contracts with customers</b>	<b>27,422</b>	<b>35,224</b>

**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.

	2022	2021
	\$	\$

**1.2B: Other revenue**

Resources received free of charge		
Remuneration of auditors	35,000	35,000
Australian Signals Directorate	5,000	5,000
<b>Total other revenue</b>	<b>40,000</b>	<b>40,000</b>

**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.

	2022	2021
	\$	\$

**1.2C: Revenue from Government**

Appropriations		
Departmental appropriations	12,220,000	11,908,000
<b>Total revenue from Government</b>	<b>12,220,000</b>	<b>11,908,000</b>

**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

	2022	2021
	\$	\$
<b>2.1A: Cash and cash equivalents</b>		
Cash on hand or on deposit	521,864	228,304
<b>Total cash and cash equivalents</b>	<b>521,864</b>	<b>228,304</b>

#### 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.

	2022	2021
	\$	\$
<b>2.1B: Trade and other receivables</b>		
<b>Appropriation receivables</b>		
Appropriation receivable	29,736,971	26,153,449
<b>Total appropriation receivables</b>	<b>29,736,971</b>	<b>26,153,449</b>
<b>Other receivables</b>		
GST receivable from the Australian Taxation Office	20,504	15,053
Inter-agency staff leave transfers	258,186	91,272
Other	-	3,045
<b>Total other receivables</b>	<b>278,690</b>	<b>109,370</b>
<b>Total trade and other receivables (gross)</b>	<b>30,015,661</b>	<b>26,262,819</b>
<b>Less impairment loss allowance</b>	<b>-</b>	<b>-</b>
<b>Total trade and other receivables (net)</b>	<b>30,015,661</b>	<b>26,262,819</b>

Credit terms for goods and services were within 30 days (2021: 30 days).

#### Accounting Policy

##### Financial assets

Financial assets are comprised of trade and other receivables that are held for the purpose of collecting the contractual cashflows and are measured at amortised cost.

##### Impairment

OIGIS recognises a loss allowance and impairment expense 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 2021-22 (2020-21: 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
	\$	\$	\$	\$	\$
<b>As at 1 July 2021</b>					
Gross book value	1,852,212	1,290,352	22,390	908,316	4,073,270
Accumulated depreciation, amortisation and impairment	-	-	(13,268)	(256,287)	(269,555)
<b>Total as at 1 July 2021</b>	<b>1,852,212</b>	<b>1,290,352</b>	<b>9,122</b>	<b>652,029</b>	<b>3,803,715</b>
<b>Additions</b>					
Purchase or internally developed	-	5,376	-	29,578	34,954
Revaluations and impairments recognised in net cost of services	-	(2,406)	-	-	(2,406)
Depreciation and amortisation	(370,442)	(222,699)	-	(312,366)	(905,507)
Depreciation on right-of-use assets	-	-	(6,634)	-	(6,634)
<b>Total as at 30 June 2022</b>	<b>1,481,770</b>	<b>1,070,622</b>	<b>2,488</b>	<b>369,240</b>	<b>2,924,121</b>
<b>Total as at 30 June 2022 represented by</b>					
Gross book value	1,852,212	1,292,978	21,837	937,893	4,104,920
Accumulated depreciation, amortisation and impairment	(370,442)	(222,355)	(19,349)	(568,653)	(1,180,799)
<b>Total as at 30 June 2022</b>	<b>1,481,770</b>	<b>1,070,623</b>	<b>2,488</b>	<b>369,240</b>	<b>2,924,121</b>

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

**Revaluations of non-financial assets**

All revaluations were conducted in accordance with the revaluation policy stated at Note 2.2 Non-Financial Assets Accounting Policy. A comprehensive valuation was conducted at 30 June 2021 by an independent valuer, Public Private Property, however was not conducted at 30 June 2022. The carrying amounts at 30 June 2022 do not materially differ from those which would be determined using fair value at the end of the reporting period.

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

As at the reporting date, the OIGIS had no ongoing material 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.

**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**

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

**Revaluations**

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

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

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

All revaluations are independent and are conducted in accordance with the stated revaluation policy. The last Asset Valuation was conducted at 30 June 2021 and included all Leasehold Improvements and Property, plant and equipment assets. The valuation was performed by an independent valuer, Public Private Property.

**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:

	2022	2021
Leasehold improvements	5 years	5 years
Plant and equipment	1 - 25 years	1 - 11 years

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

**Impairment**

All assets were assessed for impairment at 30 June 2022. Where indications of impairment exist, the asset's recoverable amount is estimated and an impairment adjustment is made of the asset's recoverable amount less its carrying amount.

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

**Derecognition**

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

**Intangibles**

OIGIS intangibles comprise internally developed software for internal use. These assets are carried at cost less accumulated amortisation and accumulated impairment losses.

Software is amortised on a straight-line basis over its anticipated useful life. The useful lives of OIGIS software is 3 years (2021: 3 years).

All software assets were assessed for indications of impairment as at 30 June 2022.

**2.3 Payables**

	2022	2021
	\$	\$

**2.3A: Suppliers**

Trade creditors and accruals

494,034 266,086

**Total suppliers**

494,034 266,086

Average days of settlement are 20 days (2021: 20 days).

	2022	2021
	\$	\$

**2.3B: Other payables**

Salaries and wages

202,050 99,843

Superannuation

23,530 15,312

Leave Balance transfers

48,148 84,273

Other

28,883 25,890

**Total other payables**

302,611 225,318

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

## 2.4 Interest Bearing Liabilities

	2022 \$	2021 \$
<b>2.4A: Leases</b>		
Lease liabilities	2,523	9,210
<b>Total leases</b>	<b>2,523</b>	<b>9,210</b>
<b>Maturity analysis - contractual undiscounted cash flows</b>		
Within 1 year	2,523	6,686
Between 1 to 5 years	-	2,524
<b>Total leases</b>	<b>2,523</b>	<b>9,210</b>

Total cash outflow for leases for the year ended 30 June 2022 was \$6,746 (2021: \$6,746)

OIGIS has one motor vehicle lease. The lease liability represents the present value of the remaining lease payments, discounted using the relevant incremental borrowing rate (IBR) that was determined at the commencement of the 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 2022**

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

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

2. Variances between Total Appropriation and Appropriation Applied relate to underspends in Employee benefits and associated expenditure.

These have materialised due to recruitment delays associated with security clearance requirements and the impact of the COVID-19 pandemic on planned activities (which also include Capital Expenditure).

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

**Annual Appropriations for 2021**

	Annual Appropriation \$	Adjustments to appropriation <sup>1</sup> \$	Total appropriation \$	Appropriation applied in 2021 \$	Variance <sup>2</sup> \$
<b>Departmental</b>					
Ordinary annual services	11,908,000	204,205	12,112,205	(7,274,354)	4,837,851
Capital Budget <sup>3</sup>	1,001,000	-	1,001,000	(109,648)	891,352
<b>Total departmental</b>	<b>12,909,000</b>	<b>204,205</b>	<b>13,113,205</b>	<b>(7,384,002)</b>	<b>5,729,203</b>

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

2. Variances between Total Appropriation and Appropriation Applied relate to underspends in Employee benefits and associated expenditure.

These have materialised due to recruitment delays associated with security clearance requirements and the impact of the COVID-19 pandemic on planned activities (which also include Capital Expenditure).

3. Departmental Capital Budgets are appropriated through Appropriation Acts (No.1,3,5). They form part of ordinary annual services, and are not separately identified in the Appropriation Acts.

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

	2022 \$	2021 \$
<b>Departmental</b>		
Appropriation Act (No. 1) 2018-19 - DCB <sup>1</sup>	-	165,352
Appropriation Act (No. 1) 2019-20	-	5,058,338
Appropriation Act (No. 1) 2019-20 - Supply Act <sup>2</sup>	1,117,713	5,333,554
Appropriation Act (No. 1) 2019-20 - DCB <sup>2</sup>	1,413,047	1,448,000
Appropriation Act (No. 1) 2019-20 - DCB - Supply Act <sup>2</sup>	1,035,000	1,035,000
Appropriation Act (No. 1) 2020-21	5,100,446	5,100,446
Appropriation Act (No. 1) 2020-21 - Supply Act	7,011,759	7,011,759
Appropriation Act (No. 1) 2020-21 - DCB	417,000	417,000
Appropriation Act (No. 1) 2020-21 - DCB - Supply Act	584,000	584,000
Appropriation Act (No. 1) 2021-22	12,784,006	-
Appropriation Act (No. 1) 2021-22 - DCB	274,000	-
Cash and cash equivalents	521,864	228,304
<b>Total departmental</b>	<b>30,258,835</b>	<b>26,381,753</b>

1. Appropriation lapsed on 1 July 2021.

2. Appropriation will lapse on 1 July 2022.

### 3.2 Net Cash Appropriation Arrangements

	2022 \$	2021 \$
<b>Total comprehensive income/(loss) - as per the Statement of Comprehensive Income</b>	<b>2,123,478</b>	3,453,210
<b>Plus</b> : depreciation/amortisation of assets funded through appropriations (departmental capital budget funding and/or equity injections) <sup>1</sup>	<b>905,507</b>	1,253,419
<b>Plus</b> : depreciation of right-of-use assets <sup>2</sup>	<b>6,634</b>	6,634
<b>Less</b> : lease principal repayments <sup>2</sup>	<b>(6,687)</b>	(6,622)
<b>Net Cash Operating Surplus/ (Deficit)</b>	<b>3,028,932</b>	4,706,641

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

	2022	2021
	\$	\$

#### 4.1A: Employee provisions

Leave	2,384,806	1,727,923
<b>Total employee provisions</b>	<b>2,384,806</b>	<b>1,727,923</b>

#### 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 2022. The estimate of the present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

#### Superannuation

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

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

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

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



#### 4.2 Key Management Personnel Remuneration

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

	2022	2021
	\$	\$
Short-term employee benefits	1,342,832	1,163,688
Post-employment benefits	171,200	183,496
Other long-term employee benefits	19,583	81,611
<b>Total key management personnel remuneration expenses<sup>1</sup></b>	<b>1,533,615</b>	<b>1,428,795</b>

The total number of key management personnel that are included in the above table are 8 (2021: 6). Substantively, 4 key management personnel positions remain in place during 2022, however there were a number of acting arrangements in place over the course of the year.

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

#### 4.3 Related Party Disclosures

##### **Related party relationships:**

OIGIS is an Australian Government controlled entity. Related parties to OIGIS are Key Management Personnel including their close family members and entities controlled or jointly controlled by either, the Portfolio Minister, and other Australian Government entities.

##### **Transactions with related parties:**

Given the breadth of Government activities, related parties may transact with the government sector in the same capacity as ordinary citizens. These transactions have not been separately disclosed in this note.

Significant transactions with related parties can include:

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

Giving consideration to relationships with related entities, and transactions entered into during the reporting period by OIGIS, it has been determined that there are no related party transactions to be separately disclosed (2021: 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 2022 there were no contingent assets or liabilities (2021: nil).

#### **Unquantifiable Contingencies**

As at 30 June 2022 there were no unquantifiable contingent assets or liabilities (2021: 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

	2022	2021
	\$	\$

**5.2A: Categories of financial instruments****Financial assets at amortised cost**

Cash and cash equivalents	521,864	228,304
Trade and other receivables	258,186	94,317
<b>Total financial assets at amortised cost</b>	<b>780,050</b>	<b>322,621</b>
<b>Total financial assets</b>	<b>780,050</b>	<b>322,621</b>

There were no gains or losses on financial assets at amortised cost (2021: nil).

**Financial Liabilities****Financial liabilities measured at amortised cost**

Suppliers	494,034	266,086
<b>Total financial liabilities measured at amortised cost</b>	<b>494,034</b>	<b>266,086</b>
<b>Total financial liabilities</b>	<b>494,034</b>	<b>266,086</b>

There were no gains or losses on financial liabilities measured at amortised cost (2021: nil).

**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	
	2022 \$	2021 \$
<b>Non-financial assets</b>		
Leasehold Improvements	1,481,770	1,852,212
Property, plant and equipment	1,070,623	1,290,352
<b>Total Non-financial assets</b>	<b>2,552,393</b>	<b>3,142,564</b>

#### 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 last engaged the services of an independent valuer, Public Private Property (PPP) to conduct a review of carrying amounts for leasehold improvements and property, plant and equipment assets as at 30 June 2021. Comprehensive valuations are carried out at least once every 3 years with the last comprehensive valuation occurring at 30 June 2021. An annual assessment is undertaken to determine whether the carrying amount of the assets is materially different from the fair value.

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

## Other information

### 6.1 Current/non-current distinction for assets and liabilities

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

	2022	2021
	\$	\$
<b>Assets expected to be recovered in:</b>		
<b>No more than 12 months</b>		
Cash and cash equivalents	521,864	228,304
Trade and other receivables	30,015,661	26,262,819
Prepayments	169,187	147,272
<b>Total no more than 12 months</b>	<b>30,706,712</b>	<b>26,638,395</b>
<b>More than 12 months</b>		
Leasehold Improvements	1,481,770	1,852,212
Property, plant and equipment	1,070,623	1,290,352
Right-of-use	2,488	9,122
Intangibles	369,240	652,029
Prepayments	868	2,026
<b>Total more than 12 months</b>	<b>2,924,989</b>	<b>3,805,741</b>
<b>Total assets</b>	<b>33,631,701</b>	<b>30,444,136</b>
<b>Liabilities expected to be settled in:</b>		
<b>No more than 12 months</b>		
Suppliers	494,034	266,086
Other payables	302,611	225,318
Leases	2,523	6,686
Employee provisions	1,242,151	714,168
<b>Total no more than 12 months</b>	<b>2,041,320</b>	<b>1,212,258</b>
<b>More than 12 months</b>		
Leases	-	2,524
Employee provisions	1,142,655	1,013,755
<b>Total more than 12 months</b>	<b>1,142,655</b>	<b>1,016,279</b>
<b>Total liabilities</b>	<b>3,183,975</b>	<b>2,228,537</b>

# APPENDIX A: ENTITY RESOURCE STATEMENTS AND RESOURCE FOR OUTCOMES

Figure 5.1: Entity Resource Statement and Resource for Outcomes 2021–22

		Actual available appropriation for 2021–22 \$'000 (a)	Payments made 2021–22 \$'000 (b)	Balance remaining 2021–22 \$'000 (a) – (b)
<b>Ordinary annual services</b>				
<b>Departmental appropriation</b>				
Prior year departmental		26,217	9,025	17,192
Appropriation <sup>1</sup>		12,494	–	12,494
Departmental appropriation <sup>2</sup>		573	–	573
s74 Relevant Agency Receipts				
<b>Total ordinary annual services</b>	<b>A</b>	<b>39,284</b>	<b>9,025</b>	<b>30,259</b>
<b>Other services</b>				
Departmental non-operating		–	–	–
<b>Total other services</b>	<b>B</b>	<b>–</b>	<b>–</b>	<b>–</b>
Special appropriations		–	–	–
<b>Total special appropriations</b>	<b>C</b>	<b>–</b>	<b>–</b>	<b>–</b>
Special accounts		–	–	–
<b>Total special accounts</b>	<b>D</b>	<b>–</b>	<b>–</b>	<b>–</b>
<b>Total net resourcing and payments for agency</b>	<b>A + B + C + D</b>	<b>39,284</b>	<b>9,025</b>	<b>30,259</b>

1. The carried forward unspent prior year Departmental appropriation includes ordinary annual services (Appropriation Act Nos 1, 3 and 5) and retained revenue receipts under s74 of the PGPA Act. The opening balance disclosed has been adjusted for \$165,352 that was quarantined under sunset clauses and returned to the Official Public Account on the 1st July 2021.

2. Departmental appropriation includes ordinary annual services (Appropriation Act Nos 1, 3 and 5) and Departmental Capital Budget appropriations.

**Figure 5.2: Expenses and resources for Outcome 1**

*IGIS has one outcome and one program as disclosed below.*

<b>Outcome 1: Independent assurance for the Prime Minister, senior 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</b>	<b>Budget 2021–22 \$'000 (a)</b>	<b>Actual expenses 2021–22 \$'000 (b)</b>	<b>Variation 2021–22 \$'000 (a) – (b)</b>
<b>Program 1.1: Office of the Inspector-General of Intelligence and Security</b>			
Departmental expenses			
Departmental appropriation <sup>1</sup>	12,213	9,211	3,002
Special appropriations	–	–	–
Special Accounts	–	–	–
<b>Total for Program 1.1</b>	<b>12,213</b>	<b>9,211</b>	<b>3,002</b>
<b>Outcome 1 Totals by appropriation type</b>			
Departmental expenses			
Departmental appropriation <sup>1</sup>	12,213	9,211	3,002
Special appropriations	–	–	–
Special Accounts	–	–	–
Expenses not requiring appropriation in the Budget year <sup>2</sup>	1,781	952	829
<b>Total expenses for Outcome 1</b>	<b>13,994</b>	<b>10,163</b>	<b>3,831</b>
	<b>Budget 2021–22</b>	<b>Actual 2021–22</b>	<b>Variation 2021–22</b>
<b>Average Staffing Level (number)</b>	56	42	14

1. Departmental appropriation combines ordinary annual services (Appropriation Act Nos 1, 3 and 5) and retained revenue receipts under s 74 of the PGPA Act.

2. Expenses not requiring appropriation in the budget year are made up of depreciation expense, amortisation expense and information technology and audit fees provided free of charge.



# **SECTION SIX**

## REVIEW OF INTELLIGENCE AGENCIES

# THE INTELLIGENCE AGENCIES

## Office of National Intelligence



**Australian Government**

### Office of National Intelligence

ONI is responsible for enterprise-level management of the National Intelligence Community (NIC) and ensures a single point of accountability for the NIC to the Prime Minister and National Security Committee of Cabinet. ONI produces all source assessments on international political, strategic and economic developments to Government. ONI uses information collected by other intelligence and government agencies, diplomatic reporting and open sources, including the media, to support its analysis. The functions and powers of ONI are set out in the *Office of National Intelligence Act 2018* (ONI Act). The responsible minister for ONI is the Prime Minister.

### KEY STATISTICS:



**1**

Inspection completed



**1**

Compliance incident reported



**1**

Ministerial letter sent to relevant minister



**2**

Biannual Meetings

## Australian Security Intelligence Organisation



### Australian Government

#### Australian Security Intelligence Organisation

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

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

#### KEY STATISTICS:



**21**

Inspections completed



**30**

Compliance incidents reported



**2**

Ministerial letters sent to relevant minister



**2**

Triannual Meetings

## Australian Secret Intelligence Service



**Australian Government**  
**Australian Secret Intelligence Service**

The primary function of ASIS is to obtain and communicate intelligence not readily available by other means, about the capabilities, intentions and activities of individuals or organisations outside Australia. Further functions set out in the *Intelligence Services Act 2001* (IS Act) include communicating secret intelligence in accordance with government requirements, conducting counter-intelligence activities and liaising with foreign intelligence or security services. Under the IS Act, ASIS's activities are regulated by a series of ministerial directions, ministerial authorisations and Privacy Rules. The responsible minister for ASIS is the Minister for Foreign Affairs.

### KEY STATISTICS:



**14**

Inspections completed



**6**

Compliance incidents reported



**3**

Triannual Meetings



**2**

Ministerial letters sent to relevant minister

## Australian Signals Directorate



**Australian Government**

**Australian Signals Directorate**

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

### KEY STATISTICS:



**11**

Inspections completed



**12**

Compliance incidents reported



**3**

Triannual Meetings



**3**

Ministerial letters sent to relevant minister



**1**

Inquiry completed

## Australian Geospatial-Intelligence Organisation



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

### KEY STATISTICS:



**13**

Inspections completed



**1**

Compliance incident reported



**3**

Ministerial letters sent to relevant minister



**3**

Triannual Meetings

## Defence Intelligence Organisation



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

### KEY STATISTICS:



**3**

Inspections  
completed



**2**

Ministerial letters sent  
to relevant minister



**1**

Biannual Meeting

# AGENCY OVERSIGHT ACTIVITIES 2021–22

## OFFICE OF NATIONAL INTELLIGENCE

The Office's engagement with ONI in 2021–22 was constrained with only one inspection completed and two underway. This is fewer than planned and is attributed to the COVID-19 lockdown in the ACT in second half of 2021 (which required the Office to prioritise inspection resources to higher risk activities in agencies) and to resourcing due to staffing changes in both ONI and the Office. Engagement increased in the first half of 2022.

The first of the planned biannual engagements between the Office and ONI seniors occurred in May 2022, and ONI provided two separate senior level briefings on priority activities in December 2021 and March 2022.

The Office anticipates the increased engagement in early 2022 will continue into 2022–23. Inspections in 2022–23 will look at relevant activities in ONI that were not subject to inspection this year.

The Inspector-General did not commence any inquiries under s 8 of the IGIS Act in relation to ONI.

## INSPECTIONS

### COMPLIANCE WITH ONI PRIVACY RULES

The Office reviewed ONI's compliance with the Rules to Protect the Privacy of Australian Persons as governed by the ONI Act, ONI's Privacy Rules and internal guidelines.

Under s 53 of the ONI Act, the Prime Minister must make rules regulating the collection and communication of identifiable information regarding Australian persons. Under the ONI Privacy Rules, ONI can only collect or communicate this information in specific circumstances where needed to properly perform its functions. Records of instances where ONI has collected or communicated this information are kept by ONI and reviewed annually by IGIS officers. To provide further independent assurance, IGIS officers monitor ONI reporting for references to Australian persons and use this to cross-check provided material.

The inspection identified no legality concerns, and the Office observed good compliance overall with ONI's internal Privacy Rules procedures. However, the Office identified several propriety and administrative findings, and made recommendations to ONI regarding relevant policy updates to remediate these issues:

- 4 instances of non-compliance with ONI's internal guidelines
- delayed approvals to communicate information in reporting
- administrative errors
- some inconsistency with how Privacy Rules forms are used and cleared within ONI.

As of 30 June 2022, ONI were considering the Office's inspection findings and recommendations. The Office will continue to review ONI's compliance with Privacy Rules in 2022–23.



## COMPLIANCE INCIDENTS

ONI reported one compliance incident to the Office. This incident related to an administrative aspect of ONI's assumed identities arrangements, as governed by the Crimes Act, and which constituted a non-compliance with s 15LG(2). More information on this incident is on page 101.

## OTHER REVIEWS

Aside from inspection and compliance investigation activities, the Office also reviews ONI policies and procedures relevant to ONI's compliance with legislation or other directions. In November 2021, ONI provided the Office with copies of its updated policies covering cooperation with approved foreign authorities and prohibition on condoning, encouraging, or assisting torture and other cruel, inhuman or degrading treatment. ONI also provided a copy of the relevant ministerial submission, its internal audit into the foreign authority approval framework, and detail on its internal training and communications to support the implementation of the new policies.

The Office made no findings or recommendations from its review of these policies and procedures.

## AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION

The Office implements a risk-based approach to its inspections of ASIO, given the breadth of ASIO's functions under the ASIO Act. COVID-19 restrictions delayed some inspections, but did not result in a significant impact on the inspection program and engagement activities.

The Office continued to independently review all compliance incident reports relating to non-compliance of legislation or the Minister's Guidelines, or non-compliance with ASIO's internal policies and procedures. ASIO provided all required statutory notifications to the Inspector-General. In one instance, a notification was provided outside the statutory timeframe; more information on this notification is provided on page 87.

Senior level meetings between the Inspector-General, the Office senior leadership team and ASIO senior executives took place during the reporting period to discuss oversight issues. Separately, the Office sought briefings on matters to support its inspection and other oversight activities. These briefings were supplemented by briefings from ASIO on matters it considered appropriate to bring to the Office's attention.

The Inspector-General did not commence any inquiries under s 8 of the IGIS Act in relation to ASIO.

## INSPECTIONS

The Office undertook 21 inspections of ASIO activities in 2021–22.

Of those 21 inspections, the Office did not identify any matters of legality or propriety in the following inspections:

- access to Australian Taxation Office information
- COVID-19 app data (2 inspections)
- visa and citizenship complaints (2 inspections)
- internal security
- adverse and qualified security assessments
- access to and use of AUSTAC information

- investigative cases
- compliance remediation
- computer access under s 25A of the ASIO Act.

In some instances, the Office identified matters relating to ASIO's record keeping, adherence to internal policies and procedures, and procedural issues. The Office also identified issues relating to the currency, clarity and effectiveness of ASIO's internal policies and procedures.

Out of the 21 inspections undertaken, several inspections commenced in 2021–22 remained in progress at the end of the reporting period. This included inspections relating to: ASIO's interaction with minors, human source management, use of powers under the TIA Act, use of a particular technical capability, special intelligence operations and warrants. The Office's findings will be reported in the 2022–23 Annual Report.

In 2 inspections, the Office identified matters of legality or propriety. A high level description of the findings and recommendations are outlined below:

Ministerial submissions: The Office inspected ministerial submissions made to the Attorney-General in support of requests for Ministerial Authorisations (MA) under s 9 of the IS Act. The inspection methodology was designed to revisit issues identified in the Office's previous inspection of ministerial submissions (discussed below). In a small number of cases, the Office raised questions about the completeness and clarity of the information provided to the Attorney-General. The Office noted the importance of the Attorney-General being provided with clear and complete information, including ASIO's objective assessment of that information, to make a properly informed decision. The Office will continue to monitor this issue in future inspections.

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

The Office observed general improvement in ASIO's data governance framework for data deletion. While no systemic issues were identified, the Office identified 5 instances where data reported to have been deleted had not been deleted fully from all systems for various reasons. In 2 instances the Office identified that the data deletion requests were either not submitted, or did not capture all relevant data required, or reported, to have been deleted. The other instances occurred as a result of a typographical error in a deletion request, complexities associated with the volume of data to be deleted and a technical issue, and as a result of the data deletion backlog discussed below.

With regard to data held in one system for multiple warrants, the Office observed that there was a backlog of data yet to be deleted. ASIO advised the Office of the measures it is taking to improve its processes, and the Office will monitor this issue through future inspections. The Office also identified limitations in one database which meant that the date and time that data was collected could not be identified. The Office will discuss with ASIO how its specifications and standards for new systems capture and address all relevant compliance and oversight requirements.

## INSPECTIONS COMMENCED IN 2020–21 AND FINALISED DURING REPORTING PERIOD

In addition to the above inspections, the Office finalised 8 inspections that commenced in the previous reporting period and remained in progress at 30 June 2021.

The Office did not identify any matters of legality or propriety in the following inspections:

- compliance remediation
- human sources
- security assessments
- warrants.

The Office's warrants inspection identified some instances where ASIO's internal policies for reporting to the Attorney-General had been applied inconsistently. The Office will continue to monitor this issue in future inspections.

In 4 inspections, the Office identified matters of legality or propriety. A high level description of the findings and recommendations are outlined below:

Temporary Exclusion Orders: The Office inspected temporary exclusion orders that relied on assessments made by ASIO under s 10(2)(b) of the CT(TEO) Act. The Office identified a number of concerns with the analytical integrity of ASIO's assessments under s 10(2)(b), which it considered lacked the analytical rigor observed in other ASIO assessments. The Office also identified several areas where it considered ASIO's processes for producing these assessments could be improved. ASIO accepted the Office's findings and subsequently briefed the Deputy Inspector-General on changes it would implement to address the Office's concerns. The Office will review the effectiveness of these changes during 2022–23.

Surveillance device warrants: This inspection included ASIO's surveillance operations conducted under a warrant or internal authorisation. The Office observed that warrant documentation was generally of a high standard and that there were rigorous processes for ensuring the legality and propriety of surveillance device operations. The Office identified several areas where there were inconsistencies between operational practices and internal policies and procedures, as well as some record-keeping issues.

For operations approved under internal authorisation, the Office's inspection included matters arising from the compliance incident reported in last year's Annual Report. The Office identified that data obtained from the internally authorised tracking device that was the subject of this compliance incident remained in one of ASIO's systems, despite advice to the Office that all data had been deleted. The Office subsequently verified that this data had been deleted and was satisfied with the revised data deletion processes implemented by ASIO. The Office also observed that the register of internally authorised tracking devices, required under s 26Q of the ASIO Act, did not meet legislative requirements. The Office was satisfied with ASIO's proposed action to update the register to ensure it meets its purpose and is compliant with the ASIO Act.

Special intelligence operation: Special intelligence operation (SIO) powers allow ASIO to seek authorisation from the Attorney-General to undertake activities, in support of its functions, that would otherwise be unlawful. Unlike warrants issued under Division 2 of the ASIO Act, there is no legislative requirement for an SIO to be discontinued if the requirement for special intelligence conduct has ceased.

In its 2019–20 Annual Report, the Office reported that then Inspector-General the Hon Margaret Stone AO FAAL, had advised ASIO that, as a matter of propriety, where ASIO makes a determination that conduct authorised under the SIO has ceased, the authority should be cancelled as soon as practicable. ASIO updated its processes to ensure this expectation was clearly reflected. In 2020–21, the Office observed that delays were still occurring between a decision that authorised conduct under the SIO had ceased or was no longer required and cancellation of the SIO. The Office advised that further changes to ASIO's internal policies and procedures were required to more explicitly capture the requirement that SIO cancellations be progressed as a matter of priority. ASIO agreed and implemented additional changes to its policies and procedures.

Ministerial submissions: The Office inspected submissions to the Attorney-General and the Minister for Home Affairs, particularly focusing on submissions to the Attorney-General relating to support for requests for MAs under s 9 of the IS Act. The Office identified a small number of instances where there were inconsistencies in the use of language between ASIO's internal documents and its submissions to the Attorney-General. The Office considered the use of different definitions for the same terms in different contexts had the potential to be misleading. The Office revisited this issue in its 2021–22 inspection (discussed above).

## OTHER REVIEWS

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

### Special intelligence operations

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

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

### Compulsory questioning

ASIO's compulsory questioning powers, including provisions relating to the Office's oversight of the questioning or apprehension of a person, are contained in Part III Division 3 of the ASIO Act. For each questioning warrant authorised by the Attorney-General, ASIO provided the requisite notifications and information to the Office. The Acting Inspector-General attended questioning sessions conducted during the review period, and did not raise any concerns during the questioning sessions.

### Use of force

Warrants issued under the ASIO Act must explicitly authorise the use of force necessary and reasonable to do the things specified in the warrant. Under s 31A of the ASIO Act, when force is used against a person in the execution of a warrant ASIO must notify the Inspector-General in writing and as soon as practicable. No notifications of use of force were received during the reporting period.

## COMPLIANCE INCIDENTS

The Office independently reviews all compliance incidents that meet the threshold for reporting to the Office.<sup>1</sup> In doing so, the Office may seek additional information or undertake further investigation.

Matters that do not meet the threshold for reporting to the Office are included in ASIO's periodic compliance reports, and a copy of this report is provided to the Inspector-General. ASIO also reports matters to the Office on propriety grounds. In these circumstances, ASIO has assessed that there was no non-compliance with legislation or other non-compliance but considers it would be proper for the Office to be informed of the matter. As with other compliance incidents, the Office reviews the matter and may seek additional information or undertake further investigation.

The Office's review includes consideration of ASIO's remediation action, which frequently entails amendments to ASIO's internal policies and procedures to provide greater clarity for ASIO officers. As an additional assurance measure, the Office conducts periodic inspections to confirm that implementation of proposed remediation action has occurred and to review the effectiveness of this action.

In 2021–22, ASIO reported 30 compliance incidents to the Office. This included notification of 2 incidents that were ultimately confirmed to be compliant.

In addition, ASIO provided notification of 7 incidents that resulted from events outside ASIO control but that ASIO considered it appropriate to report to the Office. This included incidents arising from the actions of another Australian intelligence agency as it exercised the authority conferred by warrants under the TIA Act managed by ASIO.

There were some common themes among the incidents reported to the Office during the reporting period, including:

- **Potential non-compliance with s 175 of the TIA Act or s 3.7 of the Minister's Guidelines – telecommunications data**

During the reporting period, ASIO notified the Office of 11 incidents related to the collection of telecommunications data that it considered to be actual or potential non-compliance with s 175 of the TIA Act or non-compliance with s 3.7 of the Minister's Guidelines. Section 175 of the TIA Act empowers certain ASIO personnel to authorise the collection of historical telecommunications data from telecommunications carriers or carriage service providers in connection with the performance of ASIO's functions. Section 3.7 of the Minister's Guidelines requires ASIO to take all reasonable steps to ensure that personal information used or disclosed by ASIO is relevant, accurate and not misleading. These matters, together with an additional incident reported in June 2021, remained under assessment by ASIO at the end of the reporting period and the Office will review ASIO's findings once received.

<sup>1</sup> ASIO's reporting guidelines require it to notify IGIS of any breaches or potential breaches of legislation or the Minister's Guidelines, and of any non-compliance with policies, procedures or MOUs that involve propriety or human rights concerns.

- **Potential non-compliance with Part IAC of the Crimes Act – assumed identities**

ASIO's creation and use of assumed identities is governed by Part IAC of the Crimes Act and corresponding state and territory laws. During 2021–22, ASIO reported several incidents relating to non-compliance or potential non-compliance with the Crimes Act. These incidents included: assumed identity evidence being obtained without appropriate authorisation, use of the evidence supporting an assumed identity after the assumed identity had been cancelled, approval of the variation of an assumed identity and an assumed identity review where the approver was not authorised to do so, and failure to review an assumed identity within the timeframes stipulated in the Crimes Act. In addition, ASIO reported failures to appropriately record secondary evidence for certain assumed identities, in contravention of its internal policies and potentially in non-compliance with the Criminal Code. ASIO's use of assumed identities generally and the Office's findings in relation to these incidents are discussed on page 100 of this report.

- **Non-compliance with s 2.5 of the Minister's Guidelines – annual review of investigations**

The Minister's Guidelines are issued under s 8A of the ASIO Act and are to be observed by ASIO in the performance of its functions. Section 2.5 requires ASIO to review each of its ongoing investigations on an annual basis. ASIO reported a small number of investigations that were not ceased, and were not reviewed within the 12-month timeframe. The Office was satisfied with the procedures implemented by the relevant teams to reduce the risk of future incidents, and with the action taken by ASIO's compliance directorate to provide guidance to staff across ASIO to mitigate the risk of similar incidents occurring.

The Office also reviewed a number of other legislative non-compliances and propriety matters reported by ASIO. These incidents and the Office's findings, where the matter has been finalised, are outlined below.

Non-compliance with s 94 of the ASIO Act – annual reporting: s 94 of the ASIO Act sets out matters that must be included in ASIO's Annual Report. ASIO notified the Office that it had incorrectly reported 2 matters in the appendices to its 2020–21 Annual Report, resulting in non-compliance with s 94(1)(d) and s 94(2BD) of the ASIO Act. In the first instance, ASIO incorrectly reported the total questioning period under two questioning warrants executed during the reporting period, resulting in the non-compliance with s 94(1)(d). In the second instance, ASIO omitted from the classified appendix to its annual report statistics on the use of internally authorised tracking devices, resulting in the non-compliance with s 94(2BD). The Office was satisfied with ASIO's response once these errors were identified.

Potential non-compliance with s 30 of the ASIO Act – informing Attorney-General that warrant grounds cease to exist: s 30 of the ASIO Act requires the Director-General of Security, in circumstances where the Director-General is satisfied that the grounds on which a warrant issued under Division 2 of the ASIO Act have ceased to exist, to inform the Attorney-General and take steps to ensure action under the warrant is discontinued. ASIO notified the Office of a potential non-compliance with s 30 of the ASIO Act, where it considered that the grounds for a warrant had ceased some time before a decision was made to notify the Attorney-General. Due to the complexity of the circumstances surrounding the incident, it remains under review by ASIO. The Office will consider ASIO's compliance incident report once received.

Potential non-compliance with the Surveillance Devices Act – authorisation for continued use of listening device: ASIO notified the Office of a potential non-compliance with the ASIO Act where collection under a listening device continued for 5 days after the relevant surveillance device authorisation had expired. ASIO immediately ceased collection and requested that data collected during this period be deleted. ASIO obtained legal advice. ASIO considered that there was not a

non-compliance with the ASIO Act or the Surveillance Devices Act. Nonetheless, ASIO undertook to introduce policy and procedural changes, as well as system changes, to reduce the chance of reoccurrence. This matter remains under review by the Office.

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

Potential non-compliance with s 34AAD of the ASIO Act – informing Attorney-General that device access order grounds cease to exist: Under s 34AAD of the ASIO Act, ASIO may obtain an order from the Attorney-General that requires a specified person to provide information and assistance to either access, copy or convert data from a computer or data storage device in the circumstances specified in that section. A person may commit an offence if they fail to comply with an order made under this section. ASIO notified the Office of an incident where an order obtained under s 34AAD to support the execution of a search warrant was not revoked when it should have been. ASIO considered the incident to be a potential non-compliance with s 34AAD. The matter remains under assessment by ASIO and the Office will consider ASIO's compliance incident report once received.

Non-compliance with s 65(2) and s 137(3) of the TIA Act – communication of information: This incident related to the sharing by AGO of intelligence collected under a warrant issued to ASIO, where it did not have the Attorney-General's authorisation to do so. The incident was reported to the Office by both ASIO and AGO, and is discussed in the AGO section of this report.

Non-compliance with the Foreign Acquisitions and Takeovers Act – non-disclosure of protected information: Section 121 of the Foreign Acquisitions and Takeovers Act sets out the circumstances in which 'protected information', as defined by that Act, can be disclosed or otherwise used. ASIO notified the Office of an incident where human error resulted in 2 analytical reports that contained protected information being made available to a broader audience than was authorised. Upon identifying the issue, ASIO implemented immediate remediation action and reported the matter to Treasury, which administers the Foreign Acquisitions and Takeovers Act. The Office was satisfied with ASIO's assessment of the incident, remediation action and reporting.

Non-compliance with the Telecommunications Act – notification of technical access request: ASIO notified the Office that it had failed to provide notification to the Inspector-General within the required timeframe of the issue of a technical access request, as required by s 317HAB(1) of the Telecommunications Act. This matter remains under assessment by ASIO and the Office will review the compliance incident report once received.

Propriety matter – visa application: ASIO notified the Office of a propriety matter relating to its assessment of a visa application. Due to an administrative error, ASIO did not refer the visa assessment case to the correct area for assessment for more than 12 months. By the time the error was identified, the applicant had withdrawn their visa application. While this is concerning, the Office's review identified that due to a known delay affecting these types of applications, it was unlikely the visa would have been granted before the application was withdrawn (even if the administrative error had not occurred). ASIO subsequently reviewed its case load to ensure that no other applications were affected by a similar error. The Office was satisfied with ASIO's response to this incident.

Propriety matter – inadvertent sharing of data files with a partner agency: ASIO notified the Office of a matter relating to the inadvertent sharing of three data files with a partner agency during an authorised transfer of other data files. The receiving agency identified and deleted the files before they were ingested into relevant systems and then advised ASIO. This matter remains under review by the Office.

## FINALISATION OF 2020–21 COMPLIANCE INCIDENTS

Several compliance incidents that had been reported during 2020–21 were also finalised during this reporting year.

This included the following incidents, which were reported in the Office's 2020–21 Annual Report.

Potential non-compliance with s 13 of the TIA Act and s 30 of the ASIO Act: This incident involved two related warrants, one issued under the TIA Act and one issued under the ASIO Act, where the grounds for the warrant had ceased to exist. When reporting this incident to the Office, ASIO initially considered it to be a potential non-compliance with s 13 of the TIA Act and s 30 of the ASIO Act. Section 13 of the TIA Act requires that, where the Director-General is satisfied that the grounds for a warrant have ceased to exist, action under the warrant must be discontinued and notification provided to the Attorney-General. There is a similar requirement in s 30 of the ASIO Act.

Following investigation, ASIO determined that, based on the circumstances of the case, there was no non-compliance with s 13 of the TIA Act. However, ASIO concluded that there was a non-compliance with s 30 of the ASIO Act because action continued under the ASIO Act warrant for 7 days after the Attorney-General was informed that the grounds for the warrant had ceased to exist. The Office agreed with ASIO's conclusion. More generally though, the Office considers that the extent to which any delay in discontinuing action under a warrant and notifying the Attorney-General is justified will depend on the individual circumstances of each case.

Potential non-compliance with s 15(7) of the TIA Act: ASIO notified the Office of potential non-compliance with s 15(7) of the TIA Act, which requires warrants and notifications to be given to an 'authorised representative' of a carrier. This incident was attributed to circumstances where it had become unclear whether ASIO's established contacts could be characterised as 'authorised representatives' of the companies identified in the warrant. ASIO sought legal advice on this matter. ASIO considered that the requirements of s 15(7) had been met and therefore there was no legislative non-compliance. The Office agreed with this assessment.

Potential non-compliance with s 25A(4)(ba) and s 18 of the ASIO Act: This incident arose as a result of human error when ASIO's technical systems were configured to receive computer access intercept information under a particular warrant. The configuration error meant that information collected in relation to a telephone service was incorrectly stored in ASIO's data holdings and subsequently forwarded to ASD. Following its investigation, ASIO concluded that the matter was a non-compliance with s 63 of the TIA Act, rather than s 25A(4)(ba), because the error occurred during storage and communication of the intercepted information, rather than during its interception. The Office agreed with ASIO's assessment that it was a non-compliance with s 63(1)(a) of the TIA Act, and verified that the relevant data was deleted by both agencies.

Non-compliance with s 34DP(1) of the ASIO Act: Following questioning conducted pursuant to a questioning warrant, ASIO notified the Office of a potential non-compliance with the ASIO Act concerning the video recording of proceedings. Section 34DP(1) requires the Director-General to ensure that video recordings are made of the appearance of the subject of a questioning warrant for questioning. Due to a technical issue, a small portion of the proceedings was not recorded. In addition, separate technical issues meant that a contingency copy of the recording was not made.



In assessing this incident, ASIO also considered whether it constituted a non-compliance with s 14 of the Statement of Procedures made under s 34AF of the ASIO Act, which imposes additional requirements for the prescribed authority to be notified if the video recording facilities fail to record as intended. Due to the specific circumstances of the incident, ASIO concluded that it was a non-compliance with s 34DP(1), but not of s 14 of the Statement of Procedures. The Office concurred with ASIO's assessment and the measures ASIO intended to implement to prevent a similar reoccurrence in any future questioning sessions.

Non-compliance with s 15KI(4)(a) of the Crimes Act: In May 2021, ASIO identified an incident relating to a request for evidence of 3 assumed identities sent to an issuing agency in February 2020. The request did not include the date that the assumed identity authority was granted, in non-compliance with s 15KI(4)(a) of the Crimes Act. ASIO reviewed and updated its templates in response to the incident and conducted a review to ensure that other similar letters fulfilled the legislative requirements. The Office was satisfied with ASIO's response to this incident.

## AUSTRALIAN SECRET INTELLIGENCE SERVICE

The Office's engagement with ASIS in 2021–22 was partially constrained by the COVID-19 restrictions in the ACT in the second half of 2021, but this did not significantly affect the inspection or engagement program.

The Inspector-General, and the Office senior leadership team met with Director-General ASIS and senior ASIS executives at regular points through the year, and the Office inspection team attended ASIS premises for review activities and briefings to increase knowledge of ASIS activities and operations.

The Inspector-General did not commence any inquiries under s 8 of the IGIS Act in relation to ASIS.

## INSPECTIONS

The Office completed 14 inspections of ASIS activities in 2021–22.

Of the 14 inspections, the Office did not identify any matters of legality or propriety in the following 11 inspections:

- operational files from 2 particular locations
- operational files for a particular priority thematic issue
- use of bulk data holdings
- access to and use of AUSTRAC information
- internal security investigations, particularly where there may be an impact on an individual's clearance
- ministerial submissions (4 inspections)
- use of weapons and weapons training.

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

Liaison with foreign services: One of ASIS's functions under s 6(1)(d) of the IS Act is to liaise with intelligence or security services of other countries. The Office conducted an inspection of operational files relating to ASIS's human rights assessments (HRA) of these foreign services, which was finalised in July 2021.

Overall, the Office found that ASIS consistently managed any individual human rights issues or concerns that arose over the year, in its regular activities and liaison relationships.

However, the Office identified non-compliance with ASIS's internal policy concerning the management of HRAs, specifically regarding assessments and annual reviews that were not completed or not reviewed within the specified timeframe. ASIS kept the Office informed of progress in updating its procedures in response to the inspection findings, and has finalised updates to the relevant policy. The next inspection of HRAs will review ASIS's ongoing compliance.

Operational file reviews at particular locations: Between August and September 2021 the Office conducted an operational file inspection focused on ASIS activities at a particular overseas location. The Office identified 4 instances of non-application of the ASIS Privacy Rules and a significant number of missing records. The ASIS Privacy Rules are issued by the Foreign Minister and regulate ASIS's communication and retention of intelligence information about Australian persons. The IS Act prohibits ASIS from communicating intelligence information about an Australian person other than in accordance with those rules. In this case, ASIS conducted its own investigation of the missing records and undertook appropriate action to remind staff of record-keeping obligations. The Office agreed with the action taken.

In addition, the Office identified a case concerning an Australian person in which it was not clear if ASIS had a specific interest in producing intelligence on the person. In order to produce intelligence on an Australian person, the IS Act requires that ASIS obtain the Minister's approval via a ministerial authorisation (MA). The Office discussed the case with ASIS, and is satisfied that ASIS did not have a specific interest in the person however, ASIS advised it will improve its practices and record keeping to ensure its intelligence interest is documented, and provide updated internal guidance and training to staff.

In a separate inspection for a different location, the Office identified one instance of non-compliance with s 8 of the IS Act, where intelligence assets were tasked to produce intelligence on an Australian person without an MA in place. This incident was due to a misunderstanding between officers regarding the requirement for an MA. The Office notes that ASIS was given the approval to produce intelligence shortly after this.

The inspection also found two instances (the first was identified by the Office, and second by ASIS during the inspection) where the ASIS Privacy Rules should have been applied to the communication of information concerning Australian persons. This non-application of the ASIS Privacy Rules was noted in the inspection findings to ASIS. The Office is satisfied that ASIS understands the legislative requirements and notes that ASIS has committed to developing procedures to mitigate similar errors in the future.

Inspections underway: As of 30 June 2022, the Office had commenced 4 inspections of ASIS activities or programs in 2021–22 that were not finalised. The outcomes of these inspections will be reported in the next Annual Report. These inspections include:

- management and use of ASIS assumed identities
- review of files relating to arrangements pursuant to s 13B of the IS Act
- operational files from 2 additional priority thematic areas (2 inspections).

## COMPLIANCE INCIDENTS

The Office independently reviews all compliance incidents that ASIS reports. In doing so, the Office may seek additional information or undertake further investigation. The Office's review includes consideration of ASIS's remediation action, and any relevant internal legal advice and may include providing further suggestions to remediate the incident or mitigate further occurrence.

In 2021–22 ASIS reported 6 compliance incidents to the Office. The Office reviewed each reported incident and where appropriate worked with ASIS to identify the cause. In some instances the Office provided recommendations for remediation to minimise recurrence.

A specific incident worth highlighting relates to ASIS activities around an Australian person without an MA. This incident constituted a legislative non-compliance that was identified by the Office initially via a ministerial submission inspection in 2020–21 and subsequently reported to the Office by ASIS.

In this case, ASIS had been issued an MA on an Australian person that expired. A new authorisation for the same Australian person was not signed by the Minister until over 1 month later due to an administrative oversight within ASIS. In the period between authorisations, ASIS conducted activities in breach of the Minister's direction under s 8 of the IS Act.

The Office engaged with ASIS to understand the operational challenges that led to this non-compliance, and provided recommendations to highlight and enhance the importance of clear and timely processes to prevent such breaches. ASIS has since refined its practices to ensure more timely action for renewals and reporting as per the legislative requirements.

Themes, findings and recommendations across the remaining incidents include:

Non-application of the ASIS Privacy Rules: In these cases, ASIS did not apply their Privacy Rules before communicating information concerning Australian persons. These communications were in contravention of s 15 of the IS Act. In some instances, ASIS Privacy Rules were applied after the fact, and ASIS undertook to reinforce the requirements through regular training.

Non-recording of the application of the ASIS Privacy Rules: In these cases, ASIS did not record its application of the ASIS Privacy Rules, in contravention of ASIS internal policy. ASIS recorded the application after the communication, and the Office reiterated the importance of contemporaneous records.

Non-compliance with s 10A(2) of the IS Act: This instance of non-compliance with s 10A(2) occurred as ASIS did not provide a report to the Minister within 3 months from when the MA ceased to have effect. The report was delivered to the Minister 1 week past the deadline, and ASIS undertook to internally communicate to staff the importance of administrative processes and tracking reporting deadlines.

Non-compliance with s 15KP of the Crimes Act: This is an ongoing review as at 30 June 2022. The Office agrees with ASIS's assessment that this case represents a non-compliance with s 15KP of the Crimes Act. More information on this incident is on page 101.

## AUSTRALIAN SIGNALS DIRECTORATE

COVID-19 restrictions partially constrained some activities with ASD, but did not significantly impact the Office's inspection program. The Office's inspections were supplemented by briefings on various matters from ASD, with a particular focus on the development of technical capabilities used by ASD.

The Inspector-General met with ASD's Director-General and senior ASD executives several times throughout the reporting period. During these meetings, ASD provided briefs on emerging challenges – including the recent investment that will significantly increase ASD's capabilities through Project REDSPICE (Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers). While the REDSPICE investment is not proposed to add new, or expand existing, ASD functions or authorities, it will increase the scale and geographic dispersal of ASD's existing functions and capabilities – for that reason, and to enable the Office to begin preparing for ASD's future expansion in this area, the Office's inspection program for 2022–23 will have a stronger focus on targeted inspections across the breadth and scale of ASD's activities, including cyber-focused inspection activities.

### INQUIRIES

On 7 May 2021 the Inspector-General commenced an inquiry into a complaint relating to ASD pursuant to subs 8(2) of the IGIS Act. The complaint was originally made to the Inspector-General as a Public Interest Disclosure. The complainant alleged that a security breach for which senior ASD staff had been responsible led to the suspension of the complainant's security clearance with consequences for their future employment.

The Inspector-General conducted a series of interviews to supplement the written evidence considered as part of the investigation. Some interviewees attended the IGIS office for follow-up interviews. ASD cooperated fully with the Inspector-General's requests for information.

The inquiry found that, based on the evidence obtained and reviewed, the allegations made by the complainant were not made out.

The inquiry made two observations relating to administrative procedures for consideration by ASD. ASD undertook to develop a policy to embed the practices recommended by the Inspector-General by July 2022. The Inspector-General was provided a copy of the ASD policy on 12 July 2022.

### PRELIMINARY INQUIRIES

In May 2022, the Inspector-General decided to commence a preliminary inquiry into a particular MA issued to ASD and activities approved under that authorisation. The preliminary inquiry is examining:

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

The preliminary inquiry is also examining whether the Minister for Defence was properly advised of the relevant legal and operational risks associated with the authorisation, the novelty of the proposed activities and reliance on the functions cited in the authorisation, and whether the Minister was adequately advised of any residual legal risk posed by the proposed activities.

This preliminary inquiry remained underway at the end of the reporting period. A report will be prepared at the conclusion of the inquiry, and findings summarised in the 2022–23 Annual Report.

## INSPECTIONS

The Office completed 11 inspections of ASD activities in 2021–22.

Of the 11 inspections, the Office did not identify any matters of legality or propriety in 10 inspections covering the following topics:

- MAs (including specific reviews of authorisations to undertake certain activities)
- application of the ASD Privacy Rules made under the IS Act
- interception under Part 21 of the TIA Act
- interception under Part 22 of the TIA Act.

In one inspection of joint ASD and AGO activities, the Office identified concerns relating to the content and completeness of MAs and covering submissions sought jointly by AGO and ASD to conduct activities in support of a military operation.

While the Office identified no matters of legality or propriety in respect of the operational activities, there were several issues which arose in relation to the sufficiency of the submissions to the Minister for Defence in support of the requests for the MAs. Under s 25A of the IGIS Act, the Inspector-General issued two reports covering the findings and recommendations from the inspection. The first report was submitted to the Minister for Defence and ASD and AGO on 3 March 2022, and dealt with the Inspector-General's views about the legal construction of a section of the IS Act. The second report was submitted to the agencies on 26 April 2022, and dealt with the sufficiency of the submissions made to the Minister to provide a sound legal and factual framework to inform the Minister in his decision under s 9 of the IS Act.

Following the recommendations made by the Inspector-General, ASD and AGO undertook to review how their MA and submissions could be amended to enhance the advice provided to the Minister to ensure they are appropriately informed, pursuant to the requirements of the IS Act. ASD and AGO also jointly sought legal advice about a separate issue raised by the Inspector-General.

## COMPLIANCE INCIDENTS

ASD reported 12 compliance incidents to the Office in 2021–22. The Office independently reviews all compliance incidents that meet the threshold for reporting by agencies, and in doing so, the Office may seek additional information or undertake further investigation. Given the technical complexity of ASD's capabilities, some compliance incidents can involve lengthy review processes – particularly where independent legal advice is required. ASD also provided the Office with an additional 4 early notifications of possible compliance incidents, and these matters remain with ASD while it finalises its initial investigation.

Of the 12 compliance incidents reported to the Office in 2021–22:

- 3 compliance incidents remain under review by the Office
- 4 compliance incidents were confirmed by the Office as legislative non-compliance, and are discussed further below
- 3 compliance incidents were found to be non-compliant with ASD's policies and procedures
- 2 incidents were ultimately determined to be compliant, as they were not non-compliant with legislation or ASD's policies and procedures.

The Office observed some common themes among the incidents reported to our Office during the reporting period, including:

- ASD's operating environment is complex and challenging. The Office's inspections staff often require supplementary information or technical briefings from ASD while investigating compliance incidents to ensure the Office fully understands the circumstances surrounding the incident to ensure the Office can form an independent view.
- To achieve its purpose, ASD must keep pace with rapidly evolving technologies which includes the development and application of cutting-edge capabilities. While ASD has robust governance frameworks to implement and manage its capabilities, inadvertent technical errors and system design issues can result in unanticipated outcomes.
- The technical complexity surrounding many of ASD's compliance incidents may result in requests for additional legal advice by either ASD or the Inspector-General, which can substantially lengthen the overall time taken to finalise the investigation of an incident.
- In addition to these non-compliances, ASD will, at times, advise the Office of 'potential breaches' where it is technically possible that there was a non-compliance but it cannot be proven – usually due to data limitations or the absence of essential details.

Non-compliance with s 7(1)(c) of the TIA Act – July 2021 and March 2022: In July 2021 and March 2022, ASD confirmed it was non-compliant with ss 7(1)(c) of the TIA Act following incidents where a combination of system design issues and human error enabled ASD to potentially intercept communications passing over a telecommunications system. Depending on the circumstances, ASD may be considered to have enabled interception where it has done the things necessary to intercept particular communications, but no interception of such communications has been identified. The Office independently investigated the circumstances of these incidents and found that ASD's response and the remedial actions taken, including updating processes for obtaining communications, were appropriate in the circumstances.

Two non-compliances with s 63 of the TIA Act: In January 2022, ASD confirmed that it was non-compliant with s 63(1)(a) of the TIA Act by making a record of unlawfully intercepted information which had been provided to ASD by a partner agency that, at the time, believed the information had been lawfully obtained. While conducting an independent review of this matter, the Office identified a possible additional non-compliance with s 63(1)(a) of the TIA Act, and asked ASD to investigate the underlying circumstances further. ASD confirmed this as a separate legislative non-compliance issue in August 2021, and provided the Office with a finalised report in April 2022. In this matter, ASD received and stored a record of data that it was not legislatively authorised to receive, following a configuration error by a partner agency.

The Office's independent review of both incidents found that ASD could not have reasonably foreseen or prevented either incident from occurring. In investigating these matters, the Office concluded ASD has robust technical safeguards and governance measures in place to minimise the risk of such incidents occurring where possible.

Compliance with ASD Privacy Rules: The Minister for Defence issues written rules (the ASD Privacy Rules) to regulate ASD's communication and retention of intelligence information about Australian persons. Among other things, the ASD Privacy Rules require ASD to provide the Office with access to all of ASD's intelligence holdings concerning Australian persons and report to the Office any non-compliance with the ASD Privacy Rules.

ASD must report to the Office when ASD has revised its determination that a person previously presumed to be foreign is an Australian person – which is known as 'overturning a presumption of nationality' – and usually occurs when ASD obtains further information on an individual. If the initial

presumption was reasonable, such incidents do not represent a non-compliance with legislation or the ASD Privacy Rules.

During the 2021–22 period, ASD provided the Office with 24 such reports. 19 of these reports were independently reviewed by the Office and in each of these cases, the Office assessed that the initial presumption was reasonable, and ASD took appropriate measures to protect the privacy of Australian persons. The review of 5 reports remains underway at the end of the reporting period.

## COMPLIANCE INCIDENTS RECEIVED IN EARLIER REPORTING PERIODS

The Office finalised its independent review of an additional 3 compliance incidents which ASD provided to our Office in earlier reporting periods – these outcomes are discussed below. A further 3 compliance incidents from previous reporting periods remain under investigation at the end of this reporting period due to their complexity, and will be reported once finalised.

Two incidents regarding ASD's Privacy Rules: In its 2020–21 Annual Report, the Office reported it had commenced an indepth review of two overturned presumption of nationality reports provided by ASD. These cases were selected as it appeared that ASD may have conducted activities on Australian persons without appropriate MAs in place. Following an extensive review of the circumstances of both cases, the Office has determined neither matter constituted a non-compliance with the IS Act nor ASD's Privacy Rules. During the Office's review, it was noted that ASD had acted inconsistently with its own policies and procedures in its handling of both cases. ASD has subsequently applied appropriate remediation measures.

Incident regarding the IS Act: In the 2020–21 reporting period, ASD proactively notified the Office of an incident involving a possible non-compliance with the IS Act. As detailed in last year's Annual Report, in seeking any MA for its activities, ASD must ensure there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the authorisation beyond what is necessary for the proper performance of ASD's functions. In early 2021, ASD advised the Office that because of human error, arrangements that ASD had advised the Minister were in place had not been consistently applied while ASD was conducting activities pursuant to the authorisation. The Office's independent review of the matter found that while this was the case, the circumstances were such that it remained compliant with the IS Act and the authorisation was valid. In finalising its review, the Office confirmed that ASD had issued a written report of the incident to the Minister, and ASD's Compliance and Oversight team had made appropriate recommendations to prevent similar incidents from reoccurring.

## AUSTRALIAN GEOSPATIAL-INTELLIGENCE ORGANISATION

The Office's engagement with AGO in 2021–22 was partially constrained by the COVID-19 lockdown in the ACT. Regular senior level meetings between the Inspector-General and Director AGO proceeded as planned, and AGO's detailed briefs on emerging issues throughout the year provided the Office with a more detailed understanding of AGO's functions which informed inspection activities.

Given the breadth of AGO's functions, the Office's inspection program is continuous and includes quarterly scheduled inspection activities and proactive reviews of areas of higher risk or sensitivity, as well as reviews of reported compliance incidents.

The Inspector-General did not commence any inquiries under s 8 of the IGIS Act in relation to AGO.

## INSPECTIONS

The Office completed 13 inspections of AGO activities in 2021–22.

Of the 13 inspections, the Office did not identify any matters of legality or propriety in the following 12 inspections:

- ministerial authorisations to undertake certain activities
- ministerial submissions
- application of the AGO Privacy Rules made under the IS Act
- Director's Approvals and Post Activity Reporting
- AGO's support to Defence advice to the Foreign Investment Review Board
- provision of geospatial products to partners.

In one inspection of joint ASD and AGO activities, the Office identified concerns relating to the content and completeness of MAs and covering submissions sought jointly by AGO and ASD to conduct activities in support of a military operation.

While the Office identified no matters of legality or propriety in respect of the operational activities, there were several issues which arose in relation to the sufficiency of the submissions to the Minister for Defence in support of the requests for the MAs. Under s 25A of the IGIS Act, the Inspector-General issued two reports covering the findings and recommendations from the inspection. The first report was submitted to the Minister for Defence and ASD and AGO on 3 March 2022, and dealt with the Inspector-General's views about the legal construction of a section of the IS Act. The second report was submitted to the agencies on 26 April 2022, and dealt with the sufficiency of the submissions made to the Minister to provide a sound legal and factual framework to inform the Minister in his decision under s 9 of the IS Act.

Following the recommendations made by the Inspector-General ASD and AGO undertook to review how their MA and submissions could be amended to enhance the advice provided to the Minister to ensure they are appropriately informed, pursuant to the requirements of the IS Act. ASD and AGO also jointly sought legal advice about a separate issue raised by the Inspector-General.

## COMPLIANCE INCIDENTS

Non-compliance with ss 65(2) and 137(3) of the TIA Act: AGO notified the Office of a non-compliance with ss 65(2) and 137(3) of the TIA Act. The incident related to AGO's use and communication of foreign intelligence information without required approvals from the Attorney-General.

In this case, AGO staff embedded in ASIO were provided lawfully collected foreign intelligence information to enable them to produce intelligence product based on that information. These embedded AGO staff were authorised, pursuant to s 12 of the TIA Act, to exercise the power conferred by a warrant. While the AGO staff were authorised to pass the information to their parent agency they were not authorised to pass intelligence product derived from the information back to ASIO. To do this lawfully a further authorisation from the Attorney-General was required. Upon discovery of this deficiency AGO took appropriate steps to cease production activity, recall product and quarantine access to the information. Appropriate legal advice was obtained and approval was provided by the Attorney-General on 17 December 2021 for AGO to communicate intelligence product generated from the foreign intelligence information from AGO to other NIC agencies.

The Office noted the close cooperation between AGO and ASIO in resolving the issue and implementing process and training measures to mitigate the risk of a recurrence. The Office reviewed documentation relevant, actions taken at the time and remedial steps implemented following the incident and concurred with AGO and ASIO's findings.



Compliance with AGO Privacy Rules: As part of AGO's routine reporting to the Office, AGO noted one instance of non-compliance in the application of the AGO Privacy Rules to a product which was related to AGO's support for an Australian Defence Force training exercise. The Office's independent review of the matter found that AGO's response and the remedial actions taken were prompt and appropriate to the circumstances.

## OTHER REVIEWS

Over the 2021–22 inspection period, AGO's Compliance area continued to engage with the Office regarding any instances where intelligence or privacy matters concerning Australian persons were considered with regard to the Australian Hydrographic Office's (AHO) (a component of AGO) products.

The Office was unable to conduct planned outreach and inspection activities at AHO's Wollongong site due to COVID-19 restrictions and will seek to undertake this activity in the next inspection year.

## DEFENCE INTELLIGENCE ORGANISATION

Disruptions caused by COVID-19 lockdowns in the ACT, and other factors, has partially constrained engagement and inspection activities with DIO in 2021–22. However, engagement with DIO increased in the first half of 2022.

The Office anticipates that our engagement will continue to grow into 2022–23, and will involve periodic inspection activity and frequent meetings between the Inspector-General and the Chief of Defence Intelligence.

The Inspector-General did not commence any inquiries under s 8 of the IGIS Act in relation to DIO.

## INSPECTIONS

The Office undertook 4 inspections of DIO's activities in 2021–22.

Of the 4 inspections, the Office did not identify any matters of legality or propriety in the following 2 inspections:

- compliance with the DIO Privacy Rules
- ministerial submissions.

DIO specified program: The Office inspected a program of specified activities, which is established and governed by a Five-Eyes Memorandum of Understanding. The Office identified some propriety and procedural concerns arising from the early stage of maturity of the capability. In addition, some record-keeping issues were identified by the Office. These findings were delivered to DIO in March 2022, and DIO confirmed it had remedial measures underway which were likely to address the Office's concerns. The Office will undertake further inspection of the program in the 2022–23 reporting period, to continue to monitor measures being implemented by DIO.

Inspections underway: As at 30 June 2022, the Office had commenced one inspection of DIO's processes and practices relating to maintaining its analytic integrity which has not been finalised. The outcomes of this inspection will be reported in the next Annual Report.

## OTHER REVIEWS

In addition to inspection activities, the Office also reviews DIO policies and procedures relevant to DIO's compliance with legislation or other directions. In 2021–22, DIO provided the Office with copies of its newly established analytic standards, and its updated mandatory training policy which ensures DIO's workforce compliance with their mandated and legislated requirements. The Office identified no findings or recommendations from our independent review of these policies.

## ACIC AND AFP

During 2021–22, IGIS's jurisdiction was expanded with enactment of the *Surveillance Legislation Amendment (Identify and Disrupt) Act*. The Act provides new enforcement powers for the ACIC and AFP to combat serious online crime. One of these new powers is a network activity warrant (NAW), which allows the ACIC and AFP to collect intelligence on criminal networks operating online. IGIS has oversight responsibility for this warrant power.

As reported in its 2020–21 Annual Report, the Office reported initiatives to ensure its capability and readiness for its expanded oversight role. This included establishing relationships with key contacts and senior managers in the ACIC and AFP. The Office's established engagement with both agencies enabled inspections to proceed efficiently and effectively.

## ACIC INSPECTIONS

The Office inspected the ACIC's first use of a NAW. The Office's inspection focused on the policies and procedures put in place by the agency for this warrant, the appropriate segregation of information obtained under a NAW from any evidentiary processes and ensuring that the ACIC's delegations related to NAWs are appropriate and up-to-date. The Office did not identify any matters of legality or propriety.

## AFP INSPECTIONS

The Office inspected the AFP's first use of a NAW. As with the inspection of the ACIC, the Office focused on the policies and procedures put in place by the agency for this warrant, the appropriate segregation of information obtained under a NAW from any evidentiary processes and ensuring that the AFP's delegations related to NAWs are appropriate and up-to-date. The Office did not identify any matters of legality or propriety, but made some suggestions to improve AFP processes.

## CROSS-AGENCY INSPECTION ACTIVITIES

During 2021–22 the Office undertook three cross-agency inspection activities where it inspected agency activities related to:

- compliance with Part VIIIA of the Privacy Act in relation to handling of incidentally collected COVID-19 app data
- compliance with the AMLCTF Act in relation to access to, and management of, financial intelligence information created or held by Australian Transaction Reports and Analysis Centre (AUSTRAC)
- compliance with the Crimes Act and corresponding state and territory laws in the use and management of assumed identities.

## COVID-19 APP DATA

In November 2021 and May 2022 the Office undertook an inspection of the agencies to confirm they were compliant with Part VIIIA of the Privacy Act in relation to handling of incidentally collected COVID-19 app data. At the completion of these inspections a report was provided to the Office of the Australian Information Commissioner and Privacy Commissioner. In both of those inspections the Office found:

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

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

## ACCESS TO AND MANAGEMENT OF AUSTRAC INFORMATION

The AMLCTF Act provides a legal framework for designated agencies to access and share financial intelligence information created or held by AUSTRAC.

Under a memorandum of understanding with AUSTRAC, the Office had a role in monitoring agencies' access to and use of AUSTRAC information.

The Office verified that there is a demonstrated intelligence purpose pertinent to the functions of the agency, that access is appropriately limited, searches are focused, and information passed to both Australian agencies and foreign intelligence counterparts is correctly authorised.

In May 2022 the Chief Executive Officer of AUSTRAC and the Inspector-General agreed that the role the Office has played in monitoring was no longer required. This is due to changes in technology for accessing AUSTRAC information, which provided a greater ability for AUSTRAC to audit access and use itself and provide agencies the ability to self-audit and manage access to and use of AUSTRAC information. As such, the memorandum of understanding was terminated by mutual agreement.

Prior to termination, the Office commenced an inspection at ONI and completed inspections of access to, and use of, AUSTRAC information in ASIO and ASIS. The Office identified:

- ASIO: Suggestions relating to improving the documentation of reasons to support approvals for access to AUSTRAC information and the need for appropriate recordkeeping of agreements covering the dissemination of AUSTRAC material to a foreign partner to ensure compliance with s127(1) of the AMLCTF Act.
- ASIS: No issues of legality, propriety or non-compliance with provisions of the AUSTRAC–ASIS memorandum of understanding were identified.

## USE AND MANAGEMENT OF ASSUMED IDENTITIES

Part IAC of the Crimes Act and corresponding State and Territory laws enable ASIO, ASIS and ONI officers, and from 1 April 2022, ASD officers, to create and use assumed identities for the purpose of performing their functions. The legislation protects authorised officers from civil and criminal liability where they use an assumed identity in circumstances that would otherwise be considered unlawful. Similarly, the legislation protects the Commonwealth, State and Territory agencies responsible for issuing identity documents in relation to an assumed identity in accordance with the Act.

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

The Office conducted inspections of the reporting provided by ASIS, ONI and ASIO and also received compliance incident reporting from all three agencies in 2021–22.

## ASIO

ASIO has addressed the non-compliance with the Crimes Act identified in the Office's 2020–21 Annual Report regarding timeliness of periodic reviews of assumed identities.

However, in 2021–22 ASIO notified the Office of 5 incidents relating to assumed identities.

The first incident concerned evidence of an assumed identity being obtained without appropriate authorisation to do so, as a result of an error in the original approval provided in June 2018. ASIO's initial review of this incident concluded that there was no non-compliance with the Crimes Act. However, following the Office's review, ASIO agreed that a non-compliance with s15KX of the Crimes Act had likely occurred, but did not raise issues of criminal liability under s 15LB. This incident occurred at a time when ASIO relied on manual processes for the approval and management of assumed identities. The Office agreed that the more recent establishment of an automated system means that this type of error was less likely to occur in future.

The second incident involved the continued use of mobile phone service registered using an assumed identity after the assumed identity had been cancelled. ASIO initially reported the incident to the Office as a potential non-compliance with the Crimes Act, however following legal advice, ASIO concluded that no legislative non-compliance had occurred. ASIO considered instead that the incident was non-compliant with ASIO's internal procedures, and the Office agreed with ASIO's assessment.

The third incident involved 2 instances where approvals were provided in circumstances where the approving officer did not have the authorisation to do so. Both cases related to circumstances where the IT system for managing assumed identities had not been updated following staffing changes, which allowed the approvals to proceed. This matter was reported as a potential non-compliance with the Crimes Act and remains under assessment by ASIO. The Office will review the compliance incident report once received.

Section 15KF of the Crimes Act requires that assumed identities granted by the chief officer of an intelligence agency are to be reviewed at least once every 3 years. In the fourth incident, an assumed identity had not been reviewed since its creation in 2013. This incident is another historic matter and is attributed to a data entry error that resulted in the record not being transferred when IT systems were upgraded. ASIO concluded that it was a non-compliance with s 15KF of the Crimes Act and non-compliant with ASIO's internal procedures. The Office agreed with ASIO's assessment.

ASIO's internal policies require, for the purpose of compliance with the Criminal Code, that personas used for certain ASIO operations are listed as 'secondary evidence' against the relevant assumed identity. The fifth incident was reported by ASIO after the relevant area identified multiple instances of non-compliance with this requirement. ASIO's assessment of this matter, and consideration of its legal position on this requirement, is ongoing. The Office will review the compliance incident report once received.

## ASIS

In its annual reporting, ASIS identified issues including overdue reviews and the potential risk of assumed identities being used for purposes other than the authorised purpose.

In addition, ASIS reported a non-compliance with s 15KP of the Crimes Act. In this incident, ASIS inadvertently used an assumed identity for a purpose that was consistent with its functions, but other than the authorised purpose. ASIS ceased using the assumed identity, and commenced cancellation. ASIS undertook to expand the scope of its audit processes to incorporate review of the actual use of an assumed identity. The Office is nearing finalisation of an investigation and recommendations to ASIS and this will be included in next year's annual report.

The Office began a more in-depth inspection of the use of assumed identities in ASIS, which will confirm issues reported and make recommendations on how to address them. This inspection is approaching completion as at 30 June 2022, and the outcomes will be reported in next year's annual report.

## ONI

ONI reported to the Office a non-compliance incident regarding s 15LG(2).

ONI is required to conduct an audit of its assumed identities records every 6 months. Additionally, the Director-General must submit a report to the Office as soon as practicable after the end of each reporting period providing an overview of the assumed identities activities. Although ONI completed its audit and report to the Office within the statutory timeframes set out in the Crimes Act, the auditor was not formally appointed until after the statutory timeframe due to an administrative oversight. ONI subsequently appointed a person under s 15LG(2) of the Crimes Act and has updated its procedures to minimise the risk of recurrence of this issue. The Office is satisfied the agency is complying with its legislative obligations but will review ONI's use of assumed identities in a dedicated inspection in 2022–23.

# COMPLAINTS AND PUBLIC INTEREST DISCLOSURES

Figure 6.1: Complaints process



## KEY STATISTICS



**80**

IGIS Act complaints



**10**

PID Act disclosures  
(received and/or allocated)



**431**

Other correspondence handled\*

\* Included purported complaints that did not meet the jurisdiction of the IGIS Act or PID Act)

The Office has a broad jurisdiction to receive and inquire into complaints and disclosures concerning the conduct of intelligence agencies, and the ACIC and AFP, in relation to their intelligence functions regarding network activity warrants.

Matters that are brought to the Office may fall within the jurisdiction of the IGIS Act or the PID Act. The IGIS also receives a large amount of other correspondence that do not fall within the jurisdiction of those Acts. This can include concerns and grievances about entities other than Australian intelligence agencies, and requests for information about intelligence agencies, both of which fall outside of IGIS's jurisdiction. The Office reviews all correspondence it receives to determine whether a matter falls within the jurisdiction of the IGIS Act or the PID Act.<sup>2</sup>

**Table 6.1: Complaints and PID statistics**

	2021–22 FY (1 July 2021 – 30 June 2022)	2020–21 FY* (1 July 2020 – 30 June 2021)	2019–20 FY (1 July 2019 – 30 June 2020)
<b>Complaints that fell within the jurisdiction of the IGIS Act</b>	80	344*	35
<b>Other correspondence that did not fall within the jurisdiction of the IGIS Act or PID Act</b>	431	N/A*	180
<b>Visa &amp; citizenship complaints and correspondence</b>	141	124	300
<b>PIDs</b>	10	16	2

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

2 Such correspondence was previously referred to by this Office as 'contacts'. However they are now described as 'complaints and other correspondence that do not fall within the jurisdiction of the IGIS Act or PID Act'.

## COMPLAINTS

### NON-VISA AND CITIZENSHIP RELATED

The number of correspondence lodged with the Office increased significantly during the reporting period – from 344 matters in 2020–21 to 511 matters in 2021–22. There was also an increase in the number of matters that fell within the jurisdiction of the IGIS Act, from 35 complaints in 2019–20 (when this data was last collected) to 80 complaints in 2021–22. The Office assessed each piece of correspondence to determine the most appropriate course of action, including to determine whether the matter fell within the jurisdiction of the IGIS Act or PID Act.

Where a matter was found not to engage either Act, the Office provided advice to the complainant about the IGIS's jurisdiction (where possible).

IGIS officers sought information from agencies relating to complaints by speaking with relevant agency staff, reviewing files and undertaking independent searches of agency databases to identify issues of legality or propriety and by making preliminary inquiries of the agencies under section 14 of the IGIS Act. Most matters were able to be resolved in a short period of time; however, COVID-19 restrictions did impact the Office's ability to resolve some matters in a timely manner.

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

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

### VISA AND CITIZENSHIP APPLICATION COMPLAINTS

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

The number of complaints regarding visa and citizenship applications increased slightly in 2021–22. An increased proportion of these complaints and correspondence related to matters that did not fall within the Office's jurisdiction or had not exceeded the timeframes that the Office used as a threshold for further investigating the complaint.

While a number of visa or citizenship applications were the subject of a known processing delay, the Office did not identify any systemic compliance issues in the visa and citizenship complaints investigated in 2021–22.



## PUBLIC INTEREST DISCLOSURES

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

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

At the end of 2021–22, the Office had 20 authorised officers under the PID scheme in addition to its principal officer, the Inspector-General. These officers were accessible to intelligence agency staff in the course of their regular attendance at agencies for routine activities such as inspections and briefings. The Office's authorised officers were also contactable via secure email and phone.

The Office received 10 disclosures relating to intelligence agencies during 2021–22. Of these disclosures:

- the Office allocated 4 disclosures to intelligence agencies for investigation
- the Office was allocated 6 disclosures:
  - one disclosure was allocated to the Office from an intelligence agency
  - the Office allocated 5 disclosures to itself for investigation
- Of the 6 disclosures allocated to the Office, the Office:
  - decided not to investigate one disclosure in accordance with s 49(1) of the PID Act so it could be investigated under the IGIS Act
  - decided not to investigate 3 disclosures further under s 48 of the PID Act
  - investigated 2 matters under the PID Act.

The kinds of disclosable conduct allocated to the Office during the reporting period included maladministration, danger to health or safety, contraventions of Commonwealth, State or Territory law, abuse of a position of trust and conduct which could lead to disciplinary action. Of the 10 PIDs received, table 6.2 provides details on the types of disclosable conduct claimed. One PID may relate to one or more agency or type of disclosable conduct.

**Table 6.2: Types of Disclosable Conduct**

Disclosable Conduct	Number of Disclosures
Maladministration	9
Contravention of a law of the Commonwealth, State or Territory	1
Danger to health or safety	2
Could lead to disciplinary action against a public official	2
Abuse of position of trust	1
Conduct that perverts the course of justice	1

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

During 2021–22, no PIDs were made about this Office.

## OVERSEEING THE OPERATION OF THE PID SCHEME IN THE INTELLIGENCE AGENCIES

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

During the reporting period IGIS was advised of 10 PIDs received by the intelligence agencies or the ACIC or AFP, and 4 of these were allocated to the agencies by the IGIS.

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

IGIS also has statutory responsibilities for assisting agency staff in their obligations under the PID Act and for conducting training and awareness raising exercises. Although COVID-19 restrictions affected the Office's ability to conduct general training throughout the reporting period, IGIS engaged with intelligence agencies on the handling of PID matters and remained available to assist when required.

# SECTION SEVEN

## ANNEXURES

# ANNEXURE 7.1

## OTHER MANDATORY INFORMATION

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

## ADVERTISING AND MARKET RESEARCH

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

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

## ECOLOGICALLY SUSTAINABLE DEVELOPMENT AND ENVIRONMENTAL PERFORMANCE

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

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

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

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

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

These include:

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

# 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
<b>17AD(g)</b>	<b>Letter of transmittal</b>			
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
<b>17AD(h)</b>	<b>Aids to access</b>			
17AJ(a)	Preliminaries	Table of contents (print only).	Mandatory	iv–v
17AJ(b)	Annexures	Alphabetical index (print only).	Mandatory	119
17AJ(c)	Preliminaries	Glossary of abbreviations and acronyms.	Mandatory	vii–viii
17AJ(d)	Annexures	List of requirements.	Mandatory	109
17AJ(e)	Preliminaries	Details of contact officer.	Mandatory	Inside front cover
17AJ(f)	Preliminaries	Entity's website address.	Mandatory	Inside front cover
17AJ(g)	Preliminaries	Electronic address of report.	Mandatory	Inside front cover
<b>17AD(a)</b>	<b>Review by accountable authority</b>			
17AD(a)	Section 1	A review by the accountable authority of the entity.	Mandatory	1–4
<b>17AD(b)</b>	<b>Overview of the entity</b>			
17AE(1)(a)(i)	Section 2	A description of the role and functions of the entity.	Mandatory	8

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AE(1)(a)(ii)	Section 2	A description of the organisational structure of the entity.	Mandatory	10
17AE(1)(a)(iii)	Section 3	A description of the outcomes and programmes administered by the entity.	Mandatory	18
17AE(1)(a)(iv)	Section 2	A description of the purposes of the entity as included in corporate plan.	Mandatory	6
17AE(1)(aa)(i)	Section 3	Name of the accountable authority or each member of the accountable authority.	Mandatory	16
17AE(1)(aa)(ii)	Section 3	Position title of the accountable authority or each member of the accountable authority.	Mandatory	16
17AE(1)(aa)(iii)	Section 4	Period as the accountable authority or member of the accountable authority within the reporting period.	Mandatory	32
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
<b>17AD(c)</b>	<b>Report on the Performance of the entity</b>			
	<b><i>Annual Performance Statements</i></b>			
17AD(c)(i); 16F	Section 3	Annual performance statement in accordance with paragraph 39(1)(b) of the Act and section 16F of the Rule.	Mandatory	16–24
<b>17AD(c)(ii)</b>	<b><i>Report on Financial Performance</i></b>			
17AF(1)(a)	Section 5	A discussion and analysis of the entity's financial performance.	Mandatory	71–72

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AF(1)(b)	Section 5	A table summarising the total resources and total payments of the entity.	Mandatory	71–72
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
<b>17AD(d)</b>	<b>Management and Accountability</b>			
	<b>Corporate Governance</b>			
17AG(2)(a)	Section 4	Information on compliance with section 10 (fraud systems).	Mandatory	41
17AG(2)(b)(i)	Preliminaries	A certification by accountable authority that fraud risk assessments and fraud control plans have been prepared.	Mandatory	iii
17AG(2)(b)(ii)	Preliminaries	A certification by accountable authority that appropriate mechanisms for preventing, detecting incidents of, investigating or otherwise dealing with, and recording or reporting fraud that meet the specific needs of the entity are in place.	Mandatory	iii
17AG(2)(b)(iii)	Preliminaries	A certification by accountable authority that all reasonable measures have been taken to deal appropriately with fraud relating to the entity.	Mandatory	iii
17AG(2)(c)	Section 4	An outline of structures and processes in place for the entity to implement principles and objectives of corporate governance.	Mandatory	35–37

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(2)(d) – (e)	n/a	A statement of significant issues reported to Minister under paragraph 19(1)(e) of the Act that relates to noncompliance with Finance law and action taken to remedy noncompliance.	If applicable, Mandatory	n/a
<b>Audit Committee</b>				
17AG(2A)(a)	Section 4	A direct electronic address of the charter determining the functions of the entity's audit committee.	Mandatory	35
17AG(2A)(b)	Section 4	The name of each member of the entity's audit committee.	Mandatory	36–27
17AG(2A)(c)	Section 4	The qualifications, knowledge, skills or experience of each member of the entity's audit committee.	Mandatory	36–37
17AG(2A)(d)	Section 4	Information about the attendance of each member of the entity's audit committee at committee meetings.	Mandatory	36–37
17AG(2A)(e)	Section 4	The remuneration of each member of the entity's audit committee.	Mandatory	36–37
<b>External Scrutiny</b>				
17AG(3)	Section 4	Information on the most significant developments in external scrutiny and the entity's response to the scrutiny.	Mandatory	42
17AG(3)(a)	Section 4	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	42
17AG(3)(b)	Section 4	Information on any reports on operations of the entity by the AuditorGeneral (other than report under section 43 of the Act), a Parliamentary Committee, or the Commonwealth Ombudsman.	If applicable, Mandatory	42
17AG(3)(c)	Section 4	Information on any capability reviews on the entity that were released during the period.	If applicable, Mandatory	42



PGPA Rule Reference	Part of Report	Description	Requirement	Page
<b>Management of Human Resources</b>				
17AG(4)(a)	Section 4	An assessment of the entity's effectiveness in managing and developing employees to achieve entity objectives.	Mandatory	26–29
17AG(4)(aa)	Section 4	Statistics on the entity's employees on an ongoing and nonongoing basis, including the following: (a) statistics on fulltime employees; (b) statistics on parttime employees; (c) statistics on gender (d) statistics on staff location	Mandatory	29–30
17AG(4)(b)	Section 4	Statistics on the entity's APS employees on an ongoing and nonongoing basis; including the following: <ul style="list-style-type: none"> <li>• Statistics on staffing classification level;</li> <li>• Statistics on fulltime employees;</li> <li>• Statistics on parttime employees;</li> <li>• Statistics on gender;</li> <li>• Statistics on staff location;</li> <li>• Statistics on employees who identify as Indigenous.</li> </ul>	Mandatory	29–30
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	31
17AG(4)(c)(i)	Section 4	Information on the number of SES and nonSES employees covered by agreements etc identified in paragraph 17AG(4)(c).	Mandatory	31–32
17AG(4)(c)(ii)	Section 4	The salary ranges available for APS employees by classification level.	Mandatory	30
17AG(4)(c)(iii)	Section 4	A description of nonsalary benefits provided to employees.	Mandatory	31

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(4)(d)(i)	n/a	Information on the number of employees at each classification level who received performance pay.	If applicable, Mandatory	n/a
17AG(4)(d)(ii)	n/a	Information on aggregate amounts of performance pay at each classification level.	If applicable, Mandatory	n/a
17AG(4)(d)(iii)	n/a	Information on the average amount of performance payment, and range of such payments, at each classification level.	If applicable, Mandatory	n/a
17AG(4)(d)(iv)	n/a	Information on aggregate amount of performance payments.	If applicable, Mandatory	n/a
<b>Assets Management</b>				
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	42
<b>Purchasing</b>				
17AG(6)	Section 4	An assessment of entity performance against the <i>Commonwealth Procurement Rules</i> .	Mandatory	42–43
<b>Reportable consultancy contracts</b>				
17AG(7)(a)	Section 4	A summary statement detailing the number of new reportable consultancy contracts entered into during the period; the total actual expenditure on all such contracts (inclusive of GST); the number of ongoing reportable consultancy contracts that were entered into during a previous reporting period; and the total actual expenditure in the reporting period on those ongoing contracts (inclusive of GST).	Mandatory	43–44

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(7)(b)	Section 4	A statement that <i>"During [reporting period], [specified number] new reportable consultancy contracts were entered into involving total actual expenditure of \$[specified million]. In addition, [specified number] ongoing reportable consultancy contracts were active during the period, involving total actual expenditure of \$[specified million]"</i> .	Mandatory	43
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	43
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	43
<b>Reportable non-consultancy contracts</b>				
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	44
17AG(7A)(b)	Section 4	A statement that <i>"Annual reports contain information about actual expenditure on reportable non-consultancy contracts. Information on the value of reportable non-consultancy contracts is available on the AusTender website."</i>	Mandatory	44

PGPA Rule Reference	Part of Report	Description	Requirement	Page
<b>17AD(daa)</b>	<b><i>Additional information about organisations receiving amounts under reportable consultancy contracts or reportable non-consultancy contracts</i></b>			
17AGA	Section 4	Additional information, in accordance with section 17AGA, about organisations receiving amounts under reportable consultancy contracts or reportable non-consultancy contracts.	Mandatory	43–44
<b><i>Australian National Audit Office Access Clauses</i></b>				
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 AuditorGeneral with access to the contractor's premises, the report must include the name of the contractor, purpose and value of the contract, and the reason why a clause allowing access was not included in the contract.	If applicable, Mandatory	44
<b><i>Exempt contracts</i></b>				
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	44
<b><i>Small business</i></b>				
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	43

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(10)(b)		An outline of the ways in which the procurement practices of the entity support small and medium enterprises.	Mandatory	43
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
<b>Financial Statements</b>				
17AD(e)	Section 5	Inclusion of the annual financial statements in accordance with subsection 43(4) of the Act.	Mandatory	46–70
<b>Executive Remuneration</b>				
17AD(da)	Section 4	Information about executive remuneration in accordance with Subdivision C of Division 3A of Part 23 of the Rule.	Mandatory	31–32
<b>17AD(f)</b>	<b>Other Mandatory Information</b>			
17AH(1)(a)(i)	n/a	If the entity conducted advertising campaigns, a statement that “During [reporting period], the [name of entity] conducted the following advertising campaigns: [name of advertising campaigns undertaken]. Further information on those advertising campaigns is available at [address of entity’s website] and in the reports on Australian Government advertising prepared by the Department of Finance. Those reports are available on the Department of Finance’s website.”	If applicable, Mandatory	n/a
17AH(1)(a)(ii)	Annexures	If the entity did not conduct advertising campaigns, a statement to that effect.	If applicable, Mandatory	108

PGPA Rule Reference	Part of Report	Description	Requirement	Page
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	33
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	44
17AH(1)(e)	n/a	Correction of material errors in previous annual report	If applicable, mandatory	n/a
17AH(2)	Section 4 Annexures	Information required by other legislation	Mandatory	33, 108

# INDEX

## A

- AAT *see* Administrative Appeals Tribunal
- abuse of trust *see* public interest disclosures
- Accountable Authority Instructions, 43
- ACIC *see* Australian Criminal Intelligence Commission
- ACLEI *see* Australian Commission for Law Enforcement Integrity
- ACSC *see* Australian Cyber Security Centre
- ACT Health, 33
- ADF *see* Australian Defence Force
- Administrative Appeals Tribunal (AAT), 12
- advertising and market research, 108
- AFP *see* Australian Federal Police
- AGD *see* Attorney-General's Department
- agency oversight activities, 80–101
- AGO *see* Australian Geospatial-Intelligence Organisation
- AHO *see* Australian Hydrographic Office
- AHRC *see* Australian Human Rights Commission
- AHRC Act *see* *Australian Human Rights Commission Act 1986*
- AMLCTF *see* *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
- ANAO *see* Australian National Audit Office
- annual performance statement, vi, 16–24
  - 2021–22 performance review, 19–22
  - accountable authority statement, 16
  - Objective 1: Inquiries, 19
  - Objective 2: Inspections, 20
  - Objective 3: Complaints, 21–22
  - Objective 4: Public Interest Disclosures, 23–24
  - reporting framework, 17–18
  - results, 16
- annual reports, requirements for, 109–113
- Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AMLCTF), 98, 99
- APS *see* Australian Public Service
- Archives Act 1983*, 8, 12
- ASD *see* Australian Signals Directorate
- ASIO *see* Australian Security Intelligence Organisation
- ASIS *see* Australian Secret Intelligence Service
- ASL *see* average staffing level
- asset management, 42
- see also* financial statements
- Assistant Inspectors-General, 32
- assumed identities, 90, 98
  - use and management, 99–100
- Attorney-General, iii, 9, 46, 75, 82, 83, 84, 86–88, 96
- Attorney-General's Department (AGD), 26, 34, 37, 38
  - Office of IGIS co-location with, 108
- Attorney-General's Department (AGD), 3
- audit and assurance activities, 35
- Audit Committee, 35–37, 40
- audit, internal, 37
- Auditor-General, 44, 46, 47, 111
  - report, 42
- AusTender, 43–44
- AUSTRAC *see* Australian Transaction Reports and Analysis Centre
- Australian Commission for Law Enforcement Integrity (ACLEI), 38
- Australian Criminal Intelligence Commission (ACIC), 3, 98
  - inspections, 98
  - oversight by IGIS, 8
  - PID scheme, 106
- Australian Cyber Security Centre (ASCS), 77
- Australian Defence Force (ADF), 77, 78, 79, 97
- Australian Federal Police (AFP), 3, 98
  - inspections, 98
  - oversight by IGIS, 8
  - PID scheme, 106
- Australian Geospatial-Intelligence Organisation (AGO), 8, 78, 87, 95–97
  - and ASD joint activities, 96
  - compliance incidents, 96–97
  - compliance with Privacy Rules, 97
  - COVID-19 restrictions, effect of, 97
  - Defence advice to Foreign Investment Board, 96
  - IGIS Act, 95
  - inspections, 96
  - joint activities with ASD, 93
  - key statistics, 78
  - ministerial authorisation, 96
  - other reviews, 97
  - Post Activity Reporting, 96
  - Privacy Rules, 96 provision of geospatial

- products to partners, 96
- Australian Human Rights Commission (AHRC), 38
- Australian Human Rights Commission Act 1986* (AHRC Act), 38
- Australian Hydrographic Office (AHO), 97
- Australian Information Commissioner, 3, 12, 39, 99, 111
- Australian National Audit Office (ANAO), 36, 42, 44, 46–47
- Australian National University
  - National Security College, 27, 44
- Australian Public Service (APS), 29
  - classifications, 30
  - code of conduct, 26, 41
  - integrity and values, 26, 41
  - reporting of disability statistics, 33
- Australian Public Service Academy (APS Academy), 27
- Australian Public Service Commissioner, 3
- Australian Secret Intelligence Service (ASIS), 8, 76, 89–91
  - assumed identities, 99–100, 101
  - AUSTRAC information, 99
  - compliance incidents, 91
  - compliance with Crimes Act, 91
  - data holdings, 89
  - human rights assessments, 89–90
  - inspections, 89–90
  - inspections underway, 90
  - key statistics, 76
  - liaison with foreign services, 89–90
  - operational file reviews, 90
  - operational files, 89
  - Privacy Rules, 90, 91
  - Australian Security Intelligence Organisation (ASIO), 8, 75
    - assumed identities, 86, 99–100
    - AUSTRAC information, 99
    - compliance incidents, 85–88
    - compliance of warrants with law, 88
    - compliance reviews, 81
    - compliance with Crimes Act, 86
    - compulsory questioning, 84
    - COVID-19 restrictions, impact of, 81
    - data deletion, 88
    - data sharing, 88
    - deletion of information, 82, 83
    - finalisation of 2020–21 compliance incidents, 88–89
    - grounds for warrants, 86
    - IGIS inspections commenced in 2020–21, 83
    - inspections, 81–84
    - key statistics, 75
    - ministerial submissions, 82, 84
    - Office of IGIS engagement, 81
    - other reviews, 84
    - questioning sessions, 88–89
    - review of directions, 6
    - special intelligence operation (SIO) powers, 83–84
    - surveillance device warrants, 83
    - surveillance devices, 86–87
    - temporary exclusion orders, 83
    - use of force, 84
    - use of telecommunications data, 85
    - video recordings, 88–89
    - visa applications, 87
  - Australian Security Intelligence Organisation Act 1979* (ASIO Act), 81, 84, 86, 88–89
    - Minister's Guidelines, 86
    - search warrants, 87
- Australian Signals Directorate (ASD), 8, 77, 92–95
  - alleged staff misconduct, 92
  - communications interception, 94
  - Compliance and Oversight Team, 95
  - compliance incidents, 88, 93–95
  - compliance with Privacy Rules, 94–95
  - earlier compliance incidents, 95
  - inquiries, 92
  - inspections, 93
  - interception under the TIA Act, 93
  - IS Act, 95
  - key statistics, 77
  - ministerial authorisations, 92, 93, 95
  - preliminary inquiries, 92–93
  - Privacy Rules, 93, 95
  - Public Interest Disclosure, 92
  - TIA Act, 94
- Australian Transaction Reports and Analysis Centre (AUSTRAC), 3, 89, 98
  - access to information, 99
  - authorised representatives, 88
  - average staffing level (ASL), 29



## B

baseline measure for assessment, 19  
 BellChambersBarrett, 43  
 Brookes, Chris, 10, 32  
 business continuity framework, 35

## C

Canada *see* Five Eyes  
 CCSSC *see* Cultural and Corporate Shared Services Centre  
 Chief of Defence Force, 79  
 Chief of Defence Intelligence, 97  
 citizenship and visa complaints, 103–104  
 classified material and remote working, 2  
 Code of Conduct (APS), 26, 41  
 Commissioner of Intelligence Warrants of New Zealand, 39  
 committee structure, 35  
 Commonwealth Contracting Suite, 42, 44  
*Commonwealth Electoral Act 2018*, 108  
 Commonwealth Ombudsman, 39, 42, 111  
 Commonwealth Procurement Rules (CPRs), 42, 43  
 communications interception, 94  
 complaints (Objective 3), 9, 21–22  
     jurisdiction of the Office, 103  
     key statistics, 103  
     other than visa and citizenship matters, 104  
     PID statistics, 103  
     process, 102  
     visa and citizenship matters, 22, 81, 103, 104  
 compliance with standards, 2  
 concerns and grievances *see* complaints  
 conduct leading to disciplinary action *see* public interest disclosures  
 conflict of interest *see* ethical standards  
 consultants, 43  
 contracts, 44  
 contravention of law *see* public interest disclosures  
 Convention on the Rights of Persons with Disabilities, 33  
 Cook, Katherine, 10, 32  
 corporate governance, 3, 35–37, 110  
 Corporate Plan, 18  
 Corporate Plan 2021–22, 16  
 Corporate Plan 2022–23, 19  
*Counter-Terrorism (Temporary Exclusion Orders) Act 2019* (CT(TEO) Act), 83

COVID-19, 2, 3

app *see* COVIDSafe app data  
 impact on inspections, 20  
 impact on interviews, 19  
 lockdowns, 13, 80, 95, 97  
 restrictions, 89, 92, 97  
 travel restrictions, 13, 39  
 workplace health measures, 33

COVIDSafe app data, 3, 11, 39, 98, 99

CPR *see* Commonwealth Procurement Rules (CPRs)

credit cards, corporate, 42

crime *see* Australian Criminal Intelligence

Commission; Australian Federal Police

*Crimes Act 1914*, 81, 86, 91, 98, 99–101

Criminal Code, 86

cross-agency inspection activities, 98–101

CT(TEO) Act *see* *Counter-Terrorism (Temporary Exclusion Orders) Act 2019*

Cultural and Corporate Shared Services Centre (CCSSC), 38

cyber security, 40, 77, 92

## D

danger to health or safety *see* public interest disclosures

Defence Intelligence Organisation (DIO), 8, 79, 97–98

analytic integrity, 97

COVID-19 lockdowns, disruptions, 97

Five-Eyes Memorandum of Understanding, 97

inspections, 97–98

key statistics, 79

other reviews, 98

Privacy Rules, 97

Department of Defence, 78

Department of Home Affairs, 104

Deputy Inspector-General (IGIS), 30, 32, 36, 83

DIO *see* Defence Intelligence Organisation

Director-General of AGO, 95, 96

Director-General of ASD, 92

Director-General of ASIS, 89

Director-General of ONI, 101

Director-General of Security, 86, 88

disability reporting mechanism, 33

Disability Strategy, 33

disclosures *see* public interest disclosures

discrimination, 104

diversity and inclusion

Health Check, 26–27

Diversity and Inclusion Committee, 26

## E

ecologically sustainable development, 108

Employee Assistance Program, 33

employment frameworks, 31

*see also* human resources

energy-saving, 108

Enterprise Agreement 2020–2023, 31

entity resource statements, 71–72

*Environment Protection and Biodiversity Conservation Act 1999*, 108

environmental performance, 108

ethical standards and fraud control, iii, 35, 41

Fraud Control Plan, 40

Ethics Contact Officer Network of APS Commission, 41

Executive Board, 28, 33, 35, 40

executive remuneration, 31–32

exempt contracts, 44

external scrutiny, 42–44

## F

Fallen, Brad, 10, 32

financial statements, 45–72

FIORC *see* Five Eyes Intelligence Oversight and Review Council

Five Eyes Intelligence Oversight and Review Council (FIORC), 3, 39, 97

FOI Act *see* *Freedom of Information Act 1982*  
force, use of, 84

Foreign Acquisitions and Takeovers Act, 87

Foreign Investment Review Board, 96

Foreign Minister, 90

fraud control *see* ethical standards and fraud control

*Freedom of Information Act 1982* (FOI Act), 8, 12, 44

## G

gender balance of employees, 30

Gillian Beaumont Recruitment Pty Ltd, 43

governance committee structure, 35

Governance Directorate, 37

grievances *see* complaints

## H

harassment or surveillance, alleged, 104

Harradine Order, 44

health, 33, 40, 105, 106

Health Check, diversity and inclusion, 26–27

HR *see* human resources

human resources (HR), 3–4

average staffing level, 29

challenges of recruiting staff, 3

diversity and inclusion, 26–27

employment frameworks, 31

executive remuneration, 31–32

gender balance of employees, 30

Indigenous employees, 29

key management personnel, 31–32

labour market shortages, 29

learning and development, 27

*OGIS Enterprise Agreement 2020–2023*, 31

ongoing employees, 29

performance pay, 33

staffing profile, 30

workplace health and safety, 33

human rights

ASIO, 85

ASIS, 89–90

assessments, 89–90

Australian Human Rights Commission, 38

inquiries, 19

inspections, 20

purpose of IGIS, 6, 8, 18

## I

ICT *see* information and communications technology

identities, assumed *see* assumed identities

IGIS Act *see* *Inspector-General of Intelligence and Security Act 1986*

IGIS Audit Committee, 35–37, 40

Independent Intelligence Review (2017), 2

Indigenous businesses, commitment to, 43

Indigenous employees, 29

influenza vaccination, 33

information and communications technology (ICT), 3, 34, 38

Information Commissioner *see* Australian Information Commissioner

information governance, 3, 34  
 Information Governance Framework, 34  
 information management  
     AUSTRAC information, 99  
     requirements, 34  
 Information Publication Scheme (IPS), 44  
 informing the public, 13  
 inquiries (Objective 1), 2, 7, 8, 9, 19 *see also*  
 preliminary inquiries  
     AGO, 95  
     ASD, 92–93  
     ASIO, 81  
     ASIS, 89  
     DIO, 97  
     ONI, 80  
 inspection activities, cross-agency, 98–101  
 inspections (Objective 2), 2, 7, 8, 9, 20  
     ACIC, 98  
     AFP, 98  
     AGO, 78, 96  
     ASD, 77, 92–94  
     ASIO, 75, 81, 83–85  
     ASIS, 76, 89–90  
     COVIDSafe app data, 99  
     DIO, 79, 97  
     ONI, 80–81  
 Inspector General of the Intelligence Community  
 of the United States, 39  
 Inspector-General of Intelligence and Security  
     international engagement, 39  
     letter of transmittal, iii  
     review, 2–4  
     role of, 8  
*Inspector-General of Intelligence and Security Act*  
*1986*, vi, 2, 6, 8, 11, 18, 19, 20, 21, 23–24, 80, 81, 92,  
 93, 96, 97, 102–103, 104  
 Inspector-General of Intelligence and Security of  
 New Zealand, 39  
 Integrity Agencies Group, 3, 38  
 Intelligence Commissioner of Canada, 39  
 Intelligence Oversight and Other Legislation  
 Amendment (Integrity Measures) Bill 2020, 3  
*Intelligence Services Act 2001*, 76, 78, 82, 89–90, 91,  
 93, 96  
 interception under the TIA Act, 93  
 internal audit, 37  
 international stakeholders, 39

investigative powers, 8  
 Investigatory Powers Commissioner's Office of the  
 United Kingdom, 39  
 IPS *see* Information Publication Scheme  
*IS Act see Intelligence Services Act 2001*

## J

Jessup, the Hon Christopher KC (formerly QC), iii,  
 10, 16, 32

## K

Kensey, Nathan, 32  
 key activities of IGIS, 9  
 key management personnel, 31–32  
 KMP *see* key management personnel

## L

law enforcement integrity, 38

## M

MA *see* ministerial authorisations  
 maladministration *see* public interest disclosures  
 management and accountability, 25–44  
*see also* corporate governance; external scrutiny;  
 human resources; purchasing and procurement  
 market research and advertising, 108  
 McFarlane, Steve, 32  
 Minister for Defence, 77, 78, 79, 92, 93, 96  
 Minister for Foreign Affairs, 76  
 Minister for Home Affairs, 84  
 ministerial authorisations (MA), 82, 90, 91

## N

National Archives of Australia information  
 management policy, 34  
 National Centre for Intelligence Training and  
 Education, 27  
 National Intelligence Community (NIC), 26, 28, 29,  
 74  
 National Museum of Australia, 38  
 National Security and Intelligence Review Agency  
 of Canada, 39  
 National Security College, ANU, 27  
 National Security Committee of Cabinet, 74  
 National Security Legislation Amendment Bill  
 2021, 11, 12  
 nationality, presumption of, 94–95  
 network activity warrants (NAW), 3, 8, 98, 103, 106

New Zealand *see* Five Eyes

NIC *see* National Intelligence Community

non-compliance with standards, 2

Notzon-Glenn, Bronwyn, 10, 32

## O

OAIC *see* Office of the Australian Information Commissioner

Office of National Intelligence (ONI), 8, 99

assumed identities, 99–100, 101

compliance incidents, 81

compliance with privacy rules, 80

COVID-19, impact of, 80

engagement with Office of IGIS, 80

functions, 2

inspections, 80

key statistics, 74

Office of IGIS engagement, 80

other reviews, 81

Privacy Rules, 80

role, 74

*Office of National Intelligence Act 2018* (ONI Act), 74, 80

Office of the Australian Information Commissioner (OAIC), 3, 39, 99, 111

Office of the Commonwealth Ombudsman, 39

*OGIS Enterprise Agreement 2020–2023*, 31

ONI *see* Office of National Intelligence

ONI Act *see* *Office of National Intelligence Act 2018*

online crime, 98

organisation chart, 10

organisational profile, 29–34

outreach, 13, 26, 97

diversity and inclusion, 26

public outreach activities, 13

Oversight Capability Review, 28

oversight, proactive, 28

## P

paper saving, 108

parliamentary committees, 42

Parliamentary Joint Committee on Intelligence and Security (PJCS), 3, 11, 12

PBS *see* Portfolio Budget Statements

performance agreements, 27, 41

performance analysis *see* annual performance statement

performance monitoring and reporting, 35

performance review *see* annual performance statement

personas *see* assumed identities

perverting the course of justice *see* public interest disclosures

PGPA Act *see* *Public Governance, Performance and Accountability Act 2013*

PGPA Rule *see* Public Governance, Performance and Accountability Rule 2014

PID *see* public interest disclosure

PID Act *see* *Public Interest Disclosure Act 2013*

PJCIS *see* Parliamentary Joint Committee on Intelligence and Security

Portfolio Budget Statements (PBS), 16–18

PQQC Consulting, 43

preliminary inquiries, 9, 21, 92–93, 104

Prime Minister, 9, 11, 17, 18, 72, 74, 80

*Privacy Act 1988*, 39, 98, 99

Privacy Rules, 80, 94–95

procurement, 42–43

Project REDSPICE, 92

*Public Governance, Performance and Accountability Act 2013* (PGPA Act), vi, 16, 35, 42, 43

Public Governance, Performance and Accountability Rule 2014, vi, 42, 43, 108

*Public Interest Disclosure Act 2013* (PID Act), 8, 9, 23–24, 102–103, 104, 105–106

public interest disclosure(s) (Objective 4), 23–24

public interest disclosures (Objective 4), 9, 19, 24, 105–106

*Public Service Act 1999*, 31

purchasing and procurement, 42–44, 108

## Q

Quiggin, Peter, 37

## R

Reconciliation Action Plan, 26

recruitment campaigns, 29

recycling, 108

remote working, 2

*see also* COVID-19

remuneration *see* human resources

Remuneration Tribunal, 31

reporting framework, 18

requirements for annual reports, 109–113

Resilience, Effects, Defence, Space, Intelligence,

Cyber, Enablers, 92

*Review of Administration and Expenditure No. 20 (2020–2021)*, 12

review of reporting period, vi, 2–4

*Review of the Counter-Terrorism (Temporary Exclusion Orders) Act 2019*, 12

*Review of the Migration and Citizenship Legislation Amendment Bill 2020*, 12

*Review of the National Security Legislation Amendment Bill 2021*, 12

risk management, 35, 40–41

Risk Register, 40

Royal-Commission-like powers, 8, 9

Rules to Protect the Privacy of Australian Persons, 80

## S

Safe Work Australia, 33

salaries *see* human resources

scrutiny, external, 42–44

Searle, Julia, 32

Secretary for Defence, 79

security assessments, 104

Senate Continuing Order for Indexed File Lists, 44

SIOs *see* special intelligence operations

special intelligence operations (SIOs), 75, 82, 83–84

staff *see* human resources

stakeholders

domestic, 38–39

international, 39

State of the Service reports (APS), 33

Statement of Procedures, 89

Statistical Bulletin (APS), 33

Stone, the Hon Margaret (former Inspector-General), 84

strategic corporate planning, 35

*Surveillance Devices Act 2004*, 86–87

*Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*, 3, 8, 98

surveillance or harassment, alleged, 104

Synergy Group Australia Pty Ltd, 43

systems technology and information governance, 34

## T

*Telecommunications (Interception and Access) Act 1979* (TIA Act), 82, 88, 93, 94, 96

trust, abuse of *see* public interest disclosures

## U

United Kingdom *see* Five Eyes

United Nations Convention on the Rights of Persons with Disabilities, 33

United States *see* Five Eyes

utilities consumption, 108

## V

vaccination, influenza, 33

Vandenbroek, Sarah, 36

visa and citizenship complaints, 103–104

## W

warrants, 3, 8, 75, 82–85, 88, 103, 106

Waugh, Linda, 37

weapons and weapons training, 89

wellbeing allowance, 33

WHS Act *see* *Work Health and Safety Act 2011*

women *see* human resources

Women's Network, 26

*Work Health and Safety Act 2011* (WHS Act), 33

workplace health and safety, 33

## Y

Yardstick Advisory Pty Ltd, 43