



**IGIS**

INSPECTOR-GENERAL OF  
INTELLIGENCE AND SECURITY

# 2020–2021

## ANNUAL REPORT

# IGIS CONTACT INFORMATION

## LOCATION

3-5 National Circuit  
BARTON ACT 2600

## WRITTEN INQUIRIES

Inspector-General of Intelligence and Security  
3-5 National Circuit  
BARTON ACT 2600

## PARLIAMENTARY AND MEDIA LIAISON

Phone: (02) 6141 3330  
Email: [info@igis.gov.au](mailto:info@igis.gov.au)

## GENERAL INQUIRIES

Phone: (02) 6141 3330  
Email: [info@igis.gov.au](mailto:info@igis.gov.au)

## COMPLAINTS

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

## 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.

## INTERNET

Homepage:  
[www.igis.gov.au](http://www.igis.gov.au)

Annual report:  
[www.igis.gov.au/about/annual-report](http://www.igis.gov.au/about/annual-report)

ISSN: 1030-4657

© Commonwealth of Australia 2021



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)

Typesetting by Typeyard Design & Advertising [typeyard.com.au](http://typeyard.com.au)  
Printed by CanPrint Communications [canprint.com.au/AboutUs/](http://canprint.com.au/AboutUs/)



Senator the Hon Michaelia Cash  
Attorney-General  
Parliament House  
CANBERRA ACT 2600

Dear Attorney-General

I am pleased to present the Inspector-General of Intelligence and Security annual report for the period 1 July 2020 to 30 June 2021.

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

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

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

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

Yours sincerely

The Hon Christopher Jessup QC  
Inspector-General of Intelligence and Security  
4 October 2021

# CONTENTS

IGIS contact information	inside cover
Letter of transmittal	iii
About this report	vi
Guide to the report	vi
Glossary	vii

## SECTION ONE

### **OVERVIEW 1**

---

Inspector-general's review	2
The role of the igis	5
Organisational structure	7
Outcome and program structure	7
Purpose	8
The intelligence agencies	9

## SECTION TWO

### **ANNUAL PERFORMANCE STATEMENT 11**

---

2020–21 Annual performance statement	12
Statement by the accountable authority	12
Results	12
IGIS performance framework for 2021–22	18
Analysis	19
<b>Objective 1</b> – Assisting ministers	19
<b>Objective 2</b> – Assuring parliament	19
<b>Objective 3</b> – Informing the public	21
<b>Objective 4</b> – Inquiries	22
<b>Objective 4</b> – Inspections	25
<b>Objective 4</b> – Complaints and public interest disclosures	61
<b>Objective 5</b> – Infrastructure and stakeholders	65
<b>Objective 6</b> – High-performing workforce	68

## SECTION THREE

### **MANAGEMENT AND ACCOUNTABILITY** **69**

---

Corporate governance	70
External scrutiny	76
Management of human resources	77
Asset management	80
Purchasing and procurement	80

## SECTION FOUR

### **FINANCIAL MANAGEMENT** **83**

---

Financial statements	84
<b>Appendix A:</b> Entity resource statements and resource for outcomes	108

## SECTION FIVE

### **ANNEXURES** **111**

---

<b>Annexure 5.1:</b> IGIS salary scale	112
<b>Annexure 5.2:</b> Key management personnel	113
<b>Annexure 5.3:</b> Other mandatory information	115
<b>Annexure 5.4:</b> Requirements for annual reports	117
Index	127

# 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 2020–21 financial year.

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. This section also outlines the role and functions of the Inspector-General and the Office, its published outcomes and program structure and a brief description of each of the 6 intelligence agencies the Inspector-General oversees.

**Section Two** contains the Annual Performance Statement, detailing the Office’s performance during the reporting period against the indicators identified in the IGIS Corporate Plan 2020–21.

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

**Section Four** contains a summary of the Office’s financial management and audited financial statements.

**Section Five** contains the annexures to this report. The annexures contain a range of additional information about the Office, including staff salary ranges and an index.

# GLOSSARY

AAT	Administrative Appeals Tribunal
ACIC	Australian Criminal Intelligence Commission
ACSC	Australian Cyber Security Centre
ACT	Australian Capital Territory
ADF	Australian Defence Force
AFP	Australian Federal Police
AGD	Attorney-General's Department
AGO	Australian Geospatial-Intelligence Organisation
AHO	Australian Hydrographic Office
AMLCTF Act	<i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i>
ANAO	Australian National Audit Office
APS	Australian Public Service
Archives Act	<i>Archives Act 1983</i>
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ASIO Act	<i>Australian Security Intelligence Organisation Act 1979</i>
ASIS	Australian Secret Intelligence Service
AUSTRAC	Australian Transaction Reports and Analysis Centre
Comprehensive Review	Comprehensive Review of the Legal Framework of the National Intelligence Community
Crimes Act	<i>Crimes Act 1914</i>
Criminal Code	<i>Criminal Code Act 1995</i>
DIO	Defence Intelligence Organisation
FIORC	Five Eyes Intelligence Oversight and Review Council
The Five Eyes	The Five Eyes countries comprising an intelligence alliance of Australia, Canada, New Zealand, the United Kingdom and the United States
FOI Act	<i>Freedom of Information Act 1982</i>
KMP	Key Management Personnel
IATD	Internally authorised tracking device
ICT	Information and Communications Technology
IGIS/The Office	The statutory agency of the Inspector-General of Intelligence and Security
IGIS Act	<i>Inspector-General of Intelligence and Security Act 1986</i>
IPS	Information Publication Scheme
IS Act	<i>Intelligence Services Act 2001</i>
NIC	National Intelligence Community
OCO	Office of the Commonwealth Ombudsman
ONI	Office of National Intelligence
ONI Act	<i>Office of National Intelligence Act 2018</i>
PBS	Portfolio Budget Statement
PGPA Act	<i>Public Governance, Performance and Accountability Act 2013</i>
PGPA Rule	Public Governance, Performance and Accountability Rule 2014
PID Act	<i>Public Interest Disclosure Act 2013</i>
PID	Public Interest Disclosure
PJCIS	Parliamentary Joint Committee on Intelligence and Security
Privacy Act	<i>Privacy Act 1988</i>
SES	Senior Executive Service
SIO	Special intelligence operations
The intelligence agencies	ONI, ASIO, ASIS, ASD, AGO and DIO
TIA Act	<i>Telecommunications (Interception and Access) Act 1979</i>
Telecommunications Act	<i>Telecommunications Act 1997</i>
WHS Act	<i>Work Health and Safety Act 2011</i>





# **SECTION ONE**

## OVERVIEW

# INSPECTOR-GENERAL'S REVIEW

In accordance with s 35 of the IGIS Act, this report provides details of inquiry and inspection activities during the reporting period, and on intelligence agencies compliance with certain privacy rules. It also provides details of the performance and financial position of this Office.

In the year under review, there have been 3 Inspectors-General of Intelligence and Security, either acting or substantive. Until 23 August 2020, The Hon Margaret Stone AO FAAL was Inspector-General, her 5-year term of office reaching its conclusion on that date. From then until 18 January 2021, the Deputy Inspector-General, Jake Blight, acted in the position of Inspector-General. From that date until 8 February 2021, I held the office of Inspector-General on an acting basis, after which my substantive term of office commenced. I take this opportunity to acknowledge the substantial contribution made by Ms Stone to the development and operation of the important oversight role of the Office of the Inspector-General over the 5 years in which she held the office. I also express my appreciation of the dedication and energy which Mr Blight brought to the discharge of his changing duties in the Office over a considerable period, and of the guidance which he provided for me during the early days of my own responsibilities as Inspector-General.

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. During the year under review, one inquiry (which had been commenced in a previous year) was completed and another inquiry was commenced (and remained on-going at the year-end). Further particulars of these inquiries are set out in the relevant sections of this report. By contrast, regular inspection work is a daily activity for the Office. Our inspection teams regularly encounter material in the files of intelligence 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 intelligence agencies concerned. Indeed, in many cases the matters of concern are drawn to the Office's attention by the relevant intelligence agencies themselves.

In general terms, the intelligence 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 intelligence 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 intelligence 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 our previous Annual Report, the COVID-19 pandemic disrupted the work of the Office last year and continued to have an impact on work in the year presently under review. While the Office's corporate and enabling services have been 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 was resumed and

completed as restrictions eased in the Australian Capital Territory (ACT). 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. I thank staff for their dedication and flexibility in response to changing circumstances over the year.

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. Current policy settings, reflected in the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 and the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 – both of which were introduced in the House of Representatives during the year under review – would involve an additional 3 agencies coming within the oversight jurisdiction of the Office, as to either the whole or some part of their functions. Although the Office would be required to undertake its expanded role in these respects upon the commencement of the relevant amendments, this had not occurred during the year under review. At the same time, the Office had to make an early, anticipatory, start to the engagement of the additional staff that the amendments would make necessary, involving as it did, and does, the unavoidable, but lengthy, process of security clearance.

As was the case last year, in this reporting year there were changes to the legislative framework affecting intelligence agencies within IGIS's jurisdiction. The Office was consulted on the development of these proposals for change, and continues to contribute 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 that support 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 (PJICIS) through written submissions and appearances by the Inspector-General at Committee hearings.

Engagement with our portfolio department, the Attorney-General's Department (AGD), 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. The Office works very closely at many levels with the AGD on a range of legal and corporate matters. Additionally, meetings were held with the Australian Commission for Law Enforcement Integrity and the Office of the Commonwealth Ombudsman (OCO) 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, on a project related to the COVIDSafe app, and provided 2 reports on the project to the Information Commissioner which were subsequently publicly released. 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 (FIORC) conference was cancelled for the second time due to COVID-19 travel restrictions.

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 COVID-19. 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 Office recruited staff with experience and expertise in several corporate areas, including governance, human resources and information governance. 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 approximately 55 staff has not yet been reached for a number of reasons, including those related to the necessary but lengthy security clearance process. However, the emphasis that the Office places on recruitment and retention strategies is expected to bear fruit with several new starters expected to commence early in the 2021–22 reporting period.

Finally, shortly before this Report went to print, the Office received the very sad news of the passing of the Hon Margaret Stone AO FAAL. Ms Stone's contribution to oversight, to domestic and international collaboration between oversight agencies, and to the thinking about the legal framework governing intelligence agencies and oversight was considerable. Ms Stone led the Office through its first major growth phase to set a very high standard of scholarship and rigour, and was highly regarded by staff in the Office and in the broader national security community. Her significant achievements have been recognised by many through the condolences expressed to this Office and elsewhere.

# THE ROLE OF THE IGIS

The Inspector-General provides independent assurance for the Prime Minister, senior ministers, Parliament and the public as to whether the intelligence agencies are acting with legality and propriety, and that activities are consistent with human rights. The Inspector-General 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 (ONI)
- Australian Security Intelligence Organisation (ASIO)
- Australian Secret Intelligence Service (ASIS)
- Australian Signals Directorate (ASD)
- Australian Geospatial-Intelligence Organisation (AGO)
- Defence Intelligence Organisation (DIO).

IGIS undertakes proactive inspections and conducts formal independent inquiries of its own motion, in response to complaints or public interest disclosures (PIDs) or at the request of relevant ministers and the Prime Minister. IGIS may also conduct an inquiry into an intelligence or security matter relating to another Commonwealth agency. During inquiries, the IGIS Act provides for the use of coercive powers, immunities and protections.

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

IGIS considers 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, by a credible and independent oversight body. IGIS will continue to make public as much of its work as is possible within appropriate security constraints.

Figure 1.1: IGIS key activities



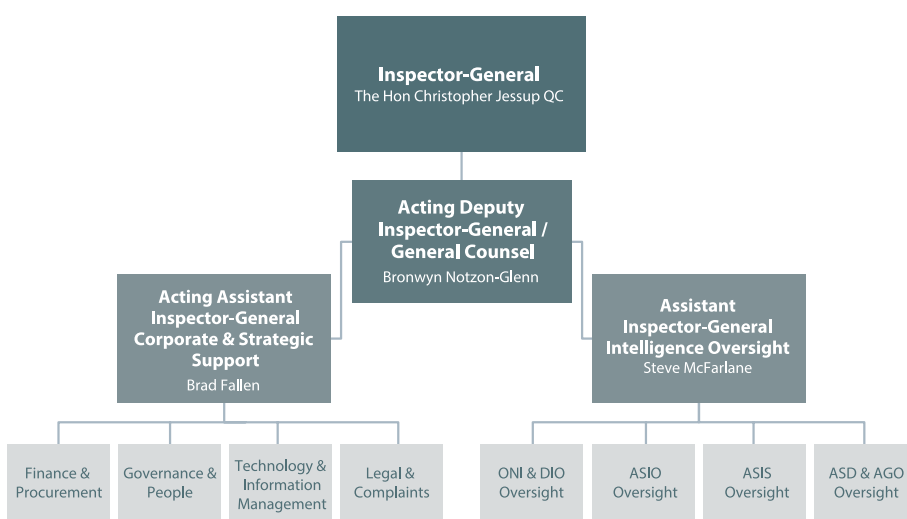
# ORGANISATIONAL STRUCTURE

As of 30 June 2021, the Inspector-General is supported by a Deputy Inspector-General and 2 Assistant Inspectors-General. The Deputy Inspector-General provides strategic leadership on the operations of the agency including oversight activities, legal issues, governance and strategy, and parliamentary matters.

The Assistant Inspector-General Intelligence Oversight leads the teams responsible for oversight programs of the intelligence agencies within IGIS's jurisdiction.

The Assistant Inspector-General Corporate and Strategic Support leads the teams responsible for governance, corporate capability, legal, and complaints handling.

**Figure 1.2: IGIS organisational structure at 30 June 2021**



## OUTCOME AND PROGRAM STRUCTURE

The Office has one outcome, as noted in the 2020–21 Portfolio Budget Statement (PBS).

The IGIS 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.

# PURPOSE

The IGIS Corporate Plan 2020–21 describes the purpose of IGIS which reflects the objectives contained in s 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 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 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.

In addition, the PID Act requires the Inspector-General to:

- receive, and where appropriate, investigate disclosures about suspected wrongdoing within the intelligence agencies
- assist current or former public officials employed, or previously employed, by intelligence agencies, in relation to the operation of the PID Act
- assist the intelligence agencies in meeting their responsibilities under the PID Act, including through education and awareness activities
- oversee the operation of the PID scheme in the intelligence agencies.

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



# THE INTELLIGENCE AGENCIES

## 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.

## 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).

## 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 *Intelligence Services Act 2001* (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.

## 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.

## 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.

## 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 the Mandate issued by the Secretary for Defence and the Chief of Defence Force.

The responsible minister for DIO is the Minister for Defence.

# **SECTION TWO**

ANNUAL

PERFORMANCE

STATEMENT

# 2020–21 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 2020–21, 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 QC  
Inspector-General of Intelligence and Security

## RESULTS

IGIS's performance framework is set out in its Corporate Plan 2020–21 and the PBS. In preparing the annual performance statement, IGIS draws data from its corporate record keeping systems.

Where the performance measure has been met, the details are provided in the Analysis section of the Annual Performance Statement.

Figure 2.1: Results against Corporate Plan 2020–21 performance criteria

Performance criteria and criteria source (from Corporate Plan unless indicated)	Performance measures (from Corporate Plan unless indicated)	Result against performance criteria
1.1 Providing ministers with an independent source of information about the activities of Australian intelligence agencies.	IGIS provides ministers with relevant and timely information about the independent oversight activities of IGIS. (Same measure appears in the PBS).	<b>Met</b>
2.1 Providing the Parliament with an independent source of information about the activities of Australian intelligence agencies.	Number and quality of intelligence and security oversight related submissions made to Parliamentary Committees.	<b>Met</b>
	Number of intelligence and security oversight related appearances before Parliamentary Committees.	<b>Met</b>
	To the extent commensurate with our secrecy obligations, the IGIS annual report describes its oversight activities and findings.	<b>Met</b>
	References to IGIS submissions (written and oral) in the reports of the PJCIS and other committees indicate the submissions are seen as relevant and useful (PBS only).	<b>Met</b>

Performance criteria and criteria source (from Corporate Plan unless indicated)	Performance measures (from Corporate Plan unless indicated)	Result against performance criteria
3.1 Providing the public with as much independent information about the work of IGIS and the activities of the Australian intelligence agencies as is commensurate with our secrecy obligations.	To the extent commensurate with our secrecy responsibilities all IGIS inquiries are described on the IGIS website.	<b>Met</b>
	IGIS has a written strategic engagement plan which includes targets for activities.	<b>Partially met</b> – With the movement towards more online activity as a result of the COVID-19 pandemic, IGIS is continuing to develop a public and parliamentary strategic engagement plan, which will include targets for activities.
	Baseline data collected on website use and reviewed biannually to measure number of visits and the ways in which the public contact IGIS regarding a complaint.	<b>Partially met</b> – Collection and analysis of baseline data began in February 2021.
4.1 Effective working relationships with the agencies IGIS oversee.	Agencies proactively disclose relevant information to IGIS in a timely way.	<b>Met</b>
	Agencies respond cooperatively to IGIS suggestions for improving their internal processes.	<b>Met</b>
	The Inspector-General or Senior Executive Service (SES) officers meet at least every 6 months with SES officers from each agency to discuss key issues and arrangements for oversight. (Same measure appears in the PBS).	<b>Met</b>

Performance criteria and criteria source (from Corporate Plan unless indicated)	Performance measures (from Corporate Plan unless indicated)	Result against performance criteria
4.2 Well-developed and effective inspection program.	Where relevant, inspections prompt changes in agency processes and agencies report on improvements.	<b>Met</b>
Inspector-General's comments on any inspection conducted under s 9A of the IGIS Act (s 35(2A) IGIS Act).	An approved inspection plan is in place for agencies within the Inspector-General's jurisdiction. (Same measure appears in the PBS).	<b>Met</b>
Inspector-General's comments on the extent of compliance by ASIS, AGO and ASD with rules made under s 15 of the IS Act (s 35(2B) IGIS Act).		
4.3 Well-developed and effective inquiry capability.	Program of own-motion inquiries and inquiries triggered by inspection findings or complaints.	<b>Met</b>
	100% of inquiry recommendations accepted in that the relevant agency accepts that a substantive issue requiring attention has been identified in the recommendation. (Same measure appears in the PBS).	<b>Met</b>
	All inquiries are conducted in accordance with IGIS legislation and internal inquiry guidelines.	<b>Met</b>

Performance criteria and criteria source (from Corporate Plan unless indicated)	Performance measures (from Corporate Plan unless indicated)	Result against performance criteria
4.4 Well-developed and effective complaint and PID management processes.	90% of complaints acknowledged, triaged and allocated within 5 working days. (Same measure appears in the PBS).	<b>Not met</b> – IGIS responded to 83% of complaints in 5 business days. Further information is available in the Section 2 Analysis section.
	All visa and citizenship complaints managed in line with a complaint management process published on the IGIS website.	<b>Met</b>
	An approved plan is in place for examining intelligence agency handling of visa and citizenship referrals.	<b>Met</b>
	IGIS conducts and arranges education and awareness initiatives on the PID scheme for each intelligence agency within its jurisdiction.	<b>Partially met</b> – COVID-19 restrictions impacted on IGIS's ability to fully meet this measure.
5.1 Appropriate infrastructure and governance.	Premises meet all applicable security accreditation standards.	<b>Met</b>
	Information and Communications Technology (ICT) systems meet all applicable security accreditation standards.	<b>Met</b>
	Implementation of the internal governance review recommendations.	<b>Partially met</b> – The Office has implemented a number of recommendations following an internal governance review in 2020; however all internal policies are yet to be finalised due to resource constraints.



Performance criteria and criteria source (from Corporate Plan unless indicated)	Performance measures (from Corporate Plan unless indicated)	Result against performance criteria
5.2 Effective and efficient support arrangements both internally and externally.	Arrangements including service level agreements in place to provide corporate and property services including payroll, finance and relevant ICT.	<b>Met</b>
	All new records are stored in the electronic records management system except where specific security rules prevent this.	<b>Partially met</b> – IGIS works across 3 ICT systems. An electronic records management system has been implemented on the PROTECTED-level system. Implementation is ongoing on the 2 higher classified systems.
	The case management system is used for 100% of complaints except where specific security requirements preclude this.	<b>Met</b>
5.3 Positive relationships with other integrity agencies.	Meet at least twice per year with other integrity agencies to ensure cooperative arrangements are working efficiently.	<b>Met</b>
	Engagement with other integrity agencies leads to improvements in our processes.	<b>Met</b>
6.1 High performing professional officers.	The Office has a performance management framework that integrates performance expectations and professional development.	<b>Met</b>
	The Office has sufficient officers with the skills necessary to support oversight activities including inspections, inquiries and complaint management, as well as IGIS engagement with the legislative process.	<b>Met</b>

Performance criteria and criteria source (from Corporate Plan unless indicated)	Performance measures (from Corporate Plan unless indicated)	Result against performance criteria
6.2 Recruitment and professional development.	The Office runs at least 10 modules of internal professional development per year.	<b>Met</b>
	All staff participate in an induction program that is completed within the first week and an office orientation program that is completed within 3 months of commencement.	<b>Partially met</b> – One staff member attended the orientation program more than 3 months after commencement due to staff availability.
	The recruitment strategy is reviewed annually to ensure it meets the Office's requirements.	<b>Met</b>
6.3 Office culture and ethos.	IGIS officers comply with Australian Public Service (APS) and security obligations.	<b>Met</b>
	Where flexible working arrangements are utilised they are recorded appropriately and reviewed periodically.	<b>Met</b>
	The Office conducts a staff survey at least once every 2 years, the survey has at least a 90% response rate, and feedback in the survey is addressed.	<b>Met</b>
	Development and implementation of a Diversity and Inclusion Plan and a Reconciliation Action Plan that are appropriate for the Office.	<b>Met</b>

## IGIS PERFORMANCE FRAMEWORK FOR 2021–22

In 2021–22, IGIS will refresh its performance framework, including its objectives and performance measures, to provide a useful tool by which to measure the performance of the work across the agency. The new framework is aligned with IGIS's key activities to create links between its purpose, activities and performance. The IGIS 2021–22 Corporate Plan is available on its website at [www.igis.gov.au/about/corporate-plan](http://www.igis.gov.au/about/corporate-plan). The updated performance criteria and measures will be reported against in future annual performance statements.

# ANALYSIS

## OBJECTIVE 1 – 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. There was no occasion for any such report in 2020–21.

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 2020–21, the Inspector-General wrote to responsible ministers to provide updates regarding IGIS inspection and review activities, the preliminary inquiry into national security classifications, the COVIDSafe app report, legislative change and complaints. The Inspector-General and IGIS officers also met with several staff of responsible ministers to discuss how IGIS conducts inspection and review activities, and to provide relevant updates.

During 2020–21, no requests were made by ministers or the Prime Minister for the Inspector-General to conduct an inquiry under the IGIS Act.

## OBJECTIVE 2 – ASSURING PARLIAMENT

### SENATE ESTIMATES HEARINGS

The then Acting Inspector-General appeared before the Senate Standing Committee on Legal and Constitutional Affairs on 22 October 2020 for Budget Estimates, and responded in writing to 2 questions taken on notice. The Inspector-General was not called to appear before the Additional Estimates hearing on 23 March 2021 or Budget Estimates on 27 May 2021. Following these 2 Estimates hearings, IGIS responded to written questions on notice from members of the Committee.

### PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

The Inspector-General gave evidence in 4 inquiries conducted by the PJCS during the reporting period, relating to the inquiry into proposed legislation concerning Australian intelligence agencies.

- On 3 July 2020, the Inspector-General provided a written submission to the PJCS relating to the review of the Australian Security Intelligence Organisation Amendment Bill 2020. The Inspector-General appeared before the Committee at a public hearing on 10 July 2020. The then Acting Inspector-General provided a supplementary submission on 20 November 2020.

- On 12 February 2021, the Inspector-General provided a written submission to the PJCIS for its review of the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020. The Inspector-General and Acting Deputy Inspector-General appeared before the Committee at a public hearing on 6 May 2021.
- On 26 February 2021, the Inspector-General provided a written submission to the PJCIS for its review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020. The Inspector-General and the Acting Deputy Inspector-General appeared before the Committee at a public hearing on 10 March 2021.
- On 23 March 2021, the Inspector-General provided a written submission to the PJCIS for its review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020. The Inspector-General and Acting Deputy Inspector-General appeared before the Committee at a public hearing on 11 June 2021.

Consistent with established practice, the Inspector-General's submissions made a number of remarks in the context of IGIS's oversight and review role, but did not comment on the policies underpinning the bills.

IGIS also participated in one inquiry conducted by the PJCIS in accordance with its statutory function to review the administration and expenditure of ONI, ASIO, ASIS, AGO, ASD and DIO, including their annual financial statements. The Inspector-General regularly participates in these reviews, providing public submissions and also classified oral evidence when requested by the committee. The Inspector-General's contributions to these inquiries focus on IGIS's findings in relation to each agency during the reporting period, insofar as they are relevant to an agency's administration.

- On 23 December 2020, the then Acting Inspector-General provided an unclassified written submission to the PJCIS for its review of administration and expenditure for the 2019–20 financial year. On 14 April 2021, the Acting Inspector-General appeared at a classified hearing for the Committee's review of the administration and expenditure for the 2018–19 and 2019–20 financial years, and subsequently responded to 4 questions on notice from the committee.

## JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

On 25 February 2021, the Inspector-General provided a written submission to the Joint Committee of Public Accounts and Audit for its inquiry into matters contained and associated with the Auditor-General's Report *Implementation of the Digital Continuity 2020 Policy*, published on 31 October 2019. The Acting Inspector-General appeared before the Committee at a public hearing on 14 April 2021.

## SENATE FINANCE AND PUBLIC ADMINISTRATION LEGISLATION COMMITTEE

On 10 July 2020, the Inspector-General provided a written submission to the Senate Finance and Public Administration Legislation Committee for its review of the Intelligence and Security legislation Amendment (Implementing Independent Intelligence Review) Bill 2020. The Inspector-General did not appear before any hearing on the Bill.

## EVIDENCE TO THE AAT AND THE AUSTRALIAN INFORMATION COMMISSIONER

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

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 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, he or she is not appropriately qualified to do so.

During the reporting period, the Inspector-General received 5 requests for evidence from the Information Commissioner and one request for evidence from the AAT.

## OBJECTIVE 3 – INFORMING THE PUBLIC

A purpose of IGIS 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. IGIS does this by making unclassified information about its activities publicly available where possible, and through other activities such as its engagement program.

During 2020–21, the COVID-19 pandemic affected many of the usual activities that IGIS undertakes in this space, such as presentations at universities and participation on panels. With the movement towards more online activity as a result of the pandemic, and the appointment of a new Inspector-General, the Office has been reviewing its strategic engagement plan. Work on this revised plan will continue in the new reporting period.

### IGIS WEBSITE

In 2020–21, IGIS made improvements to its website content including making more information available about its work, publishing all public submissions and improving the way the information is presented. Ensuring information on the role, functions and activities of IGIS is easily accessible online, to the extent possible with regard to security classification, is a key element of providing public assurance that the Australian intelligence agencies under IGIS jurisdiction are open to scrutiny.

In 2021–22, further planned improvements to the website are intended to make it more user-friendly, easier to navigate and consistent with best practice approaches for website accessibility. To guide these improvements IGIS collects data on how the public interacts with its website, which will be monitored to perform analysis and gain insights as to how improvements can be made.

## PUBLIC OUTREACH ACTIVITIES

IGIS also conducts a program of presentations to the broader community. This includes presentations to groups who have a demonstrated interest in national security and intelligence matters, such as those who study and research in the area or who frequently engage with parliamentary committees on national security oversight and law reform matters. It also includes groups who may have broader interests across human rights, democratic principles, privacy, rule of law and current affairs.

During 2020–21, the COVID-19 pandemic affected many of the usual activities that IGIS would ordinarily undertake in this space. Notwithstanding this and when possible, IGIS spoke at other fora. This included 2 university lectures on the role of IGIS in September 2020 and May 2021 and one presentation to a university organisation in August 2020. Another meeting occurred in November 2020 with the Civil Society Reference Group (more information below).

## CIVIL SOCIETY REFERENCE GROUP

The IGIS Civil Society Reference Group met once during the 2020–21 reporting period.

The key objective of this group is to give civil society groups access to credible unclassified information about the work of IGIS and Australia's intelligence and security agencies; to understand the views of those who work with people directly affected by the work of intelligence and security agencies; to provide a forum to discuss different perspectives about issues relevant to the work of IGIS; and potentially to allow for an unclassified discussion of legal and technical issues with groups who possess expertise in such fields.

The meeting, held in November 2020, was attended by the Joint Councils for Civil Liberties, the Human Rights Law Centre, the Law Council of Australia and the Australian Privacy Foundation.

## OBJECTIVE 4 – INQUIRIES

The IGIS Act provides that the Inspector-General may conduct an independent inquiry into the activities of an intelligence agency either on the Inspector-General's own motion, in response to a complaint, or in response to a ministerial request. Independent inquiries enable the Inspector-General to investigate a matter thoroughly, consider its legality, propriety and appropriate regard for human rights, and make recommendations to remedy any issues identified.

Inquiries are generally conducted in private to allow examination of all classified or sensitive information. At the conclusion of an inquiry, the Inspector-General provides a report with findings and recommendations to the responsible minister. Where an inquiry is in response to a complaint, a written response is given to the complainant. Where possible, an unclassified report or summary is published on the IGIS website.

IGIS reports on inquiries from previous periods where there are outstanding recommendations to be implemented or ongoing activities of interest. The below table covers 2 inquiries from the 2018–19 reporting period and one inquiry from the current reporting period.

**Figure 2.2: Performance indicators – conducting inquiries**

Subject of Inquiry	ASD Matter 2018	ASD Matter 2021	ASIO Matter 2018
<b>Agency</b>	ASD/ASIO	ASD	ASIO
<b>Source</b>	Minister of Defence request	Complaint	IGIS own motion
<b>Date initiated</b>	30 May 2018	07 May 2021	14 February 2018
<b>Date finalised</b>	2 May 2019	Ongoing	14 June 2019
<b>Duration</b>	337 days		485 days
<b>Number of recommendations</b>	5		8
<b>Percentage of recommendations accepted</b>	100%		100%
<b>Percentage of recommendations fully implemented by 30 June 2021</b>	100%		100%

## INQUIRY INTO AUSTRALIAN SIGNALS DIRECTORATE MATTER 2018

As reported in previous annual reports, in May 2019 the Inspector-General completed an inquiry into an ASD matter pursuant to subs 8(2) of the IGIS Act. The inquiry related to the unlawful collection of communications during an operation facilitated by warrants sought by ASIO under the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

The inquiry found that the unlawful interception occurred due to an error made by ASIO in preparing the relevant warrant documentation, combined with a failure by ASD to check the accuracy of the documentation before relying on it. The inquiry also found that ASD's initial reporting of this matter to the Inspector-General and the Minister for Defence was inadequate. The classified inquiry report made 5 recommendations aimed at reducing the risk of recurrence and improving the reporting of any future breaches of the TIA Act. These recommendations were addressed to both ASD and ASIO for implementation.

To meet one of the inquiry recommendations, both agencies reported to the IGIS by October 2019 on their progress in implementing the recommendations. ASIO and ASD finalised all recommendations within the 2020–21 reporting period, and each agency head wrote to the Inspector-General with details of the implementation. This included the establishment of ASD-ASIO joint warrant training, updated processes for reporting incidents, and revised processes to manage warrants and streamline warrant documentation. The Inspector-General is satisfied that implementation of all recommendations is fully completed and IGIS officers will continue to review the effectiveness of changes to policies, practices and staff training through the regular inspection programs.

## INQUIRY INTO AUSTRALIAN SIGNALS DIRECTORATE MATTER 2021

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 inquiry is ongoing.

## INQUIRY INTO AN AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION MATTER

As reported in the 2018–19 annual report, in June 2019 the Inspector-General completed an inquiry into the conduct and details of a multi-faceted, multi-agency foreign intelligence collection operation led by ASIO. The inquiry found significant problems with the planning and execution of the operation, stemming from systemic weaknesses within ASIO's compliance management framework. However, the inquiry also concluded that it was likely most, but not all, of the activities reviewed were lawful. Importantly, there was no evidence of any deliberate wrong-doing by the officers involved in the operation. The issues identified during the inquiry were discussed in the 2018–19 annual report.

The classified inquiry report made 8 recommendations focused on: ASIO establishing a compliance team as a matter of priority; ASIO implementing a compliance training program; improving ASIO's internal provision of legal advice; and ASIO reviewing relevant policies and procedures.

ASIO accepted all 8 recommendations. To meet one of the inquiry recommendations, ASIO reported to IGIS on 30 September 2019 on the progress of implementation of the recommendations. Subsequently, ASIO has provided quarterly progress reports to IGIS, and has also provided updates through high-level meetings between the Inspector-General and senior ASIO officers, and through ongoing compliance reporting. During 2020–21, IGIS conducted additional inspections to review implementation of the inquiry recommendations. IGIS considers the 8 inquiry recommendations to be fully implemented.

## PRELIMINARY INQUIRY INTO THE APPLICATION OF NATIONAL SECURITY CLASSIFICATIONS

The IGIS Act enables the Inspector-General, of their own motion, to make inquiries of the head of an intelligence agency for the purposes of determining whether they are authorised to inquire into an action of the agency or, if authorised, whether they should inquire into that action. Conducted under subs 14(2) of the IGIS Act, such preliminary inquiries enable intelligence agencies to present relevant facts, prior to the Inspector-General making a decision as to whether or not to commence a more comprehensive own-motion inquiry.

In August 2020, the PJCS recommended that IGIS undertake a preliminary inquiry into the application of national security classifications in intelligence agencies.

The then Acting Inspector-General decided to commence a preliminary inquiry on 7 October 2020 into each of the intelligence agencies in IGIS jurisdiction about the application of national security classifications. The preliminary inquiry included a review of policy and procedures, a survey to understand how national security classification decisions are made, and a sample inspection of classified material. No significant issues were identified. On 26 February 2021, the Inspector-General provided the PJCS a report of the preliminary inquiry, in which he made 2 recommendations: ensuring written guidance about security classifications is up to date and accessible; and regularly reviewing internal training so that staff are adequately supported to make classification decisions. It was not, however, determined that a formal inquiry was necessary in relation to this matter. The preliminary inquiry report is available on the IGIS website.

As part of ongoing inspection activities IGIS officers will continue to review national security classification decisions, training, and written guidance.



## OBJECTIVE 4 – INSPECTIONS

Section 35 of the IGIS Act requires the Inspector-General to report annually on inspections conducted during the reporting period and on the extent of compliance by certain agencies with privacy rules.

IGIS regularly inspects intelligence agency activities to determine if each agency is acting in accordance with its statutory functions, and is complying with any guidance provided by the responsible minister and with its internal policies and procedures. Inspections enable IGIS to monitor the activities of agencies and to identify concerns before they develop into systemic problems that could require major remedial action.

IGIS has a risk-based approach to its inspection program, targeting high risk activities and activities with the potential to affect the lives or rights of Australian persons. Accordingly, the IGIS inspection program has a greater focus on the activities of ASIO, ASIS, ASD and AGO, each of which has intrusive powers and investigative techniques. Inspections of ONI and DIO are generally directed to ensuring that their assessments comply with their respective privacy rules and guidelines, and that their independence is not compromised. IGIS takes into account many factors, including an intelligence agency's internal control mechanisms as well as its history in compliance and reporting.

### INSPECTION OF ONI ACTIVITIES

The functions and powers of ONI are set out in the ONI Act. These include:

- to lead, and evaluate matters relating to, the NIC
- to provide advice to the Prime Minister on national intelligence priorities, requirements and capabilities
- to assemble, correlate and analyse information relating to international matters of political, strategic or economic significance to Australia (all source assessment)
- to collect, interpret and disseminate information relating to these matters that is accessible to any section of the public (open-source assessment)
- to cooperate with and assist intelligence agencies and prescribed authorities.

The ONI Act also excludes specific matters from ONI's functions: ONI cannot direct the operational activities of NIC agencies, nor direct the content of or conclusions reached in agency reporting, and it cannot inquire into complaints about the activities of agencies.

IGIS's oversight of ONI focuses on those activities most likely to raise legality, propriety or human rights concerns, including risks to the privacy of Australian persons. Historically, IGIS inspections have focused on ONI's all source assessment functions, however the range of inspection matters has now broadened in recognition of ONI's intelligence enterprise management role and its adoption of some niche intelligence capabilities.

There are biannual meetings between the Inspector-General and Director-General of National Intelligence, senior IGIS and senior ONI officers to discuss oversight issues. Inspections are aided by regular engagement with ONI's Governance and Accountability section and General Counsel, and other areas within ONI as required. Scheduled inspection activities are supplemented by briefings on emerging issues of interest, and proactive review of programs to evaluate risk. IGIS also reviews relevant ONI policies and procedures to determine whether they appropriately address compliance issues.

## COMPLIANCE WITH PRIVACY RULES

Under s 53 of the ONI Act, the Prime Minister must make rules regulating the collection and communication of identifiable information regarding Australian persons. These Privacy Rules are published on the ONI website. ONI must protect the privacy of Australian citizens and permanent residents in accordance with the Privacy Rules; it can only collect or communicate this information in specific circumstances where needed to properly perform its functions. Records of these instances are kept by ONI and audited annually by IGIS. To provide further independent assurance, IGIS officers monitor ONI reporting for references to Australian persons and use this to cross-check provided material.

In 2020–21, an IGIS inspection of compliance with the Privacy Rules identified 2 ONI products where the rules should have been applied but were not. IGIS determined that the failure to apply the rules was not systemic. There were also instances where administrative requirements were not completed within the timeframes required by ONI policy. IGIS was advised that different working arrangements for ONI staff due to the impact of the COVID-19 pandemic was a significant factor in this delay. ONI has since updated its policies to reduce the potential for similar future incidents.

## ENSURING ANALYTIC INTEGRITY

Subsection 12(2) of the ONI Act affirms that ONI is not subject to direction on the subjects or judgements of its intelligence assessments. IGIS conducts analytic integrity inspections of ONI assessments, examining large numbers of published products and associated records to confirm independence and analytic rigour. In 2020–21, IGIS found no areas of concern and considered that the majority of records reviewed were of a high standard.

## THE COLLECTION OF OPEN-SOURCE INFORMATION

As well as traditional all source assessment, ONI has placed increasing focus on collecting and analysing open-source intelligence through its Open Source Centre. A 2020–21 IGIS inspection of ONI's open-source activities found a strong professionalised foundation for open-source analysis. ONI has developed a comprehensive Open Source Collection Framework, detailed training and practical support and guidance to ONI staff undertaking collection activities. IGIS reviewed a number of these records and confirmed that only authorised collection staff were used and only publicly available information was sourced.

## LEADING THE NATIONAL INTELLIGENCE COMMUNITY

During 2020–21, IGIS conducted its first inspection into the functions of ONI relating to leading the NIC. The review focused on foreign engagement, and intelligence coordination and evaluation. IGIS found no legality or propriety concerns with these activities.

## INSPECTION OF ASIO ACTIVITIES

The functions of ASIO are set out in s 17 of the ASIO Act. ASIO undertakes a number of activities in the performance of its functions. These include:

- intelligence collection
- intelligence communication
- provision of security advice to ministers and Commonwealth authorities in relation to their functions and responsibilities
- provision of security assessments to states and states authorities

- provision of furnishing advice to ministers and Commonwealth authorities about protective security
- foreign intelligence collection
- co-operation with and assistance to other agencies.

During 2020–21, IGIS conducted a range of inspections of ASIO's activities. Given the scope of ASIO functions, IGIS implements a risk-based approach to inspections. IGIS prioritised reviewing ASIO's use of special powers under the ASIO Act and the TIA Act and other intelligence collection activities; its procedures relating to the quarantine and deletion of incidentally collected COVID app data and unlawfully intercepted information; and its security assessments and advice to ministers on security matters.

During 2020–21, IGIS inspections focused on:

- the legality of ASIO's activities
- the propriety of the investigative activities being proposed and undertaken
- compliance with ministerial guidelines
- compliance with internal policies and procedures.

IGIS conducted inspections using a variety of methodologies, including thematic reviews, risk-based sampling and random sampling. IGIS officers have direct access to the relevant ASIO information technology and records management systems to inspect and review all records. Although the approach IGIS takes to each inspection varies, it generally involves discussions with relevant officers, review of ASIO's corporate records, and formal reporting of IGIS findings at the conclusion of the inspection. The level at which ASIO is notified of inspection outcomes depends on the significance of the findings, with the Inspector-General writing to the Director-General of Security in instances where significant legality or propriety issues are identified.

IGIS also independently reviews all ASIO compliance incident reports relating to breaches of legislation or the Minister's Guidelines, or noncompliance with ASIO internal policies and procedures. Where necessary, IGIS may conduct its own investigation. The Inspector-General receives ASIO's periodic compliance reports and is briefed, as appropriate, on individual compliance incidents.

Inspections and other oversight activities are supplemented by briefings on various matters throughout the year, either at the request of IGIS, or as provided by ASIO. These briefings allow IGIS to stay abreast of emerging issues, or to follow up observations from inspection activities. There are regular meetings between the Inspector-General and the Director-General of Security as well as tri-annual meetings between the Inspector-General, senior IGIS and senior ASIO officers.

## INSPECTION OF ASIO WARRANTS

Warrants for the exercise of ASIO's intrusive powers, including searches, computer access, surveillance devices and compulsory questioning, can be issued under the ASIO Act. ASIO may also obtain warrants to intercept telecommunications under the TIA Act. All ASIO warrants are authorised by the Attorney-General.

In 2020–21, IGIS changed its approach to warrant inspections, focusing on particular warrant types as well as the reporting of warrant breaches to the Attorney-General. Across these inspections, IGIS identified a number of general record keeping issues.

Using a newly developed methodology, IGIS focused on ASIO's use of search powers under the ASIO Act. No matters of legality or propriety were identified. However, the inspection identified a need for future focus on how ASIO's decisions about warrant operations are captured in records.

IGIS also commenced an inspection focused on ASIO's use of surveillance devices under the ASIO Act. This inspection remains underway and will be reported on in the 2021–22 annual report.

A small number of compliance incidents were reported to the Attorney-General, and IGIS identified instances where these reports were noncompliant with ASIO's internal policies.

Through the year, ASIO notified IGIS of breaches and other issues relating to warrants issued under the ASIO Act and the TIA Act. A detailed summary of compliance incidents reviewed by IGIS is included later in this section.

### COMPULSORY QUESTIONING

In December 2020, ASIO's compulsory questioning powers, as set out in the ASIO Act, were amended by the *Australian Security Intelligence Organisation Amendment Act 2020*. The amended powers enable ASIO to seek either an adult questioning warrant or, in the case of a person aged between 14 and 18 years, a minor questioning warrant, from the Attorney-General. ASIO can seek an adult questioning warrant in relation to espionage, politically motivated violence or acts of foreign interference. A minor questioning warrant can only be sought in relation to politically motivated violence. The amendments removed the power to detain a person for up to 7 days, but retain an apprehension power, which allows the police to apprehend a person in order to bring them immediately before a prescribed authority for questioning.

The questioning warrant framework provides for IGIS oversight, including that the Inspector-General may be present at the questioning or apprehension of a person. Should the Inspector-General inform the prescribed authority of a concern about impropriety or illegality in connection with the exercise of powers under the warrant, the prescribed authority must ensure the concern is addressed satisfactorily. A person being questioned may make a complaint to IGIS, the Commonwealth Ombudsman and relevant police complaints agencies at any time, and must be provided with the facilities to do so.

A written statement of procedures to be followed in the exercise of authority under a questioning warrant must be approved by the Attorney-General pursuant to s 34AF of the ASIO Act. IGIS must be consulted in the preparation of this statement.

IGIS received several briefings from ASIO on its proposed use of the compulsory questioning powers, and was consulted on development of the statement of procedures and ASIO's internal policy and procedures. For each questioning warrant issued by the Attorney-General, ASIO provided the requisite notifications and information to IGIS. The Inspector-General attended the questioning sessions conducted during the reporting period. The Inspector-General did not raise any concerns about impropriety or illegality during these questioning sessions.

Following questioning conducted pursuant to a questioning warrant, ASIO notified IGIS of a potential breach of s 34DP of the ASIO Act concerning the video recording of proceedings. IGIS will review the matter once ASIO concludes its investigation.

## 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. The ASIO Act does not specify a timeframe for the provision of these reports. However, ASIO has developed a policy that requires an initial notification within 72 hours of the use of force, to be followed by more detailed information within 10 days. No notifications of use of force were received during the reporting period.

## TECHNICAL COLLECTION, RETENTION AND DELETION OF DATA

Each year IGIS conducts an inspection to provide assurance that the deletion of data from ASIO systems has been effective and that no traces of information remain unintentionally. The scope of this inspection includes data that has been deleted relating to a compliance incident reported to IGIS as well as a sample identified by IGIS during inspection activities. During 2020–21, IGIS found 9 instances where data reported to have been deleted by ASIO was still available on ASIO systems.

Five of these instances were caused by a technical issue that affected deletion protocols run during a specific time period. In these instances ASIO officers had deleted relevant data and received confirmation that the deletion was successful, but some data remained. IGIS verification of data deletion through routine inspection resulted in this technical issue being identified and remediated.

The remaining 4 instances were attributed to failures of policy and procedure, and ASIO has advised it is now conducting a body of work to improve data management practices, including taking steps to better embed compliance and assurance measures into relevant policies and procedures. IGIS will continue to monitor and assess the effectiveness of ASIO's policies and procedures for technical collection, retention and deletion of data through routine inspection activities.

## SPECIAL INTELLIGENCE OPERATIONS

Special intelligence operation (SIO) powers allow ASIO to seek authorisation from the Attorney-General to undertake activities that would otherwise be unlawful. Where the circumstances justify the conduct of an SIO, ASIO may seek these authorisations to assist in the performance of its special powers functions. 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 an SIO.

The ASIO Act also requires ASIO to provide to the Attorney-General and the Inspector-General a written report on each SIO. IGIS reviewed each authorisation and report immediately following notification to the Inspector-General. In addition, IGIS conducted periodic inspections of ASIO's SIOs. IGIS observed that ASIO responded to feedback provided during earlier inspections and considers ASIO's management of SIOs to be appropriate.

## HUMAN SOURCE MANAGEMENT

ASIO activities include collection of intelligence through human sources. During the reporting period, IGIS officers reviewed ASIO human source case files and met with ASIO officers to discuss related activities. IGIS observed that ASIO responded to feedback provided during earlier inspections and considers that ASIO is managing its human sources appropriately.

ASIO notified IGIS of one incident involving noncompliance with its internal policy for human sources. IGIS reviewed this matter and was satisfied with ASIO's response to the incident.

## INSPECTION OF INVESTIGATIVE CASES

IGIS regularly reviews ASIO's investigative cases. IGIS's 2020–21 inspections identified a number of matters that did not breach legislation but were noncompliant with ministerial guidelines or with internal policy and procedure. ASIO had reported approximately 20 per cent of these matters. ASIO has taken a number of steps to improve compliance, but IGIS has indicated that it expects more proactive reporting given ASIO has the capacity to detect most instances via system generated reporting.

## ANALYTIC RIGOUR AND INTEGRITY

ASIO produces a range of analytic products including security assessments, applications for warrants, investigative reviews and published products. Some products have greater potential to intrude into the privacy of Australians, and others may adversely affect the interests of individuals. For example, an adverse security assessment may recommend that the minister take an action that would be prejudicial to the interests of the person, such as cancelling their passport.

IGIS considers ASIO's analytic rigour and integrity across a range of inspections, and conducts a dedicated analytic products inspection on an annual basis. In this period, IGIS found variability in the way ASIO referenced material relied upon as the basis of assessments across a range of warrants, security assessments and analytic products. As a result of IGIS findings, ASIO has undertaken to update its internal policies and procedures to support improved practice. IGIS will consider the effect of these updated policies and procedures in future inspections.

## INSPECTION OF ADVERSE AND QUALIFIED SECURITY ASSESSMENTS

Security assessments issued by ASIO can result in administrative decisions, such as cancelling a visa or passport, which may significantly affect the liberty of the subject of the assessment.

In 2020–21, IGIS reviewed a sample of cases where ASIO issued prejudicial (adverse or qualified) security assessments. The inspections focused on cases where the subject of the assessment did not have review rights available under Part IV of the ASIO Act or under the jurisdiction of the Independent Reviewer of Adverse Security Assessments.

IGIS found that the majority of the inspected security assessments were well referenced and preceded by thorough investigation to form the basis of the assessment, with due consideration to procedural fairness. IGIS was satisfied with ASIO's initial response to a small number of matters identified for ASIO's further attention and will continue to examine these matters in future inspections.

A review of one qualified assessment gave rise to questions about ASIO's broader policies and procedures for interacting with minors. IGIS will conduct an inspection focused on ASIO's interaction with minors in 2021–22.

## BREACHES OF SECTION 38 OF THE ASIO ACT BY RECEIVING AGENCIES AND/OR MINISTERS

In certain circumstances, subs 38(1) of the ASIO Act requires an agency and/or minister that receives an adverse or qualified security assessment from ASIO in respect of a person to give, within 14 days, written notice to that person, including a copy of the assessment and information concerning the person's right of appeal to the AAT. IGIS has reported breaches

of subs 38(1) in previous annual reports, and in the last reporting period noted that ASIO had contributed to policies and guidance intended to minimise the likelihood of future breaches by receiving agencies and/or ministers. No breaches of subs 38(1) of the ASIO Act were reported in 2020–21.

## INSPECTION OF TEMPORARY EXCLUSION ORDERS

The Minister for Home Affairs can make temporary exclusion orders preventing a person from entering Australia for a period of up to 2 years pursuant to the *Counter-Terrorism (Temporary Exclusion Orders) Act 2019*. Subsection 10(2) of that Act sets out the circumstances in which the minister may make a temporary exclusion order, including where ASIO has assessed the person to be directly or indirectly a risk to security (within the meaning of the ASIO Act) for reasons related to politically motivated violence (within the meaning of the ASIO Act).

Inspections during the reporting period identified a need for ASIO to capture its role in the temporary exclusion order process in formal written procedures. Other matters identified by IGIS remained under consideration at the end of the reporting period.

## MINISTERIAL SUBMISSIONS

In 2020–21, IGIS inspected a number of submissions made by ASIO to the Attorney-General and the Minister for Home Affairs. These submissions provide information on current operations undertaken by ASIO and emerging issues. IGIS reviews submissions to ensure that the information provided is timely and appropriate, and that they provide accurate information to the minister and Attorney-General on relevant matters.

IGIS found that the majority of submissions provided an accurate, balanced and complete picture to the relevant minister. However, IGIS also identified a small number of instances where there appeared to be discrepancies between how certain information was presented to the Attorney-General and how it was assessed in ASIO's internal documents. These matters remained under consideration by IGIS at the end of the reporting period.

## USE OF TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) ACT 2018 POWERS

In December 2018, the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* granted ASIO new powers to obtain industry assistance under the TIA Act. Under this legislation, ASIO is required to notify the Inspector-General formally within 7 days of a request or notice being given. The changes also granted ASIO new powers in relation to requests for voluntary assistance.

IGIS reviewed each use of these powers through its inspection program. IGIS identified some concerns around ASIO's record keeping of the Director-General's decision to issue an industry assistance request or notice. IGIS also identified a need for ASIO to develop internal policy guidance on the consideration of proportionality of industry assistance powers in order to comply with the Minister's Guidelines. IGIS is satisfied with the steps ASIO is taking to address these matters, and will continue to monitor ASIO's procedures and activities around the use of these powers.

In addition to industry assistance powers, the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* amended ASIO's powers under the ASIO Act in relation to computer access and access to data. IGIS inspects ASIO's use of these powers as part of its inspection program for computer access warrants and the technical collection, retention and deletion of data.

## ASIO'S EXCHANGE OF INFORMATION WITH AUSTRALIAN GOVERNMENT AGENCIES

ASIO may exchange information with certain other Australian Government agencies. IGIS reviews and inspects the exchange of sensitive personal information.

### ACCESS TO TAXATION INFORMATION

Section 35570 of Schedule 1 to the *Taxation Administration Act 1953* provides that a taxation officer authorised by the Commissioner of Taxation or delegate may disclose protected information to an authorised ASIO officer if the information is relevant to the performance of ASIO's functions. This access to sensitive information is further governed by a memorandum of understanding between the Commissioner of Taxation and the Director-General of Security, the Minister's Guidelines and ASIO's internal guidelines and procedures. ASIO rarely requests access to this type of information.

During 2020–21, IGIS inspected ASIO's access to sensitive tax information in the previous financial year 2019–20. IGIS did not identify any concerns.

In the next reporting period, IGIS will inspect ASIO's access to taxation information for the financial year 2020–21 and review 3 instances of noncompliance reported by ASIO, where information was sought outside the requirements and delegated authorities of ASIO's memorandum of understanding with the Commissioner of Taxation.

### ASIO EXCHANGE OF INFORMATION WITH FOREIGN AUTHORITIES

The ASIO Act authorises ASIO to provide and to seek information relevant to Australia's security, or the security of a foreign country, from authorities in other countries. ASIO may also cooperate with foreign authorities approved by the responsible minister. ASIO has policies and procedures for the communication of information on Australians and foreign nationals to approved foreign authorities.

In 2019–20, IGIS conducted a specific inspection of ASIO's exchange of information with foreign authorities, having considered this issue through other inspection activity for several years. IGIS found that ASIO has frameworks in place to manage the potential human rights implications of disclosure, but there was scope for improvement in these frameworks. IGIS suggested measures to ensure that ASIO senior management oversight is directed towards areas of highest risk and that better guidance is provided to decision-makers to support their consideration of human rights issues. In response to matters raised by IGIS, ASIO updated its internal guidance. In 2020–21, IGIS conducted a further inspection of ASIO's policies and procedures governing foreign liaison and information exchange, including changes made in response to the earlier inspection. IGIS concluded it was insufficiently assured that these policies and procedures are effective. ASIO has undertaken to further refine its policies and procedures and IGIS intends to conduct further inspection activity during 2021–22.

ASIO notified IGIS of an incident where information from a foreign partner was potentially shared with other Five Eyes partner agencies outside the agreed terms governing sharing of this information. Upon identifying the issue, ASIO conducted a review and identified several products that included this information. ASIO removed partner agency access to the identified products. ASIO is currently working with the foreign partner to address this incident and implement measures for future information sharing. IGIS is satisfied with ASIO's proposed remediation action.



## INTERNAL SECURITY INSPECTION

IGIS conducts periodic inspections to assess whether ASIO manages internal security investigations into its officers appropriately, including cases where the investigation could result in the officer having their security clearance revoked (a precondition for employment at ASIO). IGIS did not identify any issues of concern in cases reviewed during the reporting period.

## REVIEW OF COMPLIANCE INCIDENTS

IGIS regularly engages with ASIO's compliance directorate on compliance matters arising from IGIS inspection activities and identified compliance incidents. For all compliance incidents that meet the threshold for proactive reporting to IGIS, the compliance directorate investigates the matter and provides IGIS with a copy of the compliance incident report. IGIS independently reviews all compliance incidents and may seek additional information or undertake further investigation. In addition, IGIS monitors the implementation of remediation action identified in compliance incident reports through the regular inspection program.

Matters that do not meet the threshold for proactive reporting to IGIS are included in ASIO's periodic compliance reports; a copy of this report is provided to the Inspector-General. ASIO also reports matters to IGIS on propriety grounds. In these circumstances, ASIO has assessed that there was no breach of legislation or other non-compliance but considers it would be proper for IGIS to be informed of the matter. As with other compliance incidents, IGIS reviews the matter and may seek additional information or undertake further investigation. In addition, IGIS considers ASIO's remediation action; frequently this entails amendments to ASIO's internal policies and procedures, to provide greater clarity for ASIO officers.

During the reporting period, ASIO concluded its review of a number of matters that remained outstanding at the end of 2019–20. Separately, ASIO reported a number of matters identified during the reporting period that met ASIO's threshold for notification to IGIS. These reports included early notification of some incidents that were ultimately confirmed to be compliant and also notification of incidents that resulted from events outside ASIO's control but which ASIO believed should be notified to IGIS in the interests of transparency.

## INCIDENTS RELATING TO INTERCEPTION WARRANTS UNDER THE TIA ACT

Several breaches of the TIA Act relating to interception warrants remained under review at the end of last the reporting period. The outcomes of these matters are discussed below.

## FINALISATION OF TIA ACT INCIDENTS REPORTED IN 2019–20

### INTERCEPTION UNDER SECTION 11B WARRANTS OF THE TIA ACT

Subsection 11D(5) of the TIA Act requires that the Director-General must not request the issue of a warrant under s 11A, 11B or 11C for the purpose of collecting information concerning an Australian citizen or permanent resident. ASIO notified IGIS of a potential breach of subs 11D(5) of the TIA Act relating to a warrant issued under s 11B of that Act, where services added to the warrant after it was authorised were subsequently identified to be those of an Australian permanent resident. Having identified this issue, ASIO immediately ceased interception of these services. ASIO reviewed the matter and, following a request from IGIS, provided detailed advice in May 2021. Following consideration of the incident, the Inspector-General wrote to the Director-General of Security to outline his views. The Inspector-General determined that IGIS would not conduct a further review of this matter based on the particular circumstances of the case.

In addition, ASIO notified IGIS about a propriety issue concerning a named person warrant where data that was lawfully collected under the warrant, but that was intended to be deleted from ASIO holdings, was not deleted. This matter remained under review by ASIO at the end of 2019–20. In May 2021, ASIO advised it had concluded that this incident was a breach of s 10.4 of the Attorney-General's Guidelines and that all relevant data collected under the warrant should be deleted. ASIO subsequently advised that this data had been deleted. IGIS has reviewed the matter and is satisfied with ASIO's assessment and subsequent remediation action.

### APPLICATION OF SUBSECTION 11B(2) OF THE TIA ACT

ASIO advised IGIS that it had identified an issue regarding the application of subs 11B(2) of the TIA Act. Subsection 11B(2) requires ASIO to advise the Attorney-General of the details of telecommunications services used by the subject of a warrant application, to the extent these details are known to ASIO. This matter involved a specific incident that was the subject of reporting to IGIS, as well as consideration of broader policy and legal questions about subs 11B(2) of the TIA Act. The matter remained under review at the end of 2019–20. In December 2020, ASIO advised that it had finalised its review of the specific incident, and concluded there was no breach of the TIA Act in that particular warrant. IGIS has reviewed the matter and is satisfied with ASIO's assessment. IGIS notes that ASIO continues to consider the broader policy and legal implications of this matter.

### BREACHES OF SUBSECTION 7(1) AND S 13 OF THE TIA ACT

Subsection 7(1) of the TIA Act prohibits interception of communications passing over a telecommunications system. However, subs 7(1) does not apply in certain circumstances, including where a warrant is in place. Section 13 requires ASIO to ensure that interception of communications under a warrant is discontinued where the grounds on which the warrant was issued cease to exist prior to expiration of the warrant, and to advise the Attorney-General accordingly. Subsection 17(1) requires ASIO to provide a report to the Attorney-General within three months after the expiration of the warrant. ASIO initially notified IGIS of breaches of subs 7(1), s 13 and subs 17(1) of the TIA Act concerning several related warrants issued under s 9 of the TIA Act. These matters remained under review at the end of 2019–20. Following additional analysis and legal review, ASIO provided an updated notification to IGIS in November 2020, which advised that it considered that the breaches were limited to subs 7(1) and s 13 of the TIA Act. IGIS has subsequently considered ASIO's assessment of these breaches and agrees with its conclusions. IGIS is satisfied with measures implemented by the relevant work area to reduce the risk of future breaches of s 7 of the TIA Act and promote compliance with the requirements of s 13.

## BREACHES OF SUBSECTION 7(1) OF THE TIA ACT

ASIO notified IGIS of a breach of s 7 of the TIA Act where human error resulted in a service that had been disconnected being included on a s 11B warrant. The error was identified several months later when the service was reconnected to a different subscriber. ASIO immediately requested that interception be discontinued and requested deletion of data that had been collected. ASIO's review of the matter concluded that no breaches occurred during the period in which the service was disconnected. However, for a period of several days following the service being reallocated to another subscriber, breaches of s 7 and 63 of the TIA Act occurred. In response to this incident, ASIO advised that the relevant work area had implemented additional measures to minimise the risk of future breaches of this nature. IGIS has reviewed this incident and is satisfied with ASIO's assessment and remediation action.

ASIO notified IGIS of an incident relating to a warrant issued under s 25A of the ASIO Act, where a valid authorisation under subs 24(2) of the ASIO Act was not in place when the warrant was executed. The incident arose because the senior officer who signed the subs 24(2) authorisation was not authorised under subs 24(3) to do so. ASIO subsequently concluded that the incident was a breach of subs 7(1) of the TIA Act. ASIO has introduced additional verification checks into its warrant authorisation process to mitigate the likelihood of a future incident of this nature. IGIS has reviewed this matter and considers ASIO's assessment of the incident and remediation action to be appropriate.

ASIO notified IGIS of an incident concerning a warrant issued under s 9 of the TIA Act. In this case, the service was disconnected after the subscriber checks for the service had been completed but before the Attorney-General signed the warrant. Disconnection of the service was not identified until documentation for a new warrant was being prepared. A limited amount of data was collected in this period. ASIO assessed that the incident did not result in a breach of subs 7(1) of the TIA Act due to the nature of the intercepted data, which was subsequently deleted. IGIS is satisfied with ASIO's assessment and remediation action.

As discussed above, each year IGIS conducts an inspection to provide assurance that the deletion of data from ASIO systems has been effective and that no traces of information remain. During this inspection, IGIS identified one breach of s 7 of the TIA Act that had been identified and remedied by ASIO but, due to an oversight, not reported to IGIS or the Attorney-General. The incident related to 2 services that had been intercepted under an earlier warrant but were not disconnected under the subsequent warrant, resulting in unlawful collection. IGIS assessed that it was an isolated incident and was satisfied with ASIO's remediation, which included appropriate reporting to the Attorney-General.

## BREACH OF SUBSECTION 7(1) AND S 13 OF THE TIA ACT

ASIO notified IGIS of a breach of s 7(1) and s 13 of the TIA Act relating to 2 warrants issued under s 9 of the TIA Act. IP address subscriber checks indicated that the service was no longer being used by the subject of the warrants at the time the warrants were issued. The results of these checks were not reviewed before the Attorney-General signed the warrants. Once identified, data collection was ceased and a request for data deletion was made. In its review, ASIO determined that the grounds for the 2 warrants had ceased to exist at the time the warrants were authorised, resulting in a breach of s 7(1) of the TIA Act. In addition, ASIO failed to notify the Attorney-General that the grounds for the warrants had ceased to exist for 2 months, breaching the requirements of s 13 of the TIA Act and not complying with ASIO's internal policy. IGIS has reviewed this incident and is satisfied with ASIO's assessment and remediation action.

## POTENTIAL BREACH OF SECTION 13 OF THE TIA ACT

In June 2021, ASIO notified IGIS of an incident that it considered a potential breach of s 13 of the TIA Act. This matter remains under review by ASIO and IGIS will consider ASIO's response following its review.

## POTENTIAL BREACH OF SUBSECTION 15(7) OF THE TIA ACT

ASIO notified IGIS of an incident where 2 warrants may not have been served on the authorised representative of a carrier as required by subs 15(7) of the TIA Act. This matter remains under review by ASIO and IGIS will consider ASIO's response when it is received.

## INCIDENTS RELATING TO SPECIAL POWERS UNDER THE ASIO ACT

ASIO notified IGIS of a potential breach of p 25A(4)(ba) and s 18 of the ASIO Act. The incident arose as a result of human error when ASIO's technical systems were configured to receive data under a particular warrant. The configuration error meant that data collected in relation to a telephone service was incorrectly stored in ASIO's data holdings and subsequently forwarded to ASD. This matter remained under review by ASIO at the end of the reporting period and IGIS will consider ASIO's response when it is received.

ASIO notified IGIS of a breach of subs 24(1) of the ASIO Act where activity was conducted against the subject of an identified person warrant without the required authorisation under subs 24(2) of the ASIO Act being in place. The incident arose when an authorisation list for computer access activity was incorrectly interpreted also to provide authority for surveillance device activity. IGIS was satisfied with ASIO's assessment and remediation activity.

IGIS continued to review 2 matters notified by ASIO in 2019–20 and one incident notified in July 2020 concerning non-compliance with ASIO's online research policy. Each incident related to an ASIO officer attempting to access restricted data within the meaning of Division 478 of the *Criminal Code Act 1995* (Criminal Code). In each incident, the relevant officer was unaware that access, or attempted access, to this data was unauthorised. On this basis, ASIO assessed that for all 3 incidents an offence had not been committed in relation to s 478.1 of the Criminal Code. In one instance, an ASIO officer obtained access to data. ASIO assessed this incident to be a breach of subs 24(2) of the ASIO Act as the relevant officer was not listed on the authorisation list for the relevant warrant. IGIS continues to consider the issues identified in this incident.

## INTERNALLY AUTHORISED TRACKING DEVICES

In December 2020, the *Australian Security Intelligence Organisation Amendment Act 2020* granted ASIO new powers to use certain types of tracking devices under internal authorisation rather than requiring a warrant to be authorised by the Attorney-General. Internally authorised tracking devices (IATDs) must not involve the remote installation of a tracking device and must not involve entry to a premises or interference with the interior of a vehicle without consent.

In February 2021, ASIO notified IGIS of an incident where a request for an IATD may not have included the level of detail required to show that the legal threshold for authorisation had been met. Applications for IATDs must set out the facts and other grounds on which the applicant considers it necessary that the authorisation should be given, and the extent to which the applicant considers that the authorisation will substantially assist the collection of intelligence in respect of a specified security matter.

Upon identifying the issue, ASIO promptly ceased collecting data using the device, quarantined data that had been collected, and initiated an internal compliance review of the operation. The authorisation was subsequently revoked and re-issued. ASIO advised that data collected under the initial authorisation was deleted from ASIO systems. The compliance review identified a number of weaknesses in ASIO's processes and made 4 recommendations directed at improving compliance with legislative requirements, providing a greater level of senior officer oversight, and strengthening collaboration between ASIO's legal and operational areas.

IGIS conducted an independent review of the incident and agreed with ASIO's findings. The Inspector-General noted there were some similarities between the issues identified in the compliance review and those identified during IGIS's 2018–19 inquiry into an ASIO matter, and suggested ASIO consider whether the remediation action identified in the review was applicable more broadly. The Inspector-General also noted some deficiencies in ASIO's templates that may have contributed to the incident.

ASIO obtained legal advice from the Australian Government Solicitor in relation to the incident, which was shared with IGIS. This advice indicated that the request likely met the minimum legal threshold, but contained shortcomings similar to those already identified by ASIO.

ASIO subsequently reported to IGIS on its implementation of the recommendations of the compliance review and provided a briefing to the Inspector-General. IGIS had commenced reviewing ASIO's revised processes and training at the end of the reporting period.

## DISCLOSURE OF INFORMATION FROM A FOREIGN PARTNER SERVICE

IGIS continues to monitor ASIO's response to an incident notified to IGIS concerning disclosure of information from a foreign partner service about an Australian citizen. This information could not have been collected lawfully by ASIO without a computer access warrant under s 25A of the ASIO Act. IGIS reviewed this matter during the previous reporting period and concluded that the incident highlighted systemic issues that could result in further breaches if not addressed. In September 2020, ASIO briefed IGIS on its intended approach to address this matter. IGIS considered ASIO's intended approach to be appropriate and notes that liaison between ASIO and the foreign partner service remains ongoing.

## INCIDENTS RELATING TO ACCESS TO TELECOMMUNICATIONS DATA UNDER THE TIA ACT

Sections 175 and 176 of the TIA Act empower certain ASIO personnel to authorise the collection of historical and prospective telecommunications data from telecommunications carriers or carriage service providers. Authorisations are limited to circumstances in connection with the performance of ASIO's functions and in accordance with the Minister's Guidelines, and must be signed by a specified eligible person.

During 2020–21, IGIS conducted inspection activities that were focused on ASIO's access to telecommunications data. IGIS did not identify any issues of legality, but did find some procedural and record keeping issues relating to internal approvals and the need for more detailed policy guidance relating to compliance reporting thresholds. ASIO is taking steps to address these issues, which will be considered by IGIS in future inspection activities to assess their effectiveness.

### PROSPECTIVE DATA AUTHORISATIONS – SECTION 176 OF THE TIA ACT

ASIO notified IGIS of 4 incidents relating to prospective data authorisations under s 176 of the TIA Act. The first and second incidents occurred when relevant areas failed to act on information in the agency's possession that a target service had been disconnected, resulting in invalid authorisations for access to prospective information or documents being issued. ASIO advised it had deleted data received following disconnection of the services and had reinforced to staff the requirements to cross check service information available to the agency before submitting authorisation requests to decision-makers. IGIS is satisfied with the steps taken by ASIO to remediate these cases and reduce the risk of recurrence.

The third and fourth incidents involved a failure to revoke prospective data authorisations in circumstances where the eligible person was satisfied that the disclosure is no longer required.

In the first of these two cases (the third incident), ASIO came into possession of information that indicated the service being collected against was no longer subscribed to by the target. ASIO's review of this matter concluded that, consistent with subs 176(6), the authorisation should have been revoked. However, a further 11 days' worth of data was collected before the revocation was actioned. ASIO advised that the data obtained during this 11-day window was deleted. In this instance, the information that the target had disconnected this service was subsequently found to be erroneous, and it was confirmed that the target was still subscribed to the service. IGIS considers this incident to be a matter of propriety, and a failure of process.

In the second of these two cases (the fourth incident), ASIO reported that a decision was made to continue a prospective data authorisation on specific conditions but that once those conditions no longer existed there was a failure to revoke the authorisation in breach of subs 176(6).

IGIS is satisfied that appropriate steps have been taken in relation to both incidents to improve staff awareness of revocation obligations and reduce the risk of future delays in actioning the revocation of authorisations.

### EXISTING DATA AUTHORISATIONS – SECTION 175 OF THE TIA ACT

ASIO also notified IGIS of 5 incidents where issues were identified with telecommunications data authorisations issued under s 175 of the TIA Act. Some cases were reported by ASIO as breaches of the Minister's Guidelines, while legal advice resulted in other cases being reported as breaches of s 276 of the *Telecommunications Act 1997* (Telecommunications Act) resulting from the issue of invalid s 175 authorisations.

In the first incident, ASIO officers requested existing information or documents based on information available to them, but which other parts of the agency knew had the potential to be unreliable. ASIO reported that in this incident, personal data for one service which was not relevant to security was acquired. This acquisition would likely have been prevented had ASIO implemented reasonable controls. This matter was assessed by ASIO to be a breach of s 4.2 of the Minister's Guidelines. ASIO has advised that the data acquired under this request has been deleted. IGIS is satisfied with the steps taken by ASIO to implement controls that will prevent recurrence of this type of breach.

In the other 4 incidents, ASIO made 5 requests for existing information or documents based on authorisations that contained erroneous information. ASIO had correct information available to it at the time the authorisations were made, but the incidents occurred as a result of a combination of human error in interpreting information about subscribers and typographical errors. For one request no data was received; for 3 requests the errors resulted in data being obtained that was earlier than the connection date of the services; and for the final request, the error resulted in data being received for a service not relevant to security. These incidents were reported by ASIO as breaches of s 3.7 of the Minister's Guidelines. ASIO also advised that the relevant data had been deleted.

The 4 incidents described above are similar to 2 incidents reported in the 2019–20 IGIS Annual Report, which at the time of publication were still under review. In concluding its review of these incidents, ASIO determined that as erroneous information was used to request disclosures under s 175, the authorisations were likely invalid and disclosure of telecommunications data was unauthorised and in breach of s 276 of the Telecommunications Act.

In reviewing these incidents, IGIS concluded that in circumstances where ASIO had in its possession correct information, but the s 175 authorisation relied wholly or partly on erroneous information, then the authorisation is wholly or partly invalidated because the eligible person should not, for the purpose of subs 175(3), have been satisfied that the disclosure would have been in connection with the performance of the organisation's functions. An invalid s 175 notice can then result in a telecommunications carrier disclosing information in breach of s 276 of the Telecommunications Act.

In June 2021, ASIO notified IGIS of an additional incident that it considered a potential breach of s 276 of the Telecommunications Act. This matter remains under review by ASIO and IGIS will consider ASIO's response following its review.

In 2019–20, ASIO notified IGIS of a case involving 3 separate incidents within the same operation where telecommunications data was obtained contrary to s 175 of the TIA Act. In the first incident, the carrier was unable to limit the results of the s 175 request to the criteria identified by ASIO, resulting in the provision of significant additional data to ASIO. ASIO advised IGIS that it was working to identify the data that was outside the specified criteria and delete it from ASIO's systems. In the second incident, data was delivered by the carrier without a valid s 175 request in place. ASIO advised that this data was quarantined and then deleted. In the third incident, the s 175 request was invalid as it sought data for a period after the date of the request. ASIO advised that this data was also quarantined and deleted. ASIO finalised its review of this matter during the reporting period, concluding in relation to the first incident that no breach had occurred. In relation to the second and third incidents, ASIO concluded that these incidents were a breach of s 175 of the TIA Act and noncompliant with ASIO's internal policy and procedure. ASIO subsequently issued each carrier with a valid s 175 request. IGIS was satisfied with ASIO's assessment and remediation action. In March 2021, ASIO notified IGIS that it had identified that data provided by one carrier included data that was outside the scope

of the authorisation. IGIS was advised that this data would be deleted from ASIO systems. IGIS will verify data deletion through its annual inspection of technical collection, retention and deletion of data.

## THE MINISTER'S GUIDELINES

The Minister's Guidelines are issued under s 8A of the ASIO Act and are to be observed by ASIO in performance of its functions. The Guidelines were issued in August 2020 and replace the Attorney-General's Guidelines issued in 2007. Among other things, the Guidelines require ASIO to review each of its investigations on an annual basis. In 2020–21, ASIO reported a small number of investigations were conducted without review for periods longer than a year, including one historical case. In addition, IGIS inspection activity identified additional cases of the Guidelines being breached and non-compliance with internal procedures regarding reviews.

Section 3.7 of the Guidelines states that ASIO will take all reasonable steps to ensure that personal information used or disclosed by ASIO is relevant, accurate and not misleading. ASIO notified IGIS of 7 incidents it assessed to be breaches of s 3.7 of the Guidelines. As discussed earlier, some of these matters were also determined to be breaches of s 276 of the Telecommunications Act.

Section 4.2 of the Guidelines requires the Director-General to take all reasonable steps to ensure that ASIO's collection, retention, use, handling, and disclosure of personal information is limited to what is reasonably necessary to perform its functions. This includes having reasonable controls to prevent the collection and processing of information in breach of a warrant or statutory authority, and procedures for appropriate remediation and reporting should this occur. ASIO notified IGIS of one incident relating to a request under s 175 of the TIA Act, discussed in the earlier telecommunications data section, which it assessed to be a breach of s 4.2 of the Guidelines. In addition, ASIO notified IGIS of an incident where a service authorised for interception under a warrant issued under s 11B of the TIA Act was identified as being subscribed to an Australian permanent resident. In this instance, ASIO had not identified that the residency status of the subscriber had changed. Once identified, ASIO ceased interception, took steps to remove the service from the warrant and requested that data that had been intercepted after the subscriber became a permanent resident be deleted. While ASIO concluded that the matter was not a breach of subs 11D(5) of the TIA Act, it considered that the incident highlighted weaknesses in processes for nationality checking. ASIO advised it had introduced processes to provide additional assurance regarding the accuracy of personal information used in warrants. IGIS has reviewed the matter and considers ASIO's assessment and subsequent remediation action to be appropriate. IGIS will verify data deletion through its annual inspection of technical collection, retention and deletion of data in August 2021.

In 2019–20, ASIO notified IGIS of a potential breach of the then Attorney-General's Guidelines concerning financial records that were provided to ASIO contrary to internal procedures and without required approvals. After the incident was identified, all records that had been provided to ASIO were quarantined and then destroyed. Other relevant cases were then reviewed with no additional contraventions identified. ASIO's review concluded that the matter was a breach of s 10.4(b)(i) of the then Attorney-General's Guidelines and non-compliant with internal procedures. IGIS reviewed the matter and is satisfied with ASIO's assessment and subsequent remediation action.



## INSPECTION OF ASIS ACTIVITIES

The functions of ASIS are set out in s 6 of the IS Act and comprise:

- intelligence collection
- intelligence communication
- support to the ADF
- counter intelligence
- foreign liaison
- cooperation and assistance to intelligence agencies and prescribed authorities
- certain activities in support of ASIO
- other activities as directed by the Minister for Foreign Affairs.

Under the IS Act ASIS can only perform these functions in the interests of Australia's national security, foreign relations or national economic well-being, and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia.

IGIS has oversight of all ASIS's activities, and in practice focuses on those that are most likely to raise legality, propriety or human rights concerns, particularly concerning Australian persons. The COVID-19 pandemic meant that IGIS did not visit any ASIS office outside Canberra in 2020–21, but has otherwise been able to conduct normal oversight activities of ASIS throughout the year. IGIS conducted a number of different inspections, including:

- operational files, covering ASIS activities at overseas locations
- advice provided to the Minister for Foreign Affairs in ministerial correspondence, including ministerial authorisations sought under the IS Act
- weapons related matters, including ASIS's implementation of a revised control framework
- access to sensitive financial information from the Australian Transaction Reports and Analysis Centre (AUSTRAC)
- how ASIS manages internal security investigations into its staff.

The purpose of IGIS inspections is to ascertain whether there are any activities that give rise to legality, propriety, human rights issues or other concerns. A risk-based approach means that operational file inspections were conducted most frequently, and topics selected were either geographically or thematically focused. The approach IGIS takes to each inspection varies, but generally involves discussions with relevant ASIS officers, review of official ASIS records and formal reporting of findings to ASIS.

The level at which ASIS is notified of inspection outcomes depends upon the significance of the findings. Communication may be from the IGIS inspection team leader (if minor or no problems are identified), escalating to the relevant Assistant Inspector-General (if some problems are identified), and then to the Inspector-General or Deputy Inspector-General (if significant legality or propriety problems are identified). Since the introduction of this tiered approach, inspection findings have not identified any issues of significance to warrant a letter from the Inspector-General or Deputy Inspector-General.

IGIS also conducts other review and oversight activities. These other activities are an important part of the oversight of ASIS, and provide additional assurance. IGIS reviews all ASIS reports of legislative non-compliance or other significant compliance matters. From time to time, ASIS also consults IGIS on the legality and propriety of certain ASIS proposals or draft internal policies before finalisation; this allows IGIS to identify any concerns with the documents before they are relied upon by ASIS officers.

#### **EXAMPLE OF CONSULTATION ON ASIS INTERNAL POLICIES – PRIVACY RULES**

On 2 occasions during 2020–21 ASIS updated its internal procedures relating to the application of the ASIS Privacy Rules. These updates addressed matters such as how the concept of ‘intelligence information’ applies in a specific context; the provision of further guidance on what could constitute ‘evidence to the contrary’ when making a presumption of nationality and associated record keeping requirements; and revised approval requirements when communicating intelligence information concerning Australian minors. IGIS did not identify any concerns with ASIS’s changes.

On each occasion IGIS was provided an opportunity to comment on the legality and propriety of the changes. ASIS made amendments to presumptions of nationality in response to IGIS findings about the procedures as part of a previous compliance incident from 2019–20.

IGIS inspections and other review activities are supplemented by awareness briefings from ASIS on various matters throughout the year, either at the request of IGIS or suggested by ASIS. These briefings allow IGIS to be apprised of emerging issues and follow up observations from inspection activities. There are regular meetings between the Inspector-General and the Director-General of ASIS, as well as tri-annual meetings between the Inspector-General, senior IGIS and senior ASIS officers.

#### **EXAMPLE OF AWARENESS BRIEFING – HUMAN RIGHTS**

One of ASIS’s functions under the IS Act is to liaise with intelligence or security services of other countries. Occasionally, ASIS will receive information that suggests that an intelligence or security service may not be respecting the human rights of individuals, for example during arrest, detention or interrogation operations. During 2020–21, ASIS briefed IGIS on such allegations relating to one of the services with which it liaises, including action ASIS took to investigate and respond to the matter. In this case, IGIS considered that ASIS was generally managing its response appropriately.

### **INSPECTION OF OPERATIONAL FILES**

IGIS inspections of operational files involve reviewing a sample of files, focusing on areas determined to be higher risk by IGIS. ASIS activities often involve the use of human sources and ASIS officers are deployed in many countries to support a wide range of activities including counterterrorism, efforts against people smuggling and support to military operations. IGIS inspections examine, among other things, the appropriate application of the ASIS Privacy Rules; compliance with internal guidelines, policies, and procedures; and human rights considerations and requirements relating to torture and other cruel, inhumane or degrading treatment.

During 2020–21 IGIS officers conducted 8 operational file inspections. Depending on the scale and complexity, these inspections were conducted over one or 2 months. The inspections focused on:

- four specific overseas locations
- one sensitive intelligence activity
- how ASIS manages its holdings of large datasets (bulk data)
- activities conducted in relation to ASIO under s 13B of the IS Act
- ASIS's management of human rights considerations (as at 30 June this inspection was ongoing).

Overall, in general IGIS was satisfied that ASIS appropriately identified and considered legality and propriety risks associated with operational activities. IGIS detected no significant concerns regarding legality, propriety or human rights. In the context of these operational file inspections, IGIS highlighted some compliance concerns and other areas for improvement, particularly around timely and complete record keeping.

### EXAMPLES OF OPERATIONAL FILE INSPECTIONS – FINDINGS

IGIS's September 2020 operational file inspection focused on ASIS activities at a particular overseas location. No issues of legality or propriety were identified. Of note, the IGIS inspection team observed that record keeping and general administration related to the location was of a high standard. From the records, IGIS determined that ASIS officers consistently considered legality, propriety, and human rights during the planning and conduct of these operational activities.

In January and February 2021, IGIS conducted an operational file inspection focusing on how ASIS manages its holdings of large datasets (bulk data). This was the first time IGIS conducted an inspection in this area. The inspection found significant non-compliance with ASIS's internal policy with respect to adhering to training requirements for accessing bulk data systems, and recording justifications for searches relating to Australian persons. While these instances of non-compliance did not give rise to a failure of legality or propriety, ASIS acknowledged the findings of the IGIS inspection and advised a number of remediation activities both underway and planned. IGIS plans to conduct another bulk data inspection in the future, which will include reviewing the effectiveness of ASIS's remediation activities.

### INTERNAL SECURITY INVESTIGATIONS INSPECTION

IGIS conducted an inspection to assess how ASIS manages internal security investigations into its officers, specifically cases where the investigation could result in the officer having their security clearance revoked (a security clearance is a precondition of employment at ASIS). The inspection examined, among other things, compliance with internal policies and procedures; record keeping; and the management of procedural fairness. This was the first IGIS inspection into ASIS management of these matters.

The inspection found that the cases reviewed were generally managed appropriately, in line with procedural requirements, and individuals were afforded appropriate procedural fairness. IGIS identified areas for improvement, including record keeping, procedural fairness processes and the need to finalise relevant draft policies and procedures. ASIS undertook to address the findings.

## INSPECTION OF MINISTERIAL SUBMISSIONS

IGIS reviews the majority of ministerial submissions sent by ASIS to the Minister for Foreign Affairs to ensure that ASIS is appropriately and accurately informing the minister on relevant ASIS matters. The majority of the submissions reviewed by IGIS relate to ministerial authorisations to produce intelligence on Australian persons. Two such cases occurred during 2020–21.

### EXAMPLE OF IGIS CONSULTATION ON A MINISTERIAL SUBMISSION

ASIS will occasionally consult IGIS on proposed ministerial submissions.

In 2020–21, 3 breaches by ASIS of Privacy Rule 4.2 were identified (these are discussed in the section on ASIS Compliance with Privacy Rules). As part of addressing the breaches, ASIS prepared a ministerial submission to advise the minister of the matter and seek the minister's agreement to add the agencies that had not been approved. As the submission related to a Privacy Rules compliance incident and referred to IGIS, ASIS provided IGIS with a draft of the proposed submission. IGIS provided comments on the content of the draft submission as it related to this Office, and IGIS's understanding of the compliance incident. The Director-General of ASIS took IGIS's comments into account in the final submission.

## MINISTERIAL AUTHORISATIONS TO PRODUCE INTELLIGENCE ON AUSTRALIAN PERSONS

ASIS is a foreign intelligence collection agency and the IS Act requires it to obtain ministerial approval before conducting intelligence activities on Australian persons. IGIS inspections of ministerial submissions that relate to such authorisations focus on the accuracy and appropriateness of information provided to the minister, and determine whether relevant requirements of the IS Act were met.

IGIS reviewed all ministerial authorisations obtained by ASIS from the Minister for Foreign Affairs in 2020–21. The inspections did not identify any significant matters. A compliance incident relating to ministerial authorisation reporting requirements under the IS Act was self-reported by ASIS before the commencement of the July 2020 inspection. IGIS considers that in general ASIS has well established processes in place to manage its submissions to the minister.

## EMERGENCY MINISTERIAL AUTHORISATIONS

There were no emergency ministerial authorisations during the reporting period.

## THE ASIS COMPLIANCE BRANCH

IGIS regularly engages with the ASIS Compliance branch. This branch works to develop and promote an agency culture of compliance, including by conducting investigation into matters of concern; when ASIS does the latter, IGIS receives a copy of the investigation report. IGIS reviews all ASIS investigation reports and considers the scope and process of the investigation and the action taken on any issues identified. IGIS may undertake further investigations, request additional information, recommend action to be taken, or request updates on implementation of remediation.

During the reporting period, IGIS met frequently with the ASIS Compliance branch and was briefed on all relevant matters and provided access as required. IGIS is satisfied with ASIS's compliance investigation processes.

## REPORTING OF COMPLIANCE MATTERS

ASIS reported to IGIS 3 breaches of s 8 of the IS Act, where ASIS failed to obtain a ministerial authorisation before producing intelligence on Australian persons. One case involved a complex legislative matter involving an authorisation under s 8 of the IS Act and foreign intelligence collection warrants which are issued by the Attorney-General under the TIA Act. This breach led to IGIS conducting an investigation into the case (see text box below).

### EXAMPLE OF AN IGIS INVESTIGATION INTO A COMPLIANCE INCIDENT

IGIS was advised by ASIS of a compliance incident regarding a complex legislative matter involving the interaction between different statutory ministerial authorisation regimes. The result was that, while the minister was made fully aware of and endorsed the activity, the minister was not specifically asked to provide a ministerial authorisation to produce intelligence on an Australian person. Ahead of ASIS finalising its review and incident report, IGIS determined its own investigation should be made into the relevant operation, given the unusual nature of the breach. IGIS reviewed relevant ASIS records and ASIO warrant paperwork, and examined associated intelligence collection activities, intelligence communication and reporting. IGIS held discussions about the incident with relevant ASIS compliance and operational staff. The IGIS investigation found 2 additional breaches of the IS Act which resulted from the same issue, as well as inadequate record keeping for the operation. The IGIS investigation found that ASIS had considered and applied the Privacy Rules. IGIS recommended that ASIS provide further guidance to ASIS officers involved in related activities, and that ASIS's Compliance Branch review other related operations to ensure those operations were compliant with legislative and policy requirements. ASIS acknowledged the findings, and IGIS concluded that ASIS actions taken in response to the breach were reasonable.

The other 2 breaches of s 8 of the IS Act reported by ASIS related to one incident involving 2 Australians that occurred in the previous reporting year. The incident involved an ASIS officer tasking an agent to use their accesses to confirm otherwise publicly available information relating to the 2 Australian persons. Before this tasking, the ASIS officer considered whether a ministerial authorisation was required, but at the time assessed that an authorisation was not required because the tasking was directed at the intentions of a foreign government. ASIS identified that the situation was unclear and obtained legal advice from the Australian Government Solicitor. Both IGIS and ASIS concluded a ministerial authorisation should have been sought. However, given the complex circumstances of this case at the time, IGIS does not consider that this case indicates any systemic issues within ASIS's compliance regime. ASIS advised that this case would be reflected in its future training.

Section 10A of the IS Act requires the Director-General of ASIS to provide a written report to the minister on activities conducted against an Australian person covered by a ministerial authorisation within 3 months of the authorisation ceasing to have effect. During 2020–21, ASIS breached this section by failing to provide a report within the required timeframe on authorised activities on 18 Australians covered by a ministerial authorisation. This was due to an administrative oversight, caused partly by ASIS including a large number of individuals under one ministerial submission and the individuals covered changing from one authorisation to the next. ASIS subsequently reported this incident to the Minister for Foreign Affairs.

On occasion ASIS will advise IGIS of compliance incidents that are initially considered possible breaches of legislation. Further investigation and legal considerations may subsequently find that the incident is not a breach of legislation, but that there are concerns or questions of

propriety One such notification relates to an incident that occurred in 2015 but was only identified by ASIS in 2019 as a possible compliance matter. The matter involved ASIS accessing an electronic device of an Australian person overseas. This case remained open at the end of 2019–20 as there was some difference of views between IGIS and ASIS as to whether this activity was consistent with the IS Act. The issue turned on whether the activity was ‘covert and intrusive’ in the circumstances. Advice from the Australian Government Solicitor was obtained to resolve the matter.

In the 2020–21 reporting period, both IGIS and ASIS agreed the way the activity was conducted was not consistent with propriety or ASIS’s procedures. IGIS has more recently observed similar scenarios where ASIS has adhered to propriety in these circumstances. In its internal compliance training program, ASIS has used the case as an example of ‘lessons learned’ to promote better practice.

### COMPLIANCE WITH PRIVACY RULES

The Minister for Foreign Affairs issues written rules (the ASIS Privacy Rules) to 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. The rules are publicly available on the ASIS website.

The ASIS Privacy Rules require ASIS to: provide IGIS with access to all of ASIS’s intelligence holdings concerning Australian persons; consult IGIS about relevant procedures; report to the IGIS any breaches of the ASIS Privacy Rules; and advise IGIS when ASIS has revised its determination that a person previously presumed to be foreign is an Australian person.

During 2020–21, ASIS reported 5 breaches of the Privacy Rules which constituted a breach of subs 15(5) of the IS Act. These breaches occurred across 3 separate incidents. This is a significant reduction compared to the last reporting year, and is primarily because ASIS has developed a new automated process for publishing liaison reporting in a manner consistent with the Rules.

Two of these breaches occurred because ASIS already had information that the individuals being reported on were Australian persons, but communicated the intelligence information without first applying the Rules, due to:

- data entry errors in a key ASIS database that contains information indicating a person’s nationality
- a failure to adequately review an attachment to a report prior to publication.

The other incident, which constituted 3 of the breaches, related to Rule 4.2. This rule requires the Minister for Foreign Affairs to approve a Commonwealth agency, together with the agency’s relevant function, to receive relevant intelligence reports from overseas agencies that contain intelligence information concerning an Australian person. Since late 2019, ASIS has largely managed the application of this rule through an automated publishing system. Following inquiries from IGIS into how the communication of reporting under this rule was operating, it was identified that there were additional Commonwealth agencies which were receiving reporting under this rule but had not been authorised by the minister to do so. ASIS’s investigation into the incident identified that a technical error had added these agencies to the automated reporting system. ASIS kept IGIS informed on the progress of its investigation and rectification measures, and also informed the minister of this matter. IGIS was satisfied with ASIS’s response to the incident.

Separately, ASIS compliance reporting to IGIS identified a small number of other cases where, while there was no breach of the Privacy Rules, record keeping relating to the application of the rules was inadequate.

IGIS considers that, given the total volume of reporting that ASIS produced on Australian persons, the incidence of Privacy Rules breaches and other related compliance matters was extremely rare. IGIS found no indication of systemic failings with ASIS's compliance controls or training. Importantly, IGIS did not identify any cases where reporting on an Australian person would not have been reasonable and proper had the Privacy Rules been correctly applied at the time.

Under the Privacy Rules, ASIS advises IGIS when it obtains further information on an individual overseas that leads ASIS to overturn its initial presumption that the individual is not an Australian person. If the initial presumption was reasonable, such incidences do not represent a breach of legislation or the Privacy Rules. In 2020–21, ASIS reported to IGIS 5 cases where such a 'presumption of nationality' was overturned. IGIS determined that in all cases ASIS's initial presumption was reasonable and in accordance with the Privacy Rules as ASIS initially had no evidence that the individuals, who were located outside Australia, were Australian.

## **AUTHORISATIONS RELATING TO THE USE OF WEAPONS**

Under the IS Act ASIS officers are prevented from undertaking activities that involve violence or the use of weapons. The Act does allow ASIS to train its officers in the use of certain weapons and self-defence techniques, and to equip its officers with weapons in certain circumstances in order to protect themselves or certain other people.

Schedules 2 and 3 of the IS Act require the Minister for Foreign Affairs and the Director-General of ASIS to provide to the Inspector-General certain documentation relating to the use of force and weapons. This includes approvals for weapons, and self-defence training; copies of the Director-General guidelines issued for the purpose of weapons, self-defence and use of force; approvals in specific circumstances where the minister approves the use of force; and notification of officers or agents who have used weapons or self-defence techniques other than in training or approved scenarios.

In 2020–21, the Minister for Foreign Affairs and the Director-General of ASIS have provided the reports required under the IS Act. IGIS continues to be satisfied that there is a genuine need for a limited number of ASIS staff to have access to weapons for self-defence to perform their duties effectively. ASIS did not report, and IGIS did not find, any cases where a weapon was discharged or self-defence techniques were used other than in training. ASIS did not report, and IGIS did not find, any instances of noncompliance with the Director-General's internal guidelines on weapons. As at 30 June, IGIS was conducting an inspection of weapons-related matters, which includes reviewing ASIS's implementation of revised weapons guidelines.

## CHANGES TO ASIS WEAPONS GUIDELINES

In December 2020, the Director-General of ASIS issued updated guidelines under Schedule 2 of the IS Act relating to the use of weapons and self-defence techniques by ASIS. The revised Guidelines represent significant structural changes compared to the previous version, issued in 2015, including some detail being moved from the Guidelines into a new associated ASIS weapons management policy. The revised Guidelines and associated new policy modernise ASIS's framework for managing weapons, and provide more detailed guidance to ASIS officers on matters such as acquisition, management and disposal of ASIS weapons as well as relevant internal delegations and authorisations.

IGIS was consulted on multiple versions of the draft Guidelines and associated policy before finalisation, and ASIS amended the documents in response to IGIS feedback. IGIS is satisfied that the new framework provides clear and appropriate guidance to ASIS officers regarding their obligations using and managing weapons.

In accordance with the IS Act, in January 2021 the then Acting Inspector-General briefed the PJCIS on the content and effect of the updated ASIS guidelines.

## INSPECTION OF ASD ACTIVITIES

The functions of ASD are set out in s 7 of the IS Act. In the performance of these functions ASD undertakes a number of activities which are categorised as follows:

- foreign intelligence collection
- intelligence communication
- prevention and disruption of cybercrime
- provision of material, advice and assistance relating to security and integrity of information
- assistance to the ADF
- protection of specialised technologies
- assistance to Commonwealth and State authorities
- assistance to certain intelligence agencies and prescribed authorities.

During 2020–21, IGIS inspections focused on:

- ASD's activities concerning Australian persons
- ASD's compliance with relevant legislation, in particular the IS Act and the TIA Act
- the propriety of ASD's activities
- requirements related to ASD's access to sensitive financial information
- the consistency of ASD's activities with human rights.

IGIS inspections of ASD activities are facilitated by regular engagement with ASD's Oversight, Compliance and Legal teams, and access to required information and systems. Given the volume and complex nature of ASD activities, the IGIS inspection program is continuous and includes scheduled inspection activities as well as proactive reviews of areas of risk or sensitivity. IGIS also reviews ASD's existing and proposed policies and procedures to determine whether they are appropriate and effective.



When ASD identifies possible breaches of legislation and significant or systemic matters of noncompliance with internal policies, ASD provides written notification of these issues to IGIS. IGIS officers review ASD's findings, and where necessary, undertake further independent investigation of the incidents.

In 2020–21, inspections were supplemented by briefings on various matters throughout the year, regular meetings with ASD's Oversight and Compliance teams and engagement with the ASD General Counsel. There are tri-annual meetings between the Inspector-General and the Director-General of ASD, senior IGIS and senior ASD officers to discuss key oversight matters and developments. In 2020–21, themes of these meetings included: compliance incidents; legislative reform; and staffing and workplace matters.

### EXAMPLE OF INSPECTIONS RELATED TO HUMAN RIGHTS

One of ASD's functions under the IS Act is to communicate, in accordance with the Government's requirements, the intelligence it obtains. In performing this function, ASD must adhere to relevant legislative requirements and act consistently with human rights.

During 2020–21, IGIS conducted an inspection of ASD's communication of certain intelligence to persons in accordance with para 7(1)(b) of the IS Act. The purpose of this inspection was to provide assurance that ASD's communication of intelligence in these circumstances is consistent with human rights. IGIS officers reviewed ASD's records relating to these activities, including associated policies and procedures. IGIS officers identified one area for improvement relating to record keeping, to ensure that ASD adequately considers and acts consistently with regard to human rights when communicating intelligence.

### MINISTERIAL AUTHORISATIONS TO UNDERTAKE CERTAIN ACTIVITIES

The IS Act requires that ASD obtains authorisation from the Minister for Defence before conducting certain activities, including producing intelligence on Australian persons. During 2020–21, IGIS inspected a sample of ASD's applications for ministerial authorisation. These applications were found to be generally of a high standard.

### EXAMPLE OF ADDRESSING SYSTEMIC ISSUES

Previous IGIS Annual Reports (2018–19 and 2019–20) noted that IGIS had identified several instances relating to ministerial authorisations where ASD did not include appropriate restrictions on certain database records. IGIS noted that this practice heightened the risk of an inadvertent breach of the IS Act by omitting a layer of additional assurance.

During the 2020–21 reporting period, IGIS identified further instances where adequate restrictions were not in place, and communicated this to ASD. Prior to remedying 2 of the identified issues, ASD conducted activities on the relevant Australian persons without a ministerial authorisation in place. While ASD has advised it does not view these activities to have required ministerial authorisation, IGIS is currently reviewing the circumstances of the activities to determine whether they constitute a breach of the requirements of the IS Act. As an ongoing area of concern, IGIS made an initial suggestion to ASD regarding the application of appropriate restrictions on certain database records, which ASD is currently implementing. In addition to its review, IGIS will continue to monitor this issue and the effectiveness of ASD's remedial actions.

### EMERGENCY AUTHORISATIONS

Situations may arise where ASD requires a ministerial authorisation to undertake activities as a matter of urgency. Under the IS Act, emergency authorisations may be provided orally by: the Minister for Defence; other select ministers where the Minister for Defence is unavailable; or the Director-General of ASD if the ministers are not readily available. Emergency authorisations are valid for 48 hours after which a new authorisation is required if ASD is to continue the activity. ASD did not obtain any emergency ministerial authorisations during the reporting period.

### REPORTS ON ACTIVITIES CONDUCTED UNDER MINISTERIAL AUTHORISATION

The IS Act requires that ASD provide the Minister for Defence with a written report in respect of each activity carried out in reliance on a ministerial authorisation. As part of regular inspections, IGIS reviews the details of these reports to provide assurance that ASD is reporting accurately and in a timely manner, and in accordance with the requirements of the IS Act.

During 2020–21, IGIS officers inspected a sample of ASD's written reports. As part of this review IGIS suggested that ASD consider including further detail about activities undertaken during the authorised period. Such additional detail would ensure that the Minister for Defence is more comprehensively informed about the activities being conducted and would better meet the requirements of the IS Act.

### MINISTERIAL SUBMISSIONS

During 2020–21, IGIS conducted a quarterly review of a sample of submissions ASD provided to the Minister for Defence. Through such inspections, IGIS seeks to ensure the Minister for Defence is provided timely and accurate information about critical ASD issues.

The 2019–20 IGIS Annual Report noted ASD had conducted an audit of ministerial submissions prepared in support of all active ministerial authorisations. This audit showed that over one third of the submissions to the minister audited contained unclear or inaccurate advice. ASD

has updated its governance arrangements for preparing submissions in support of ministerial authorisations, and implemented regular compliance audits to ensure the accuracy of information.

During the reporting period, IGIS staff continued to review ministerial submissions with a specific focus on reviewing the accuracy and clarity of the advice provided to the Minister for Defence; in 3 cases across 2 ministerial submissions ASD was found to have provided the Minister for Defence with inaccurate advice. Although these inaccuracies did not substantively influence the overall advice, such errors highlight the need for stringent quality assurance processes. IGIS will continue to monitor the effectiveness of ASD's remedial actions in this area.

## COMPLIANCE WITH 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. The IS Act prohibits ASD from communicating intelligence information about an Australian person other than in accordance with those rules. The Privacy Rules are publicly available on the ASD website.

The ASD Privacy Rules require ASD to: provide IGIS with access to all of ASD's intelligence holdings concerning Australian persons; consult IGIS about relevant procedures and report to the IGIS any breaches of the ASD Privacy Rules. Additionally, ASD must advise IGIS when ASD has revised its determination that a person previously presumed to be foreign is an Australian person – this is known as overturning a presumption of nationality.

Overturning a presumption occurs when ASD obtains further information on an individual that leads ASD to overturn its initial presumption that the individual is not an Australian person. If the initial presumption was reasonable, such incidences do not represent a breach of legislation or the Privacy Rules. ASD provides reports to IGIS that include details of the measures taken to protect the privacy of those persons, including informing other relevant intelligence agencies of overturned presumptions of nationality and applying administrative restrictions on certain database records to prevent unauthorised activities.

Through regular inspections, IGIS reviews these cases to independently determine whether ASD's presumptions of nationality were reasonable given the information available to ASD at the time. IGIS also assesses whether ASD took appropriate measures to protect the privacy of the Australian persons following an overturned presumption of nationality. During 2020–21, IGIS found that ASD's actions were largely appropriate and in accordance with the ASD Privacy Rules, noting the 2 incidents discussed below.

## SEPTEMBER 2020 INCIDENT

In September 2020, ASD advised IGIS that it had breached the ASD Privacy Rules, as it had retained intelligence information concerning Australian persons where it was unnecessary to do so for the proper performance of ASD's functions, or was not otherwise authorised or required. This occurred due to a technical issue that caused the information to be retained, despite ASD's intention to delete it. IGIS reviewed this incident and found that ASD's remedial actions, including the deletion of the information and updating relevant procedures, were appropriate in the circumstances.

## OCTOBER 2020 INCIDENT

During an inspection IGIS identified one presumption of nationality that did not take into account information available to ASD that suggested that the individual was an Australian person. In October 2020, ASD advised that this constituted a breach of its internal policies and was the result of human error. IGIS is currently reviewing the circumstances of the case to independently determine whether it constitutes a breach of the requirements of the ASD Privacy Rules or the IS Act.

## LEGISLATIVE NON-COMPLIANCE

### INCIDENTS RELATING TO INTERCEPTION CONTRARY TO PARA 7(1)(A) OF THE TIA ACT

Section 7 of the TIA Act prohibits agencies from intercepting communications except in limited circumstances, including where there is a warrant in place allowing interception. Section 12 of the TIA Act enables persons approved by the Director-General of ASIO to exercise the authority conferred by interception warrants issued under Part 2-2 of the TIA Act. Individual staff members of ASD are routinely authorised by the Director-General of ASIO to intercept communications under interception warrants issued under Part 2-2 of the TIA Act.

During 2020–21, ASD finalised its investigation of one incident which constituted a breach of para 7(1)(a) and s 63 of the TIA Act. In this incident, while the interception of foreign communications was authorised by an appropriate warrant, the interception of communications other than foreign communications was not authorised for interception. In sum, an unanticipated technical error resulted in ASD intercepting, and then dealing with, communications other than foreign communications. In reviewing this incident, IGIS found that ASD's actions, including the remedial action taken following the incident, were appropriate in the circumstances.

### INCIDENTS RELATING TO ENABLING INTERCEPTION CONTRARY TO PARA 7(1)(C) OF THE TIA ACT

Paragraph 7(1)(c) of the TIA Act prohibits ASD from enabling the interception of a communication without an appropriate warrant. Generally, 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 are identified.

## NOVEMBER 2020 INCIDENT

During the course of lawful interception of foreign communications under an appropriate warrant, ASD became aware that communications other than foreign communications might be intercepted. Despite being aware of this possibility, as a result of human error ASD failed to cease interception. While no unlawful communications were identified by enabling the interception, ASD nevertheless breached para 7(1)(c) of the TIA Act. IGIS's subsequent review found that ASD's remedial actions, including updating processes and increasing awareness of the associated risks, were appropriate in the circumstances.

## MARCH 2021 INCIDENT

In this incident certain communications were targeted for interception despite not being authorised for interception under an appropriate warrant. Again, this was the result of human error; ASD initially advised IGIS that it considered that this incident did not constitute a breach, as it considered it unlikely that unlawful communications had been enabled for interception and no unlawfully intercepted communications had been identified.

In reviewing this incident, IGIS considered a number of issues regarding the circumstances in which ASD could be said to have enabled interception. IGIS highlighted that while it was unlikely that a person was using the telecommunications service, ASD had enabled the interception of certain communications should they have been made. Following extensive engagement with IGIS on this issue, ASD concurred that the incident was a breach of para 7(1)(c) of the TIA Act as it had enabled the interception of communications without an appropriate warrant. Following ASD's finalisation of the incident, IGIS found that ASD's remedial actions, including updating processes for the targeting of communications, were appropriate in the circumstances.

### **MAY 2021 INCIDENT**

As of 30 June 2021, ASD is continuing to conduct an internal investigation of a breach of para 7(1)(c). IGIS will independently review ASD's investigation and provide findings in the 2021–22 Annual Report.

### **REMAINING INCIDENTS**

ASD also advises IGIS of cases where, during the course of lawful interception of foreign communications under an appropriate warrant, ASD unknowingly and unintentionally enables the interception of communications other than foreign communications. This can occur for a range of reasons. ASD has adopted safeguards to mitigate the occurrence of such incidents and has a practice of informing the minister should they occur. Six such cases were reported to IGIS during the reporting period.

### **INCIDENTS RELATING TO THE IS ACT**

Section 7 of the IS Act sets out the functions of ASD. These include ASD's functions to obtain intelligence, communicate intelligence, prevent and disrupt cybercrime, and the advice and assistance role ASD provides in relation to cyber security. Section 12 of the IS Act restricts ASD's activities to what is necessary for the proper performance of its functions, or as is authorised or required by or under another Act.

During 2020–21, ASD notified IGIS of 2 incidents relating to ASD's compliance with the IS Act.

### **OCTOBER 2020 INCIDENT**

In October 2020, ASD advised that an activity conducted by the ACSC fell outside the scope of ASD's functions. As a result, ASD undertook an activity that was not necessary for the proper performance of its functions and was not otherwise authorised or required by another Act, contrary to s 12 of the IS Act. As part of ASD's cyber security function, the ACSC works with industry to take down websites identified as malicious. In this instance, the ACSC requested a domain host to take down a particular website, however did not first confirm that the website was malicious. The domain host did not comply with the request because the website was not malicious in nature. Nevertheless, the request to take down the website was outside of ASD's functions and was otherwise unnecessary and unauthorised.

ASD advised that this incident occurred due to a combination of human error and a lack of adequate training within the ACSC. Subsequently, ASD undertook a range of measures including increased training and the development of new standard operating procedures. IGIS subsequently reviewed this incident and found that the remedial actions taken by ASD were appropriate in the circumstances.

## MARCH 2021 INCIDENT

The IS Act requires the Minister for Defence to issue a written direction that specifies the circumstances in which ASD must obtain an authorisation before undertaking certain activities. Prior to giving such an authorisation, the Minister for Defence is required to be satisfied that 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, and that the nature and consequences of acts carried out will be reasonable.

In this incident, in obtaining authorisation ASD advised the minister that certain arrangements were in place. However, ASD has advised IGIS that because of human error, these arrangements were not in place at the time ASD conducted the activities. ASD has since undertaken appropriate remedial actions to mitigate recurrence and IGIS is currently reviewing the circumstances of the incident to determine whether it constitutes a breach of the IS Act. The outcomes of this review will be reported in the 2021–22 annual report.

## INSPECTION OF AGO ACTIVITIES

The functions of AGO are set out in s 6B of the IS Act. AGO undertakes a number of activities that carry out these functions, which are categorised as follows:

- intelligence collection in support of the Australian Government
- intelligence collection in support of the ADF, and assistance in support of military operations
- intelligence collection in support of Commonwealth and state authorities carrying out national security functions
- communication of intelligence
- provision of imagery and other geospatial products
- provision of assistance to persons or bodies responsible for functions including emergency response, safety, scientific research, economic development, culture, and environmental protection
- cooperation with, and assistance to, intelligence agencies and prescribed authorities
- the functions of the Australian Hydrographic Office (AHO).

During 2020–21, IGIS inspections focused on:

- AGO's activities concerning Australian persons
- AGO's compliance with relevant legislation, in particular the IS Act
- the propriety of AGO's activities
- AGO's access to sensitive financial information
- the consistency of AGO's activities with human rights.

IGIS inspections of AGO activities are facilitated by regular engagement with AGO's Compliance and Legal staff, and access to required information and systems. The scheduled inspection program is supplemented by proactive reviews of areas that present new or higher risk. IGIS also reviews AGO's existing and proposed policies and procedures to determine whether they are effective and appropriate.

In 2020–21, IGIS conducted a review of AGO's communication of intelligence in certain circumstances. The purpose of this was to provide assurance that AGO's communication of intelligence in these circumstances is consistent with human rights. IGIS officers reviewed AGO's records relating to these activities, including associated policy and procedures, and did not identify any issues of concern.

There are tri-annual meetings between the Inspector-General and the Director of AGO, senior IGIS and senior AGO officers. In 2020–21, themes of these meetings included: AGO's risk management framework; emerging challenges for geospatial-intelligence; capability developments and acquisitions; analytic modernisation; staffing and workplace matters; and relevant legal and propriety subjects. AGO Compliance and Legal staff often consult with IGIS officers regarding ministerial submissions that have particular relevance to oversight arrangements, such as the ministerial directions.

Based on its inspection and review activities, IGIS is satisfied that AGO met its statutory obligations under the IS Act during 2020–21. IGIS is also satisfied that AGO continues to enhance its systems and processes to encourage compliance with legislation and internal procedures.

## **MINISTERIAL AUTHORISATIONS TO UNDERTAKE CERTAIN ACTIVITIES**

The IS Act requires that AGO obtain authorisation from the Minister for Defence before conducting certain activities, including the production of intelligence on an Australian person. This authorisation is commonly requested in conjunction with ASD, but there are instances where AGO seeks an authorisation separately. During 2020–21, IGIS officers reviewed a majority of the ministerial authorisation applications made by AGO. No legal or propriety issues were identified.

## **EMERGENCY AUTHORISATIONS**

Situations may arise where AGO requires a ministerial authorisation to undertake certain activities as a matter of urgency. Emergency authorisations may be provided orally by: the Minister for Defence; other select ministers where the Minister for Defence is unavailable; or the Director of AGO if the ministers are not readily available. Emergency authorisations are valid for 48 hours after which a new authorisation is required if AGO is to continue the activity. AGO did not obtain any emergency ministerial authorisations during 2020–21.

## **REPORTS ON ACTIVITIES CONDUCTED UNDER MINISTERIAL AUTHORISATION**

The IS Act requires that AGO gives the Minister for Defence a written report in respect of each activity carried out in reliance on a ministerial authorisation. As part of regular inspections, IGIS reviews the details of these reports to provide assurance that AGO is reporting accurately, in a timely manner, and in accordance with the requirements of the IS Act.

During 2020–21, IGIS officers inspected a sample of AGO's written reports. No significant issues were identified. However, IGIS suggested that AGO consider including additional detail about activities undertaken during the authorised period. Such additional detail would ensure that the Minister for Defence is more comprehensively informed about the activities being conducted and would better meet the requirements of the IS Act.

## DIRECTOR'S APPROVALS AND POST ACTIVITY REPORTING

The Minister for Defence requires the Director of AGO to approve AGO activities intended to produce geospatial or imagery intelligence on a person or body corporate in Australian territory or subject to Australian jurisdiction, unless the activity is one for which AGO must seek ministerial authorisation. Director's Approvals and relevant documentation were reviewed by IGIS during the reporting period and no issues were identified. At the conclusion of approved activities, AGO staff prepare a post activity compliance report for the Director, which IGIS examines. During 2020–21, no significant issues were identified with such reports.

## COMPLIANCE WITH PRIVACY RULES

The Minister for Defence issues written rules (the AGO Privacy Rules) to regulate AGO's communication and retention of intelligence information about Australian persons. The IS Act prohibits AGO from communicating intelligence information about an Australian person other than in accordance with those rules. The Privacy Rules are publicly available on the AGO website.

The Privacy Rules require AGO to: provide IGIS with access to all of AGO's intelligence holdings concerning Australian persons; consult IGIS about relevant procedures; report to IGIS any breaches of the AGO Privacy Rules; and advise where AGO has revised its determination that a person previously presumed to be foreign is an Australian person.

During 2020–21, IGIS officers regularly reviewed AGO's products to assess compliance with the Privacy Rules. No instances of non-compliance were identified. IGIS considers AGO has a strong focus on training personnel regarding the requirements of the Privacy Rules, including revision of guidance and training when required.

## AUSTRALIAN HYDROGRAPHIC OFFICE

In October 2017, AHO functions were transferred from the Royal Australian Navy to AGO. This transfer resulted in IGIS assuming oversight of the functions of the AHO relating to any intelligence collection or application of the Privacy Rules. The AHO has fully incorporated IS Act requirements into its daily workflows and has received relevant compliance training. Although the AHO primarily conducts 'non-intelligence' activities, AGO's compliance area engages with IGIS regarding instances where intelligence or privacy matters concerning Australian persons need to be considered with regard to AHO products. Additional oversight of the AHO is also provided by requests for information under the FOI Act as is laid out in the AHO Ministerial Direction.

In 2020–21, IGIS was unable to conduct planned outreach and inspection activities at the Wollongong site due to COVID-19 restrictions. Pending the finalisation of infrastructure upgrades at the Wollongong site, IGIS officers will conduct outreach and inspection activities during the next reporting period.

## INSPECTION OF DIO ACTIVITIES

DIO produces strategic all source intelligence assessments. DIO is part of the Department of Defence and operates under a Mandate issued by the Secretary for Defence and the Chief of Defence Force. DIO supports:

- the planning and conduct of ADF operations
- Defence Department policy, planning and decision-making



- the development and sustainment of Defence capability
- wider government planning and decision-making on defence and national security issues.

To fulfil its role, DIO is mandated to provide:

- assessment, advice and services to support the planning, command and conduct of current and potential ADF operations
- timely assessments of the interests, posture, policy, intent and capabilities of countries and foreign non-state actors relevant to Australia's security
- technical assessment of weapons systems, cyber threats and defence-related technologies
- specialist advice to support whole of government strategies, including to counter proliferation and combat terrorism.

DIO does not have legislated powers to conduct covert or intrusive activities. Accordingly, IGIS's regular inspections concentrate on areas of greater risk including risks to the privacy of Australian persons, analytic integrity, and the handling of sensitive financial information. In addition, IGIS receives briefings and undertakes proactive reviews and monitoring of areas and programs where there may be increased legislative, propriety or human rights risks.

The Inspector-General and the Chief of Defence Intelligence, who is 'dual-hatted' as Director DIO, met several times over the reporting period to discuss oversight issues. Oversight of DIO activities are facilitated by regular contact with DIO's Engagement team. IGIS also reviews DIO policies and procedures, where relevant, to determine whether they appropriately address compliance concerns.

## COMPLIANCE WITH PRIVACY GUIDELINES

DIO has a set of Privacy Guidelines signed by the Minister for Defence that allow it to perform its role while respecting the privacy of Australians. The Privacy Guidelines are similar to the privacy rules established under s 15 of the IS Act for ASD, ASIS and AGO and under s 53 of the ONI Act. The Privacy Guidelines are published on DIO's website.

IGIS's inspection of compliance with Privacy Guidelines found one matter where there was a significant delay in the application of the guidelines. DIO subsequently reviewed the relevant policies and procedures to give clearer guidance in these matters in regards to joint intelligence products.

## ENSURING ANALYTIC INTEGRITY

DIO is not subject to direction in regard to the judgements in its intelligence assessments. IGIS conducts analytic integrity inspections of DIO assessments, examining large numbers of published products and associated records to confirm independence and analytic rigour. IGIS found no areas of significant concern and considered that the majority of intelligence products and records reviewed were of a high standard. IGIS considers that DIO's training regime and policies and procedures reflect a commitment to analytic integrity.

## CROSS-AGENCY MATTERS

During the reporting period, IGIS conducted inspections that covered activities common to a number of agencies.

## USE OF ASSUMED IDENTITIES

Part IAC of the *Crimes Act 1914* (Crimes Act) and corresponding state and territory laws enable ASIO, ASIS and ONI 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 Crimes Act.

The Crimes Act also imposes reporting, administration and audit regimes on those agencies using assumed identities. Section 15LG of the Crimes Act requires ASIO, ASIS and ONI to conduct 6-monthly audits of assumed identity records and s 15LE requires that each agency provide the Inspector-General with an annual report containing information on the assumed identities created and used during the year. During 2020–21 the Director-General of ASIO, the Director-General of ASIS and the Director-General of ONI each provided IGIS with a report covering the activities of their respective agencies for the 2019–20 reporting period. In relation to ASIS and ONI, IGIS is satisfied from the reports that there are no issues of concern and that these agencies are complying with their legislative responsibilities.

Section 15KF of the Crimes Act requires periodic reviews of assumed identities to determine whether use of the assumed identity is still necessary. ASIO's report identified that for the period of 1 January 2020 to 30 June 2020 almost all assumed identity reviews did not comply with the review timeframes set out in s 15KF, and for the period 1 July 2019 to 31 December 2019 a high percentage of reviews did not comply with the required review timeframes. ASIO assessed that these breaches resulted in part from an undetected technical issue that occurred during data migration to a new assumed identity management system. This technical issue resulted in staff not receiving automated reminders. ASIO's report also identified several issues concerning automated verification of a delegate's authority in circumstances where an officer is acting in another position. ASIO proactively briefed IGIS on the technical issues and on the additional investigation it had undertaken to identify any other instances of noncompliance. ASIO advised IGIS that it has implemented technical changes to its systems to address the identified errors, and that it has amended its internal policies for the management of assumed identities. IGIS has considered the incident and is satisfied with ASIO's remediation measures. IGIS will review the effectiveness of these measures in the next reporting period.

Separate to its annual report, ASIO notified IGIS of an additional 5 assumed identities that were not reviewed within the required statutory timeframes. ASIO assessed that the same technical issues and also an administrative error during data migration had resulted in the breaches. Following identification of the breaches, ASIO completed the required reviews. IGIS has considered the incident and is satisfied with ASIO's notification and remediation action.

In addition, ASIO notified IGIS of a breach of para 15KI(4)(a) of the Crimes Act. Paragraph 15KI(4)(a) requires that when requesting evidence of an assumed identity, the request must include the date of the authority granted under s 15B. During a review by ASIO, one instance was identified where the authority date was not included. This matter remained under assessment by ASIO at the end of the reporting period and IGIS will consider ASIO's response following this assessment.

ASIO can obtain assumed identities under the *NSW Law Enforcement and National Security (Assumed Identities) Act 2010*. The Director-General is a 'chief officer' for the purposes of this Act and ASIO officers may apply to the Director-General for authority to obtain or use an assumed identity, including on behalf of any other person or foreign officer. Under subs 39(3),

the Director-General may delegate this function to up to 5 nominated position holders. In November 2020, ASIO advised that it considered a 2016 delegation instrument issued under subs 39(3) was likely to be defective as it exceeded the maximum number of delegations that may be in place at any one time. ASIO noted that the delegation instrument had not been used since it was issued. ASIO took steps to revoke the instrument. IGIS is satisfied with ASIO's assessment of this breach and timeliness of remediation action.

## ACCESS TO SENSITIVE FINANCIAL INFORMATION BY INTELLIGENCE AGENCIES

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AMLCTF Act) provides a legal framework for designated agencies to access and share financial intelligence information created or held by AUSTRAC. All intelligence agencies and IGIS are designated agencies for the purposes of the Act.

IGIS is party to a memorandum of understanding with AUSTRAC. This memorandum of understanding records an agreed understanding of IGIS's role in monitoring agencies' access to and use of AUSTRAC information.

In monitoring the use of AUSTRAC information by intelligence agencies, IGIS officers verify 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. IGIS prepares an annual statement summarising compliance monitoring in respect of each of the intelligence agencies and their access to, use and protection of AUSTRAC information in the preceding financial year. This statement is provided to relevant ministers and to the AUSTRAC Chief Executive Officer.

As part of its inspection program IGIS inspected ASIO's use of AUSTRAC material over 2019–20. IGIS identified one instance where internal ASIO approval was inappropriately granted to communicate AUSTRAC information in contravention of the AMLCTF Act. The approval was later rescinded and no information was communicated. While IGIS is satisfied that in this instance no information was communicated, IGIS noted that, at the time of the inspection, the recommendations of a 2017 internal ASIO audit that identified a number changes to policies and procedures were yet to be fully implemented. ASIO subsequently updated its internal policies and procedures to ensure officers have a clearer understanding of these obligations.

In July 2020, ASIO notified IGIS of an incident where AUSTRAC information was communicated to an overseas partner agency without ASIO first receiving the required undertakings from that agency. ASIO assessed the incident to be a breach of s 133 of the AMLCTF Act, with which IGIS agreed. The matter was reported to the Minister for Home Affairs and the AUSTRAC Chief Executive Officer as part of IGIS's annual compliance reporting. IGIS notes that ASIO has subsequently updated its internal policies and procedures to ensure officers have a clearer understanding of these obligations. IGIS will consider the effective implementation of these policies and procedures in its annual inspection program.

IGIS also conducted an inspection of ASIS records relating to AUSTRAC information from 2019–20, and also reviewed ASIS's use of AUSTRAC material during other inspection work where relevant. IGIS found that ASIS's governance and record keeping in relation to AUSTRAC information continue to be effective, and no instances of non-compliance in using such information was observed.

During the reporting period, IGIS officers similarly reviewed ASD, AGO, DIO and ONI access to, use and protection of sensitive financial information through 2019–20. These inspections revealed no instances of non-compliance regarding the access to, use and protection of AUSTRAC information. These agencies continued to have limited interaction with AUSTRAC material during the reporting period, and did not access any information directly via online access to AUSTRAC databases. IGIS is satisfied that ONI, ASD, AGO and DIO have effective procedures in place with regard to the handling of AUSTRAC information.

### COVIDSAFE APP PROJECT

Privacy protections specifically related to the collection of personal information through the COVIDSafe app are set out in Part VIIIA of the *Privacy Act 1988* (Privacy Act).

Part VIIIA sets out offences for the collection, use and disclosure of COVID app data. Part VIIIA also provides an exception to the offence of collecting COVID app data where that collection occurs incidentally to the collection of lawfully intercepted information. No offence is committed if the incidentally collected COVID app data is deleted as soon as practicable after an agency becomes aware that it has been collected, and if the data has not been accessed, used or disclosed after it was collected. These protections and exemptions are of particular relevance for IGIS oversight of the activities of intelligence agencies.

In 2020, IGIS established a project to identify those agencies within its jurisdiction that were most likely to collect COVID app data incidentally, and to determine if those agencies were complying with the protections and exemptions of Part VIIIA of the Privacy Act. IGIS is undertaking this project in cooperation with the Australian Information Commissioner who, under the Privacy Act, has independent oversight responsibilities of the COVIDSafe app.

The Inspector-General has provided the Australian Information Commissioner with 2 reports on the assurance activities undertaken by IGIS officers. These reports are available on the IGIS website and cover the periods 16 May 2020 to 16 November 2020, and 16 November 2020 to 15 May 2021.

The first report concluded that IGIS was satisfied that the relevant agencies had policies and procedures in place and were taking reasonable steps to avoid intentional collection of COVID app data. The report foreshadowed that IGIS inspections would verify data deletion and provide further assurance that no COVID app data has been accessed, used or disclosed.

The second report similarly concluded that the relevant agencies were taking reasonable steps to avoid intentional collection of COVID app data and that appropriate procedures for incidental collection remained in place and continued to be followed. The report noted that relevant agencies have incidentally collected COVID app data, which the Privacy Act recognises may occur. However no evidence was found to suggest that agencies have deliberately targeted or have decrypted, accessed or used such data. Further, the Inspector-General found that relevant agencies were taking reasonable steps to quarantine and delete such data as soon as practicable after the agency became aware of its collection. Finally, IGIS noted that discussions were ongoing between relevant parties about the application of the prohibition against 'disclosure' as set out in s 94D of the Privacy Act.

IGIS will continue to inspect how intelligence agencies incidentally collect and delete COVID app data, in compliance with the Privacy Act, until such time as use of the COVIDSafe app is discontinued by the Government and all related COVID app data has been deleted.

## ACTIVITIES RELATING TO THE ACIC, AFP AND AUSTRAC

### PROPOSED EXPANSION OF IGIS ROLE

While the final form and timing of any expanded jurisdiction as set out in the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 remains a matter for the Government and Parliament, IGIS has continued to build the necessary relationships and its understanding of the activities of the ACIC, AFP and AUSTRAC, and is developing interim inspection plans accordingly.

### OUTREACH

During 2019–20, IGIS continued to engage with key contacts and senior managers with the ACIC, AFP, and AUSTRAC to assist in obtaining an in-depth understanding of the intelligence activities of each of these agencies and how these activities fit within their broader functions. This engagement has included liaison visits, special operational and capability briefings, observation of inspection by OCO officers and regional visits. Outreach activities have also focused on exploring the potential role the Inspector-General would play in the oversight of these new agencies, and ascertaining possible jurisdictional limits.

## OBJECTIVE 4 – COMPLAINTS AND PUBLIC INTEREST DISCLOSURES

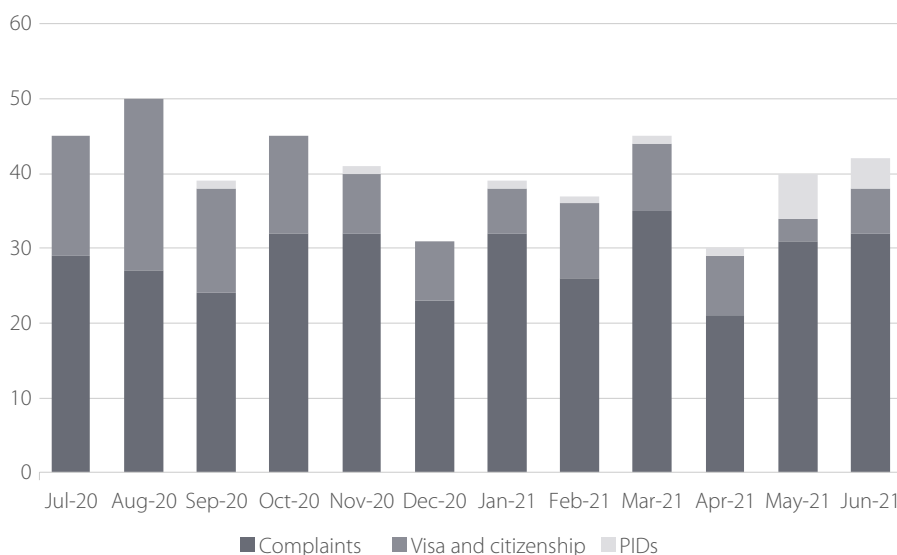
### IGIS'S COMPLAINTS JURISDICTION

IGIS has a broad jurisdiction to receive and inquire into complaints concerning the conduct of intelligence agencies. In previous reporting periods, IGIS distinguished between 'complaints' that were within IGIS's jurisdiction and 'contacts' for grievances raised that did not come within IGIS's jurisdiction. The high level of resources required to receive, consider and respond to all contacts made to IGIS is not best recognised under this demarcation and IGIS has made some adjustments and refinements to its reporting framework. Accordingly, this report does not distinguish between 'contacts' and 'complaints', and any comparison between the previous reporting periods and the current reporting period should take into account this change.

**Figure 2.3: Summary of 2020–21 complaints and PID statistics**

	2020/2021 FY (1 July 2020 – 30 June 2021)	Previous Year Totals (1 July 2019 – 30 June 2020)
Complaints	344*	35
Contacts*	N/A	180
Visa and citizenship complaints	124	300
PIDs	16	2

\*Complaints received via the IGIS web form are automatically entered as complaints in Resolve, the IGIS complaints case management system. In some cases these were found to be PIDs and the complaints were closed in Resolve, but are reflected in the total number of complaints.

**Figure 2.4: Number of complaints/PIDS received per month 2020–21**

### COMPLAINTS (NON-VISA AND CITIZENSHIP RELATED)

In the reporting period, there was a significant increase in the number of grievances lodged with IGIS from 215 in 2019–20 to 344 in 2020–21 (non-visa and citizenship related complaints). The average time taken to acknowledge complaints was 3 business days. IGIS officers responded to 83% of complaints within 5 business days, which was slightly less than the target performance measure of 90%. These slight delays in acknowledging complaints are attributed to available resources.

Each complaint received is assessed to determine the most appropriate course of action required to resolve the concerns raised, including whether the matter is most appropriately dealt with under the IGIS Act or the PID Act. The Inspector-General is authorised under s 14 of the IGIS Act to conduct a preliminary inquiry to determine whether IGIS can, or should, inquire further into a matter. Of the 344 complaints received, 177 were determined to fall outside IGIS's jurisdiction. In all such cases, where possible, advice was provided to complainants about where they could direct their concerns. Complainants were provided with advice about actions that have been taken in response to their concerns and the outcomes, to the extent possible within IGIS security obligations.

During the reporting period, IGIS sought agency information related to complaints by speaking with relevant agency staff, reviewing files and undertaking independent searches of agency databases to identify issues of legality or propriety. IGIS officers utilised established relationships with agency staff to enable most matters to be resolved in a timely manner.

On completion of the complaint investigation, all complainants were given advice regarding the action IGIS had taken in response to their complaints, IGIS consideration of agency briefings and records, and how any concerns were resolved. Where appropriate, complainants were also invited to contact IGIS again if they continued to have concerns relating to their original complaint.

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

- seizure of property under warrant
- security assessments for employment
- access to records
- complaint handling
- surveillance
- employment issues including recruitment processes
- management of security-related action.

## COMPLAINTS ABOUT VISA AND CITIZENSHIP APPLICATIONS

IGIS receives a number of complaints concerning the processing of visa and citizenship applications, particularly about the length of time taken to finalise an application beyond the indicative timeframes listed on the Department of Home Affairs website.

In the 2020–21 reporting period, there was a significant reduction in the number of complaints IGIS received about visa and citizenship applications from 300 in 2019–20 to 124 in 2020–21. In previous periods the majority of visa and citizenship related complaints were about delays in finalising student visa applications. The decrease in the number of visa and citizenship complaints received during this reporting period is likely due to COVID-19 travel related restrictions, particularly for international students.

While a number of visa or citizenship applications were the subject of processing delays, no compliance issues were identified in any of the visa and citizenship complaints investigated in 2020–21.

## COMPLAINT REVIEWS

For security reasons it is usually not possible to give complainants a complete picture of how their matters have been handled by the agency concerned and by IGIS. This means advice to complainants may be general in nature and this is often one of the reasons complainants seek a review of the way their complaint was handled.

Late in the reporting period, IGIS commenced one review into the handling and outcome of a complaint on request of the complainant. The review was ongoing at the time of this report.

## IGIS'S HANDLING OF PUBLIC INTEREST DISCLOSURES

IGIS 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.

IGIS has 14 authorised officers under the PID scheme in addition to a principal officer (the Inspector-General). These officers are accessible to the intelligence agencies in the course of their regular attendance at agencies for routine activities such as inspections and briefings. IGIS authorised officers are also contactable via email and phone.

IGIS received 16 PIDs relating to intelligence agencies during the reporting period, a significant increase on the previous period. Of the disclosures made to IGIS:

- no disclosable conduct was reported in relation to IGIS
- two disclosures were allocated to intelligence agencies for investigation
- one disclosure was allocated to IGIS and investigated under the PID Act by an external investigator
- seven disclosures were allocated to the IGIS for investigation, and closed in accordance with subs 49(2) of the PID Act for investigation under the IGIS Act
- two matters were closed without further investigation under s 48 of the PID Act.

Of the 16 PIDs received by IGIS, the kinds of disclosable conduct (as specified in s 29 of the PID Act) disclosed to IGIS during the reporting period included maladministration, danger to health or safety, conduct which could lead to disciplinary action, contraventions of Commonwealth, State or Territory law and abuse of a position of trust. One PID may relate to one or more agencies, and one or more kinds of disclosable conduct.

**Figure 2.5: PIDs by agency and conduct 2020–21**

Disclosable conduct	ASIO	ASIS	ASD
Maladministration	5	1	8
Danger to health or safety	2	–	1
Could lead to disciplinary action against a public official	2	–	1
Contravenes a law of the Commonwealth, State or Territory	–	–	4
Abuse of position of trust	–	1	–

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

In accordance with para 44(1A)(b) of the PID Act, intelligence agencies are required to meet certain reporting requirements, which include informing IGIS when a PID is allocated for investigation by an intelligence agency.

During the reporting period IGIS was advised of 13 PIDs received by the intelligence agencies. The agencies advised of the actions taken in each matter, including when the matter was being investigated under more appropriate legislation. Agencies discussed PID-related issues with IGIS, including whether concerns raised by staff reached the PID threshold and regarding investigation decisions.

IGIS has statutory responsibilities for assisting agency staff in their obligations under the PID Act and for conducting training and awareness raising exercises. While COVID-19 limited IGIS's ability to provide its usual range of assistance, IGIS engaged regularly with intelligence agencies on the handling of PID matters throughout the reporting period.



## OBJECTIVE 5 – INFRASTRUCTURE AND STAKEHOLDERS

### INFRASTRUCTURE AND GOVERNANCE

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

In mid-2020, IGIS installed a custom case management system and an electronic records management system on its PROTECTED-level ICT system. An updated classified Local Area Network was installed at the end of 2020. Following further refinement of the PROTECTED-level electronic records management system and case management systems, versions of these systems will be installed on the classified Local Area Network as appropriate. The Office is in the process of finalising an Information Governance Framework and continues to refine its governance and management of digital information assets.

The Office continues to be supported by external agencies through memoranda of understanding for services including property maintenance, payroll and finance processing, and ICT.

The Office has implemented a number of recommendations following an internal governance review in 2020. The Office has expanded its governance team with specialist governance officers to provide oversight of governance functions, risk and compliance, and human resources. Work continues to implement all recommendations from the internal governance review and outcomes will be reported in the next Annual Report.

### LIAISON WITH DOMESTIC 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 the twice yearly 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.

### PROPOSED EXPANSION OF IGIS ROLE

In December 2020, 2 bills were introduced into Parliament that propose to expand the jurisdiction of the Inspector-General: the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 and the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020. At the end of the reporting period, both bills are currently subject to inquiry by the PJCIS. The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 as introduced would provide new law enforcement powers to the AFP and ACIC to combat online serious crime. One of these new powers is a network activity warrant, which would allow the AFP and ACIC to collect intelligence on criminal networks operating online. Given network activity warrants would be an intelligence collection tool, the Bill provides IGIS with oversight responsibility for these warrants and allows IGIS and the Commonwealth Ombudsman to share relevant information.

The Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 responds to recent reviews of Australia's intelligence bodies and the legal framework.

The *2017 Independent Intelligence Review* recommended a number of changes to Australia's intelligence bodies, including the expansion of the jurisdiction of the Inspector-General to include the intelligence functions of the ACIC, AFP, AUSTRAC and Department of Home Affairs. Subsequently, the Comprehensive Review of the Legal Framework of the National Intelligence Community (Comprehensive Review), released in December 2020, considered that existing oversight mechanisms were sufficient for the AFP and Home Affairs (excluding the AFP's network activity warrants). Soon after the release of the Comprehensive Review, the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 was introduced into Parliament. The Bill proposes, among other things, to amend the IGIS Act to extend IGIS's jurisdiction to include the intelligence functions of the ACIC and AUSTRAC, in accordance with the findings of the Comprehensive Review.

Although the final form and timing of changes remains a matter for the Government and Parliament, IGIS has implemented a number of initiatives to ensure its capability and readiness to expand across its jurisdictional oversight. This has included building relationships and its understanding of the activities of the ACIC, AUSTRAC and relevant activities of the AFP. IGIS has engaged with key contacts and senior managers within the ACIC, AFP and AUSTRAC to further its understanding of the relevant functions of each agency. Following the introduction of the 2 bills, IGIS has focused this engagement to ensure its technical preparedness to undertake an expanded oversight role, including proposed arrangements for managing network activity warrants.

IGIS has also engaged with other accountability and integrity agencies on measures to ensure future changes to oversight processes are complementary and avoid overlap. Agreement-in-principle has been reached with other agencies and a Statement of Cooperation will be finalised following passage of any legislation to expand the jurisdiction of IGIS.

### AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

IGIS continued to liaise with the Australian Commission for Law Enforcement Integrity 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 *Australian Human Rights Commission Act 1986* to refer to the Inspector-General any human rights and discrimination matters relating to an act or practice of security agencies. During 2020–21, the Australian Human Rights Commission did not refer any such matters.

### INSPECTOR-GENERAL OF THE AUSTRALIAN DEFENCE FORCE

IGIS liaised with the Inspector-General of the ADF on matters of mutual interest. The Inspector-General and acting Deputy Inspector-General attended the Commonwealth Inspectors-General Meeting on 17 May 2021, chaired by the Inspector-General of the ADF.

### 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 COVID app data by relevant intelligence agencies, and their policies and procedures in place relating to Part VIIIA of the *Privacy Act 1988*. IGIS officers and Office of the Australian Information Commissioner met on matters of mutual interest during the reporting period.

## OFFICE OF THE COMMONWEALTH OMBUDSMAN

IGIS continued to engage regularly with the OCO. 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 come within the jurisdiction of both offices.

## INTERNATIONAL ENGAGEMENT WITH ACCOUNTABILITY AND INTEGRITY AGENCIES

IGIS also liaises with international accountability and integrity agencies. This gives agencies opportunities to learn from each other's practices, discuss oversight responsibilities in relation to emerging issues, and keep informed of developments in other jurisdictions.

## FIVE EYES INTELLIGENCE OVERSIGHT AND REVIEW COUNCIL

In 2020–21, the Inspector-General and IGIS officers continued to engage with the FIORC. The FIORC is comprised of the following intelligence oversight, review and security entities of the Five Eyes countries:

- IGIS 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.

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

It is usual for FIORC members to meet in person at least once each year; however in the 2020–21 period the annual conference did not occur due to COVID-19 travel restrictions. FIORC members have continued to meet via teleconference every few months, and are exploring options for conducting a virtual conference later in 2021.

At the conclusion of the 2019 FIORC annual conference, members agreed to establish working level committees on 3 topics: automated data processing and Artificial Intelligence; methods to mitigate risks of mistreatment from sharing information with foreign entities; and jurisdictional or territorial constraints on the review/oversight activities of FIORC partners that create a gap in coverage over the cumulative activities of the Five Eyes agencies.

In the 2019–20 Annual Report, IGIS noted it is developing a set of principles outlining the Inspector-General's expectations of how agencies should act to minimise the risk of information communicated to foreign entities being used by those entities in a manner inconsistent with the prohibitions on torture, cruel or inhuman treatment and punishment, and unlawful killing. IGIS has been developing these principles in liaison with Australia's intelligence agencies. This work was not able to be progressed during 2019–20 due to resource constraints and the impacts of the COVID-19 staff working arrangements. IGIS intend to progress this work in 2021–22.

## OBJECTIVE 6 – HIGH-PERFORMING WORKFORCE

In 2020–21, the Office continued its focus on recruiting, developing and retaining a capable and motivated workforce. Eleven recruitment rounds were conducted for specialist and oversight officer positions, with some remaining to be finalised in 2021–22. Specialist officers have been recruited to fill key enabling functions such as human resources, governance, procurement and information management. Recruitment continues to be a challenge for the Office due to the lengthy process associated with high level security clearances, but the Office continues to review recruitment strategies and processes to ensure recruitment is targeted and as flexible and efficient as possible.

Twelve new officers joined the Office in 2020–21, completing induction training within their first week followed by an orientation session within the first 3 months. One officer's orientation training was conducted after 3 months due to staff availability over the Christmas/January period. Capability has also been a focus in 2020–21 as the Office positions itself for current and future growth. Induction and orientation programs have been revised and training conducted to equip officers with the skills to negotiate a changing office environment. A capability framework is under development to formalise internal professional development options. Phase one of this framework was rolled out in the first half of 2021, with the second phase to be developed in the coming reporting period. Additionally, internally presented professional development seminars have been supplemented by training and information sessions led by guest presenters and through external training opportunities.

The IGIS performance management framework includes performance expectations and encourages officers to identify professional development opportunities. Over the reporting period, enhancements were made to the performance management agreement to incorporate APS and security obligations, structured professional development options aligned with phase one of the capability framework as well as guidance for managers. A comprehensive review of the performance management framework will be conducted in 2021–22 which will allow additional initiatives from the capability framework to be incorporated into performance management.

Formal flexible working arrangements were utilised throughout 2020–21, in addition to temporary or ad hoc arrangements agreed between staff and their supervisor. Changing COVID-19 restrictions, which often occurred at short notice, meant several officers worked remotely for brief periods during quarantine while interstate or on return to Canberra.

In late 2020, it was agreed between IGIS and AGD for IGIS staff to access AGD's Reconciliation Action Plan and participate in AGD Reconciliation Action Plan initiatives and events. An IGIS specific plan that is calibrated for the size of the Office will be considered in the next reporting period.

# **SECTION THREE**

## MANAGEMENT AND ACCOUNTABILITY

# CORPORATE GOVERNANCE

## ORGANISATIONAL STRUCTURE

Senior positions occupied during 2020–21 were as follows:

### **Inspector-General of Intelligence and Security (Statutory officer)**

The Honourable Margaret Stone AO FAAL, appointed 24 August 2015. Ms Stone's term as Inspector-General ended on 23 August 2020.

The Honourable Christopher Jessup QC, was appointed to the role of acting Inspector-General on 18 January 2021 and was substantively appointed to the position on 8 February 2021.

### **Deputy Inspector-General of Intelligence and Security (SES Band 2)**

Mr Jake Blight, appointed to the SES Band 2 Deputy Inspector-General on 23 October 2018. Mr Blight was the SES Band 1 Deputy Inspector-General under the previous organisational structure from January 2012. Mr Blight was Acting Inspector-General from 24 August 2020 to 17 January 2021.

Ms Bronwyn Notzon-Glenn was appointed Acting Deputy Inspector-General from 24 August 2020 to 17 January 2021. Ms Notzon-Glenn was again appointed Acting Deputy Inspector-General from 1 February 2021 until the end of the reporting period.

### **Assistant InspectorsGeneral of Intelligence and Security (SES Band 1)**

Mr Stephen McFarlane, appointed 8 February 2018. Ms Notzon-Glenn, appointed 28 February 2019. Mr Brad Fallen was appointed Acting Assistant Inspector-General from 24 August 2020 to 17 January 2021 and again from 1 February 2021 until the end of the reporting period.

## SENIOR MANAGEMENT COMMITTEES

The Office's corporate governance framework provides for 2 senior management committees.

The Executive Committee meets weekly and comprises the Inspector-General, Deputy Inspector-General and the 2 Assistant Inspectors-General. The Executive Committee assists the Inspector-General and SES to set the strategic direction of the Office and oversee its administration.

The Senior Officers Meeting is held weekly and comprises the Inspector-General, the Deputy Inspector-General, the 2 Assistant Inspectors-General and the Directors. The Senior Officers Meeting assists the Inspector-General with strategic planning, monitoring and reporting, and aligns priorities across the agency.

## CORPORATE AND ORGANISATIONAL PLANNING

The Office's corporate and operational planning processes have been enhanced during 2020–21 to support and further prepare for the growth of the Office. This has included the development and enhancement of frameworks for information governance, reporting structures, capability and risk management.

The Office addresses organisational planning through:

- an annual forward planning process to set strategic priorities and a mid-cycle review
- weekly Executive Committee meetings
- weekly Senior Officers Meetings
- monthly meetings between the Inspector-General and IGIS teams during which current operational matters and priorities are discussed
- a forward plan for inspection activities in each intelligence agency, which is determined in consultation with the relevant agency head (in accordance with s 9A of the IGIS Act)
- And other ad hoc meeting as are required.

## INTERNAL AUDIT AND RISK MANAGEMENT

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 IGIS's financial and performance reporting responsibilities, system of risk oversight and management, and system of internal control.

The membership and functions of the IGIS Audit Committee are structured according to the PGPA Act. The charter for the IGIS Audit Committee is available at <https://www.igis.gov.au/about/finance>.

During 2020–21 the IGIS Audit Committee membership comprised of:

**Figure 3.1: IGIS Audit Committee membership 2020–21**

Member name	Qualifications, knowledge, skills or experience	Number of meetings attended / total number of meetings as a member	Total annual remuneration (\$)
<b>Ms Sarah Vandenbroek</b> (Chair)	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.	4/4	0
<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.	4/4	0
<b>Mr Jake Blight<sup>1</sup></b>	Mr Blight holds a Bachelor of Arts/ Bachelor of Law and Graduate Diploma in Legal Practice and is a graduate of the Australian Institute of Company Directors course. He was a departmental member of the IGIS Audit Committee for 7 years, as well as having been on the audit committee for 2 other Commonwealth agencies.	2/4	0



Member name	Qualifications, knowledge, skills or experience	Number of meetings attended / total number of meetings as a member	Total annual remuneration (\$)
<b>Ms Bronwyn Notzon-Glenn<sup>2</sup></b>	Ms Notzon-Glenn holds a Bachelor of Arts (Honours)/Bachelor of Laws (Honours) and is admitted to practice in the ACT Supreme Court. Ms Notzon-Glenn brings experience in the Australian Parliament and several years' experience as a Senior Executive Officer and now Acting Deputy Inspector-General.	1/4	0
<b>Mr Stephen Moore<sup>3</sup></b> Independent 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 <i>Australia and New Zealand School of Government</i> 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.	3/4	1,980

1. Term ended 22 August 2020

2. Term commenced 3 September 2020. Term ended 14 December 2020

3. Term commenced 2 November 2020

The Inspector-General, Deputy Inspector-General, IGIS Officers and Australian National Audit Office (ANAO) representatives may attend Audit Committee meetings to provide updates or as an observer.

The Audit Committee meets 4 times a year to consider matters including:

- risk management
- internal control
- financial statements
- compliance requirements
- internal audit
- external audit
- governance arrangements.

During 2020–21, the Office undertook a comprehensive review of its risk management practices and developed a new Risk Management Policy and Framework and updated Risk Register. The framework provides a structured and consistent approach to identifying, analysing and mitigating risk.

The Audit Committee reviews the Risk Management Policy and Framework and the IGIS Risk Register annually based on its assessment of the risk performance over the period. The Risk Register includes controls designed to mitigate identified risks across the following categories:

- business continuity and disaster recovery
- cyber
- fraud
- health, safety and wellbeing
- legal compliance
- organisational resources (financial and workforce)
- reputation
- security.

Through the various mitigation strategies applied in the Risk Register, the residual risk accepted by the Office is maintained in the low to moderate levels in each of the categories.

The IGIS internal audit program is focused on areas which pose the greatest risk to the Office's functions, and is developed in consultation with the IGIS Audit Committee. In 2019–20 and 2020–21, 2 internal audits were completed on wages compliance and leave liabilities. Both audits led to recommendations for improvements which have been implemented. The Audit Committee receives regular updates on the progress of internal audit recommendations.

## ETHICAL STANDARDS AND FRAUD CONTROL

During 2020–21, the Office continued its commitment to high ethical standards and having high performing and professional staff. High ethical standards across the Office are maintained through:

- APS integrity and values training
- modelling of appropriate behaviours by the agency's SES
- a requirement that all IGIS officers maintain a high level security clearance
- annual declaration of known conflicts of interest by the SES and all IGIS officers
- 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.

## EXECUTIVE REMUNERATION DISCLOSURES

The Inspector-General is a statutory office holder. In addition, the Office has 3 SES positions: one SES Band 2 position and 2 SES Band 1 positions. 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 subs 24(1) determinations and are based broadly on SES remuneration within the Attorney-General's Department. Each subs 24(1) determination is reviewed annually with the Inspector-General, with more general performance discussions occurring during the year. The Inspector-General's remuneration is determined by the Remuneration Tribunal. The Office does not have a performance pay scheme. Details are in Annexure 5.2: Key Management Personnel.

## EMPLOYMENT OF PERSONS FOR A PARTICULAR INQUIRY

Subsection 35(2AA) of the IGIS Act requires the annual report to comment on the employment under subs 32(3) of any person to perform functions and exercise powers for the purposes of a particular inquiry, and any delegation under s 32AA to such a person. Ms Renee Leon was employed under this provision during 2020–21.

## ISSUES RELATING TO SIGNIFICANT NON-COMPLIANCE WITH THE FINANCE LAW

There were no significant issues relating to non-compliance with the finance law during 2020–21 that would be reportable to the responsible minister under p 19(1)(e) of the PGPA Act.

# EXTERNAL SCRUTINY

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

In 2019–20, the Office was audited by the ANAO to examine the extent to which the IGIS has implemented the Digital Continuity 2020 policy. The ANAO report made one recommendation for IGIS, with which the Office agreed. The Office is developing and implementing a coherent strategy to address ANAO's recommendation including through an implementation plan developed by the Office's recently appointed information governance specialist. The Office made a submission to the Joint Committee of Public Accounts and Audit on 25 February 2021 and appeared before the Committee on 14 April 2021 to provide an update on the implementation of the ANAO Report's recommendation for the Office. This includes the development and implementation of an Information Governance Framework, including key components of ensuring the Office's risk framework addresses information management and the establishment of a reporting mechanism to manage compliance, risk and business needs. As part of this process the Office is also undertaking a review of all information management policies and updating them where necessary.

The Office has received an unqualified audit report from the ANAO in relation to its financial statements.

Further details of the Office's interaction with parliamentary committees are available in the Annual Performance Statement section of this report.

## DECISIONS BY THE JUDICIARY, TRIBUNALS OR THE INFORMATION COMMISSIONER

During 2020–21, there were no judicial decisions, or decisions of administrative tribunals or the Information Commissioner that had, or may have, a significant impact on the operations of the Office.

## CAPABILITY REVIEWS

No capability reviews of the Office were released during 2020–21.

# MANAGEMENT OF HUMAN RESOURCES

## ORGANISATIONAL PROFILE

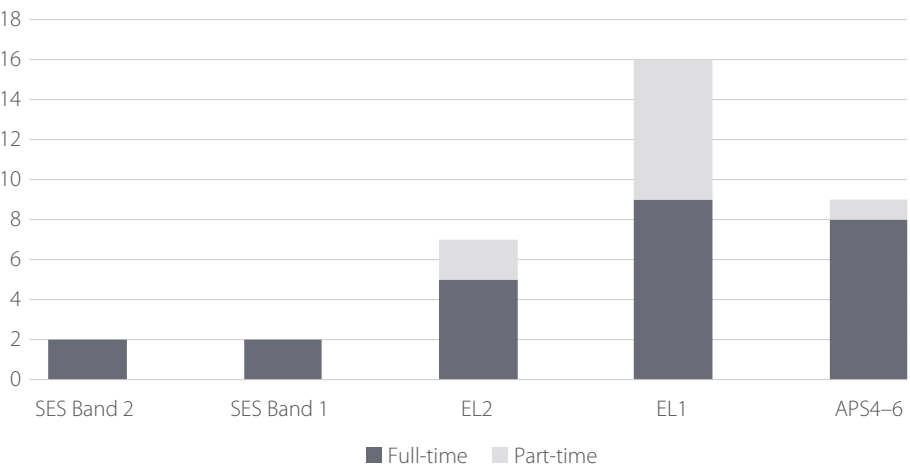
At 30 June 2021, the Office had 35 ongoing APS employees located in the ACT. The Inspector-General is a statutory officer and therefore not an employee. Ten APS employees worked part-time on individual flexibility agreements for part-time work, under the Office of the IGIS Enterprise Agreement 2020–23. One APS employee was employed on a non-ongoing basis.

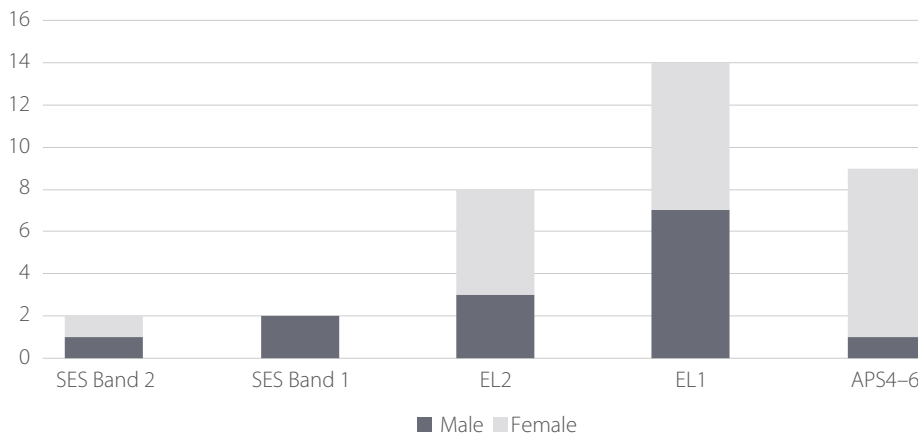
At 30 June 2020, the Office had 33 ongoing APS employees located in the ACT (not including the Inspector-General). Five APS employees worked part-time. No APS employee was employed on a non-ongoing basis in 2019–20.

No employees identified as Indigenous in 2020–21 or 2019–20.

The profile of the organisation is summarised in the following graphs:

**Figure 3.2: Organisational Profile as at 30 June 2021 (by classification and status)**



**Figure 3.3: Gender Balance as at 30 June 2021 (by classification)**

## EMPLOYMENT FRAMEWORKS

All IGIS officers are employed under the *Public Service Act 1999*. Since 6 May 2020, all non-SES officers salaries and conditions were made under the Office of the IGIS Enterprise Agreement 2020–2023. Three SES officers are presently employed in accordance with individual determinations under subs 24(1) of the *Public Service Act 1999*.

The salary range available to APS employees in the Office throughout the reporting period is provided at Annexure 5.1.

The only notable non-salary benefit for IGIS non-SES officers is a taxable annual allowance in recognition of the requirement to undergo regular and intrusive security clearance processes necessary to maintain a Positive Vetting clearance, as well as other restrictions placed on employees as a result of reviewing the activities of the intelligence agencies. The annual allowance is \$1,205.

## EMPLOYEE PERFORMANCE 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. In recognition of its anticipated expanded jurisdiction, IGIS will seek to develop the capability of its expanded workforce and to retain its current skilled staff complement.

Particular importance is placed on the retention of staff, flexible working arrangements, and workplace training to promote leadership skills and capability development. IGIS's human resources and learning and development function continues to mature and further work is being done to strengthen IGIS's professional development. Opportunities provided now include Australian Public Service Commission's management and leadership courses, National Centre for Intelligence Training and Education programs and courses with the Australian National University's National Security College.

IGIS's Performance Agreements links individual roles and development goals with organisational needs and provides the mechanism for supervisors to guide and develop staff performance.

## PERFORMANCE PAY

The Office does not have a performance pay scheme.

# 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, 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 and 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 payment 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

**Figure 3.4: Reportable consultancy contracts 2020–21**

Reportable consultancy contracts 2020–21	Number	Expenditure \$
New contracts entered into during the reporting period	7	174,403
Ongoing contracts entered into during a previous reporting period	3	155,681
<b>Total</b>	<b>10</b>	<b>330,084</b>



**Figure 3.5: Reportable consultancy contract expenditure 2020–21**

Organisations receiving a share of reportable consultancy contract expenditure 2020–21	New (\$)	Ongoing (\$)	Grand Total (\$)
Axiom Associates (Aust) Pty Ltd	27,857.00		27,857.00
BellChambersBarrett	29,429.00		29,429.00
Business Journey	770.00		770.00
Esprit Psychology		59,312.33	59,312.33
Jones Lang LaSalle Australia Pty Limited	2,750.00		2,750.00
Professional Career Coaching	2,032.00		2,032.00
Renee Leon		28,600.00	28,600.00
The ITSM Hub Pty Ltd	1,980.00		1,980.00
Wilson Psychology		67,768.82	67,768.82
Yardstick Advisory Pty Ltd	109,584.00		109,584.00
<b>Grand Total</b>	<b>174,403.33</b>	<b>155,681.15</b>	<b>330,084.48</b>
<b>Count</b>	<b>7</b>	<b>3</b>	

During 2020–21, 7 new consultancy contracts were entered into involving total actual expenditure in 2020–21 of \$174,403 (including GST). In addition, 3 ongoing consultancy contracts were active during the period, involving total actual expenditure of \$155,681 (including GST).

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.

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 take into account the abilities and resources required for the task, the skills available internally, and the cost-effectiveness of engaging external expertise.

Annual reports contain information about actual expenditure on contracts for consultancies. Information on the value of contracts and consultancies is available on the AusTender website, [www.tenders.gov.au](http://www.tenders.gov.au).

## AUSTRALIAN NATIONAL AUDIT OFFICE (ANAO) ACCESS CLAUSES

The Office's use of the Commonwealth Contracting Suite ensures all contracts for low-risk 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 2020–21, 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.

## DISABILITY REPORTING MECHANISM

The *National Disability Strategy 2010–2020* 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.

All levels of government will continue to be held accountable for the implementation of the strategy through biennial progress reporting to the National Cabinet. Progress reports can be found at [www.dss.gov.au](http://www.dss.gov.au). 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).

## 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 FOUR**

FINANCIAL

MANAGEMENT



## 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 2021:

- (a) comply with Australian Accounting Standards – Reduced Disclosure Requirements and the *Public Governance, Performance and Accountability (Financial Reporting) Rule 2015*; and
- (b) present fairly the financial position of the Entity as at 30 June 2021 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 2021 and for the year then ended:

- Statement by the Inspector-General of Intelligence and Security;
- 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 2021 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 – Reduced Disclosure Requirements

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

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



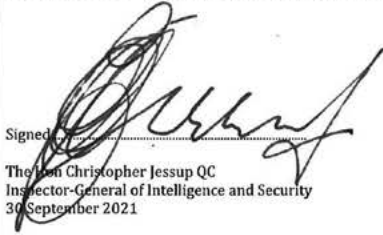
Rebecca Reilly  
Executive Director  
Delegate of the Auditor-General  
Canberra  
30 September 2021

## OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

## STATEMENT BY THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2021 comply with subsection 42(2) of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), and are based on properly maintained financial records as per subsection 41(2) of the PGPA Act.

In my opinion, at the date of this statement, there are reasonable grounds to believe that the Office of the Inspector-General of Intelligence and Security will be able to pay its debts as and when they fall due.

Signed 

The Hon Christopher Jessup QC  
Inspector-General of Intelligence and Security  
30 September 2021

## Statement of Comprehensive Income

for the period ended 30 June 2021

	Notes	2021 \$	2020 \$	Original Budget \$
<b>NET COST OF SERVICES</b>				
<b>Expenses</b>				
Employee benefits	1.1A	5,241,113	5,006,248	9,500,000
Suppliers	1.1B	1,973,596	1,631,263	2,429,000
Depreciation and amortisation	2.2A	1,260,053	922,988	2,564,000
Finance costs	1.1C	149	188	-
Write-down and impairment of other assets	1.1D	47,745	-	-
<b>Total expenses</b>		<b>8,522,656</b>	<b>7,560,687</b>	<b>14,493,000</b>
<b>Own-source income</b>				
<b>Own-source revenue</b>				
Revenue from contracts with customers	1.2A	35,224	31,266	-
Other revenue	1.2B	40,000	39,508	27,000
<b>Total own-source revenue</b>		<b>75,224</b>	<b>70,774</b>	<b>27,000</b>
<b>Total own-source income</b>		<b>75,224</b>	<b>70,774</b>	<b>27,000</b>
<b>Net (cost of)/contribution by services</b>		<b>(8,447,432)</b>	<b>(7,489,913)</b>	<b>(14,466,000)</b>
Revenue from Government	1.2C	11,908,000	12,356,000	11,908,000
<b>Surplus/(Deficit) attributable to the Australian Government</b>		<b>3,460,568</b>	<b>4,866,087</b>	<b>(2,558,000)</b>
<b>OTHER COMPREHENSIVE INCOME</b>				
<b>Items not subject to subsequent reclassification to net cost of services</b>				
Changes in asset revaluation reserve	2.2A	(7,358)	-	-
<b>Total other comprehensive income</b>		<b>(7,358)</b>	<b>-</b>	<b>-</b>
<b>Total comprehensive income/(loss)</b>		<b>3,453,210</b>	<b>4,866,087</b>	<b>(2,558,000)</b>

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

### Budget Variances Commentary

#### Statement of Comprehensive Income

##### Employee Benefits

The full year variance is reflective of the difference in the associated cost of budgeted ASL (55) and actual ASL (33). Delays in on-boarding staff are linked to the extensive time to complete security related pre-employment processes. In 2021-22, ASL will increase significantly as recruitment efforts from 20-21 materialise and also given there was a starting FTE of 38 at 30 June 2021.

##### Suppliers

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

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.

**Statement of Financial Position***as at 30 June 2021*

	Notes	2021 \$	2020 \$	Original Budget \$
<b>ASSETS</b>				
<b>Financial assets</b>				
Cash and cash equivalents	2.1A	228,304	221,012	221,000
Trade and other receivables	2.1B	26,262,819	25,872,197	26,370,000
<b>Total financial assets</b>		<b>26,491,123</b>	<b>26,093,209</b>	<b>26,591,000</b>
<b>Non-financial assets</b>				
Leasehold Improvements	2.2A	1,852,212	2,519,419	2,497,000
Property, plant and equipment	2.2A	1,290,352	1,671,802	-
Right-of-use	2.2A	9,122	15,756	-
Intangibles	2.2A	652,029	847,659	1,001,000
Other non-financial assets	2.2B	149,298	16,305	32,000
<b>Total non-financial assets</b>		<b>3,953,013</b>	<b>5,070,941</b>	<b>3,530,000</b>
<b>Total assets</b>		<b>30,444,136</b>	<b>31,164,150</b>	<b>30,121,000</b>
<b>LIABILITIES</b>				
<b>Payables</b>				
Suppliers	2.3A	266,086	273,695	-
Other payables	2.3B	225,318	105,991	251,000
<b>Total payables</b>		<b>491,404</b>	<b>379,686</b>	<b>251,000</b>
<b>Interest bearing liabilities</b>				
Leases	2.4A	9,210	15,832	16,000
<b>Total interest bearing liabilities</b>		<b>9,210</b>	<b>15,832</b>	<b>16,000</b>
<b>Provisions</b>				
Employee provisions	4.1A	1,727,923	1,598,377	2,260,000
<b>Total provisions</b>		<b>1,727,923</b>	<b>1,598,377</b>	<b>2,260,000</b>
<b>Total liabilities</b>		<b>2,228,537</b>	<b>1,993,895</b>	<b>2,527,000</b>
<b>Net assets</b>		<b>28,215,599</b>	<b>29,170,255</b>	<b>27,594,000</b>
<b>EQUITY</b>				
Contributed equity		10,446,301	14,854,167	15,855,000
Reserves		14,265	21,623	22,000
Retained surplus		17,755,033	14,294,465	11,717,000
<b>Total equity</b>		<b>28,215,599</b>	<b>29,170,255</b>	<b>27,594,000</b>

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

**Budget Variances Commentary****Statement of Financial Position**Non-Financial Assets

The variance relates predominantly to prior and current year capital acquisitions not materialising to the extent of that budgeted. The impact of the COVID-19 pandemic and lower ASL affected planned capital acquisition activities. Additionally, by having a lower asset base, the depreciation and amortisation expense generated is lower.

Supplier Payables

The variance relates to the timing of supplier invoices received and accrued at 30th June 2021.

Employee Provisions

The variance is reflective of the difference in the provision for a budgeted ASL (55) compared to actual ASL (33) at 30 June 2021.



## Statement of Changes in Equity

for the period ended 30 June 2021

	Notes	2021 \$	2020 \$	Original Budget \$
<b>CONTRIBUTED EQUITY</b>				
<b>Opening balance</b>				
Balance carried forward from previous period		14,854,167	12,371,167	14,854,000
<b>Opening balance</b>		<b>14,854,167</b>	<b>12,371,167</b>	<b>14,854,000</b>
<b>Transactions with owners</b>				
<b>Distributions to owners</b>				
Return of capital		(5,408,866)	-	-
<b>Contributions by owners</b>				
Departmental capital budget		1,001,000	2,483,000	1,001,000
<b>Total transactions with owners</b>		<b>(4,407,866)</b>	<b>2,483,000</b>	<b>1,001,000</b>
<b>Closing balance as at 30 June</b>		<b>10,446,301</b>	<b>14,854,167</b>	<b>15,855,000</b>
<b>RETAINED EARNINGS</b>				
<b>Opening balance</b>				
Balance carried forward from previous period		14,294,465	9,428,378	14,275,000
<b>Opening balance</b>		<b>14,294,465</b>	<b>9,428,378</b>	<b>14,275,000</b>
<b>Comprehensive income</b>				
Surplus/(Deficit) for the period		3,460,568	4,866,087	(2,558,000)
<b>Total comprehensive income</b>		<b>3,460,568</b>	<b>4,866,087</b>	<b>(2,558,000)</b>
<b>Closing balance as at 30 June</b>		<b>17,755,033</b>	<b>14,294,465</b>	<b>11,717,000</b>
<b>ASSET REVALUATION RESERVE</b>				
<b>Opening balance</b>				
Balance carried forward from previous period		21,623	21,623	22,000
<b>Opening balance</b>		<b>21,623</b>	<b>21,623</b>	<b>22,000</b>
<b>Comprehensive income</b>				
Other comprehensive income		(7,358)	-	-
<b>Total comprehensive income</b>		<b>(7,358)</b>	<b>-</b>	<b>-</b>
<b>Closing balance as at 30 June</b>		<b>14,265</b>	<b>21,623</b>	<b>22,000</b>
<b>TOTAL EQUITY</b>				
<b>Opening balance</b>				
Balance carried forward from previous period		29,170,255	21,821,168	29,151,000
<b>Opening balance</b>		<b>29,170,255</b>	<b>21,821,168</b>	<b>29,151,000</b>
<b>Comprehensive income</b>				
Surplus/(Deficit) for the period		3,460,568	4,866,087	(2,558,000)
Other comprehensive income		(7,358)	-	-
<b>Total comprehensive income</b>		<b>3,453,210</b>	<b>4,866,087</b>	<b>(2,558,000)</b>
<b>Transactions with owners</b>				
<b>Distributions to owners</b>				
Return of capital		(5,408,866)	-	-
<b>Contributions by owners</b>				
Departmental capital budget		1,001,000	2,483,000	1,001,000
<b>Total transactions with owners</b>		<b>(4,407,866)</b>	<b>2,483,000</b>	<b>1,001,000</b>
<b>Closing balance as at 30 June</b>		<b>28,215,599</b>	<b>29,170,255</b>	<b>27,594,000</b>

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. 3) 2017-18 - DCB of \$5,408,866 was quarantined under sunset clauses and returned to the Official Public Account on the 1 July 2020.

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

## Cash Flow Statement

for the period ended 30 June 2021

	Notes	2021 \$	2020 \$	Original Budget \$
<b>OPERATING ACTIVITIES</b>				
<b>Cash received</b>				
Appropriations		7,281,647	6,925,682	11,410,000
Net GST received		101,405	127,621	-
Other		239,429	367,273	27,000
<b>Total cash received</b>		<b>7,622,481</b>	<b>7,420,576</b>	<b>11,437,000</b>
<b>Cash used</b>				
Employees		5,274,406	4,665,766	9,000,000
Suppliers		2,175,220	2,536,690	2,429,000
Interest payments on lease liabilities		149	188	-
Section 74 receipts transferred to OPA		204,205	350,418	-
<b>Total cash used</b>		<b>7,653,980</b>	<b>7,553,062</b>	<b>11,429,000</b>
<b>Net cash from/(used by) operating activities</b>		<b>(31,499)</b>	<b>(132,486)</b>	<b>8,000</b>
<b>INVESTING ACTIVITIES</b>				
<b>Cash used</b>				
Purchase of property, plant and equipment		3,578	309,125	1,001,000
Purchase of intangibles		60,657	-	-
<b>Total cash used</b>		<b>64,235</b>	<b>309,125</b>	<b>1,001,000</b>
<b>Net cash (used by) investing activities</b>		<b>(64,235)</b>	<b>(309,125)</b>	<b>(1,001,000)</b>
<b>FINANCING ACTIVITIES</b>				
<b>Cash received</b>				
Contributed equity		109,648	363,104	999,000
<b>Total cash received</b>		<b>109,648</b>	<b>363,104</b>	<b>999,000</b>
<b>Cash used</b>				
Principal payments of lease liabilities		6,622	6,746	6,000
<b>Total cash used</b>		<b>6,622</b>	<b>6,746</b>	<b>6,000</b>
<b>Net cash from financing activities</b>		<b>103,026</b>	<b>356,358</b>	<b>993,000</b>
<b>Net increase/(decrease) in cash held</b>		<b>7,292</b>	<b>(85,253)</b>	<b>-</b>
Cash and cash equivalents at the beginning of the reporting period		221,012	306,265	221,000
<b>Cash and cash equivalents at the end of the reporting period</b>	2.1A	<b>228,304</b>	<b>221,012</b>	<b>221,000</b>

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

### Budget Variances Commentary

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

## Overview

### Objectives

The Office of the Inspector-General of Intelligence and Security (OIGIS) is an Australian Government controlled entity. It is a not-for-profit entity. The objective of OIGIS is 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 general purpose financial statements and 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 – Reduced Disclosure Requirements issued by the Australian Accounting Standards Board (AASB) that apply for the reporting period.

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

The financial statements are presented in Australian dollars.

### New Accounting Standards

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.

### Taxation

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

### Contingent Assets and liabilities

OIGIS has no contingent assets or liabilities to report at 30 June 2021 (2020: Nil).

### 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.

**1.1 Expenses**

	2021	2020
	\$	\$
<b>1.1A: Employee benefits</b>		
Wages and salaries	4,298,549	3,873,085
Superannuation		
Defined contribution plans	396,713	409,763
Defined benefit plans	288,236	275,486
Leave and other entitlements	257,615	447,914
<b>Total employee benefits</b>	<b>5,241,113</b>	<b>5,006,248</b>

**Accounting Policy**

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

	2021	2020
	\$	\$
<b>1.1B: Suppliers</b>		
<b>Goods and services supplied or rendered</b>		
Audit Fees	35,000	35,000
Consultants and Contractors	435,168	123,952
ICT and Communication	525,556	404,930
Insurance	18,941	10,146
Legal	19,329	48,996
Property	598,497	573,679
Recruitment and HR	144,948	99,620
Security Vetting	56,618	95,011
Training	63,395	50,086
Travel	20,978	120,623
Other	47,602	55,211
<b>Total goods and services supplied or rendered</b>	<b>1,966,032</b>	<b>1,617,254</b>
<b>Other suppliers</b>		
Workers compensation expenses	7,564	14,009
<b>Total other suppliers</b>	<b>7,564</b>	<b>14,009</b>
<b>Total suppliers</b>	<b>1,973,596</b>	<b>1,631,263</b>

	2021	2020
	\$	\$
<b>1.1C: Finance costs</b>		
Interest on lease liabilities	149	188
<b>Total finance costs</b>	<b>149</b>	<b>188</b>

The above lease disclosures should be read in conjunction with the accompanying notes 2.2A and 2.4A.

	2021	2020
	\$	\$
<b>1.1D: Write-down and impairment of other assets</b>		
Revaluation decrements	47,745	-
<b>Total write-down and impairment of other assets</b>	<b>47,745</b>	<b>-</b>

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

**1.2 Own-Source Revenue and gains**

	2021	2020
	\$	\$

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

Rendering of services – provision of staff car parking facilities	35,224	31,266
<b>Total revenue from contracts with customers</b>	<b>35,224</b>	<b>31,266</b>

**Accounting Policy**

Revenue from the sale of goods is recognised when control has been transferred to the buyer.

**Rendering of Services**

OIGIS provides staff with access to onsite car parking facilities. Agreements are in place for the recovery of anticipated associated Fringe Benefits Tax (FBT) expenses on a fortnightly basis via payroll deductions. 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 and is reviewed at the commencement of each FBT reporting period.

	2021	2020
	\$	\$

**1.2B: Other revenue**

Resources received free of charge		
Australian National Audit Office	35,000	35,000
Australian Signals Directorate	5,000	4,508
<b>Total other revenue</b>	<b>40,000</b>	<b>39,508</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.

	2021	2020
	\$	\$

**1.2C: Revenue from Government**

Appropriations		
Departmental appropriations	11,908,000	12,356,000
<b>Total revenue from Government</b>	<b>11,908,000</b>	<b>12,356,000</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 the entity 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.

## 2.1 Financial Assets

	2021	2020
	\$	\$

### 2.1A: Cash and cash equivalents

Cash on hand or on deposit	228,304	221,012
<b>Total cash and cash equivalents</b>	<b>228,304</b>	<b>221,012</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.

### 2.1B: Trade and other receivables

#### Appropriation receivables

Appropriation receivable	26,153,449	25,840,404
<b>Total appropriation receivables</b>	<b>26,153,449</b>	<b>25,840,404</b>

#### Other receivables

GST receivable from the Australian Taxation Office	15,053	15,436
Other	94,317	16,357
<b>Total other receivables</b>	<b>109,370</b>	<b>31,793</b>
<b>Total trade and other receivables (net)</b>	<b>26,262,819</b>	<b>25,872,197</b>

All other receivables are expected to be recovered within 12 months.

#### Accounting Policy

Receivables for goods and services, which have 30 day terms, are recognised at the nominal amounts due less any allowance for impairment. Collectability of debts is reviewed as at end of reporting period.

All financial assets are assessed for impairment at the end of each reporting period based on expected credit losses. Impairment of trade receivables is assessed on lifetime credit losses. The amount of the loss is measured as the difference between the assets carrying amount and the present value of estimated future cash flows discounted at the asset's original effective interest rate. The loss is recognised in the Statement of Comprehensive Income.

**2.2 Non-Financial Assets****2.2A: Reconciliation of the Opening and Closing Balances of Property, Plant and Equipment and Intangibles**

	Leasehold Improve- ments \$	Property, plant and equipment \$	Right-of- use Asset \$	Intangibles \$	Total \$
<b>As at 1 July 2020</b>					
Gross book value	3,407,348	1,856,901	22,390	1,002,119	<b>6,288,758</b>
Adjustments in disclosure of asset classes - Gross book value	-	154,460	-	(154,460)	-
Accumulated depreciation, amortisation and impairment	(887,929)	(339,559)	(6,634)	-	<b>(1,234,122)</b>
<b>Total as at 1 July 2020</b>	<b>2,519,419</b>	<b>1,671,802</b>	<b>15,756</b>	<b>847,659</b>	<b>5,054,636</b>
Additions					
Purchase	-	3,578	-	60,657	<b>64,235</b>
Revaluations and impairments recognised in:					
- Other comprehensive income	14,265	(21,623)	-	-	<b>(7,358)</b>
- Net cost of services	-	(47,745)	-	-	<b>(47,745)</b>
Depreciation and amortisation	(681,472)	(315,660)	(6,634)	(256,287)	<b>(1,260,053)</b>
<b>Total as at 30 June 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>Total as at 30 June 2021 represented by</b>					
Gross book value	<b>1,852,212</b>	<b>1,290,352</b>	<b>22,390</b>	<b>908,316</b>	<b>4,073,270</b>
Accumulated depreciation, amortisation and impairment	-	-	<b>(13,268)</b>	<b>(256,287)</b>	<b>(269,555)</b>
<b>Total as at 30 June 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>

No indicators of impairment for any of the above listed asset classes were identified at 30 June 2021.

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.

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

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



**Accounting Policy****Acquisition of Assets**

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. Financial assets are initially measured at their fair value plus transaction costs where appropriate.

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

**Asset Recognition Threshold**

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

**Lease Right of Use (ROU) Assets**

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.

An impairment review is undertaken for any right of use lease asset that shows indicators of impairment and an impairment loss is recognised against any right of use lease asset that is impaired. Lease ROU assets continue to be measured at cost after initial recognition in Commonwealth agency, GGS and Whole of Government financial statements.

**Revaluations**

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

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

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

All revaluations are independent and are conducted in accordance with the stated revaluation policy. An Asset Valuation at 30 June 2021 of all Leasehold Improvements and Property, plant and equipment assets 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 the entity 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:

	2021	2020
Leasehold improvements	5 years	5 years
Plant and equipment	1 - 11 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 2021. Where indications of impairment exist, the assets' recoverable amount is estimated and an impairment adjustment made if the assets' recoverable amount is less than its carrying amount.

At 30 June 2021, no indicators of impairment were identified.

**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 agency 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 life of the entity's software is 3 years (2020: 3 years).

All software assets were assessed for indications of impairment as at 30 June 2021.

	2021	2020
	\$	\$
<b>2.2B: Other non-financial assets</b>		
Prepayments	149,298	16,305
<b>Total other non-financial assets</b>	<b>149,298</b>	<b>16,305</b>

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

## 2.3 Payables

	2021	2020
	\$	\$

### **2.3A: Suppliers**

Trade creditors and accruals

#### **Total suppliers**

266,086	273,695
<b>266,086</b>	<b>273,695</b>

Supplier payables are expected to be settled within 12 months.

### **2.3B: Other payables**

Salaries and wages

Superannuation

Leave Balance transfers

Other

#### **Total other payables**

99,843	78,797
15,312	10,492
84,273	-
25,890	16,702
<b>225,318</b>	<b>105,991</b>

Other payables are expected to be settled within 12 months.

#### **Accounting Policy**

##### Payables

Liabilities are recognised to the extent that the goods or services have been received (irrespective of having been invoiced).

## 2.4 Interest Bearing Liabilities

	2021 \$	2020 \$
<b>2.4A: Leases</b>		
Lease liabilities	<b>9,210</b>	15,832
<b>Total leases</b>	<b>9,210</b>	15,832

Total cash outflow for leases for the year ended 30 June 2021 was \$6,746 (2020: \$7,174)

### Maturity analysis - contractual undiscounted cash flows

Within 1 year	<b>6,686</b>	6,622
Between 1 to 5 years	<b>2,524</b>	9,210
<b>Total leases</b>	<b>9,210</b>	15,832

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 IBR is the rate at which a similar borrowing could be obtained from an independent creditor under comparable terms and conditions.

The above lease disclosures should be read in conjunction with the accompanying notes 1.1C and 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 the department'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.

**3.1 Appropriations****3.1A: Annual appropriations ('recoverable GST exclusive')****Annual Appropriations for 2021**

	Annual Appropriation \$	Adjustments to appropriation <sup>1</sup> \$	Total appropriation \$	Appropriation applied in 2021 (current and prior years) \$	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 include 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). The budgets form part of ordinary annual services, and are not separately identified in the Appropriation Acts.

**Annual Appropriations for 2020**

	Annual Appropriation \$	Adjustments to appropriation <sup>1</sup> \$	Total appropriation \$	Appropriation applied in 2020 \$	Variance <sup>2</sup> \$
<b>Departmental</b>					
Ordinary annual services	12,356,000	350,418	12,706,418	(7,018,836)	5,687,582
Capital Budget <sup>3</sup>	2,483,000	-	2,483,000	(363,104)	2,119,896
<b>Total Departmental</b>	<b>14,839,000</b>	<b>350,418</b>	<b>15,189,418</b>	<b>(7,381,940)</b>	<b>7,807,478</b>

1. Adjustments include 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). These budgets form part of ordinary annual services, and are not separately identified in the Appropriation Acts.

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

	2021 \$	2020 \$
<b>Departmental</b>		
Appropriation Act (No. 3) 2017-18 - DCB <sup>1</sup>	-	5,408,865
Appropriation Act (No. 1) 2018-19	-	4,967,120
Appropriation Act (No. 1) 2018-19 - DCB <sup>2</sup>	165,352	275,000
Appropriation Act (No. 1) 2019-20	5,058,338	7,372,865
Appropriation Act (No. 1) 2019-20 - Supply Act	5,333,554	5,333,554
Appropriation Act (No. 1) 2019-20 - DCB	1,448,000	1,448,000
Appropriation Act (No. 1) 2019-20 - DCB - Supply Act	1,035,000	1,035,000
Appropriation Act (No. 1) 2020-21	5,100,446	-
Appropriation Act (No. 1) 2020-21 - Supply Act	7,011,759	-
Appropriation Act (No. 1) 2020-21 - DCB	417,000	-
Appropriation Act (No. 1) 2020-21 - DCB - Supply Act	584,000	-
Cash	228,304	221,012
<b>Total Departmental</b>	<b>26,381,753</b>	<b>26,061,416</b>

1. Appropriation lapsed on 1 July 2020 and includes \$3.5 million subject to Administrative Quarantine.

2. Appropriation lapses on 1 July 2021.

### 3.2 Net Cash Appropriation Arrangements

	2021 \$	2020 \$
<b>Total comprehensive income - as per the Statement of Comprehensive Income</b>	<b>3,453,210</b>	<b>4,866,087</b>
<i>Plus</i> : depreciation/amortisation of assets funded through appropriations (departmental capital budget funding and/or equity injections) <sup>1</sup>	<b>1,253,419</b>	916,354
<i>Plus</i> : depreciation of right-of-use assets <sup>2</sup>	<b>6,634</b>	6,634
<i>Less</i> : lease principal repayments <sup>2</sup>	<b>(6,622)</b>	(6,746)
<b>Net Cash Operating Surplus</b>	<b>4,706,641</b>	<b>5,782,329</b>

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 injections. 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.

## 4.1 Employee Provisions

	2021	2020
	\$	\$
<b>4.1A: Employee provisions</b>		
Leave	1,727,923	1,598,377
<b>Total employee provisions</b>	<b>1,727,923</b>	<b>1,598,377</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.

Other long-term employee benefits are measured as net total of the present value of the defined benefit obligation at the end of the reporting period minus the fair value at the end of the reporting period of plan assets (if any) out of which the obligations are to be settled directly.

### Leave

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

The leave liabilities are calculated on the basis of employees' remuneration at the estimated salary rates that will be applied at the time the leave is taken, including the entity'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 2021. The estimate of the present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

### Superannuation

The entity's 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.

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

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

#### 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 and both Assistant Inspectors-General. Key management personnel remuneration is reported in the table below:

	2021 \$	2020 \$
Short-term employee benefits	1,163,688	1,173,706
Post-employment benefits	183,496	164,114
Other long-term employee benefits	81,611	20,662
<b>Total key management personnel remuneration expenses<sup>1</sup></b>	<b>1,428,795</b>	<b>1,358,482</b>

The total number of key management personnel that are included in the above table are 6 (2020: 4). Substantively there still remains 4 key management personnel positions during 2021, however there was a change in the IGIS and acting in the Deputy IGIS role during 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, and the Portfolio Minister.

**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.

During 2020-21 year there were no (2020: Nil) related party transactions to be separately disclosed.



## 5.1 Financial Instruments

	2021	2020
	\$	\$
<b>5.1A: Categories of financial instruments</b>		
<b>Financial assets at amortised cost</b>		
Cash and cash equivalents	228,304	221,012
Trade and other receivables	94,317	16,357
<b>Total financial assets at amortised cost</b>	<b>322,621</b>	<b>237,369</b>
<b>Total financial assets</b>	<b>322,621</b>	<b>237,369</b>
<b>Financial Liabilities</b>		
<b>Financial liabilities measured at amortised cost</b>		
Suppliers	266,086	273,695
<b>Total financial liabilities measured at amortised cost</b>	<b>266,086</b>	<b>273,695</b>
<b>Total financial liabilities</b>	<b>266,086</b>	<b>273,695</b>

### Accounting Policy

#### Financial assets

In accordance with AASB 9 *Financial Instruments*, the entity classifies its financial assets in the following categories: financial assets measured at amortised cost.

Financial assets are recognised when the entity becomes a party to the contract and, as a consequence, has a legal right to receive or a legal obligation to pay cash and derecognised when the contractual rights to the cash flows from the financial asset expire or are transferred upon trade date.

#### Financial Assets at Amortised Cost

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

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

Amortised cost is determined using the effective interest method.

#### Effective Interest Method

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

OIGIS derived no (2020: Nil) interest income from Financial Assets in 2021.

#### Impairment of Financial Assets

Financial assets are assessed for impairment at the end of each reporting period. Where applicable, a write-off constitutes a derecognition event where the write-off directly reduces the gross carrying amount of the financial asset.

Credit terms are net 20 days (2020: 30 days).

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

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

Settlement is usually made within 20 days (2020: 20 days).

## 5.2 Fair Value Measurement

### 5.2A: Fair value measurement

	Fair value measurements at the end of the reporting period	
	2021	2020
	\$	\$
<b>Non-financial assets</b>		
Leasehold Improvements	1,852,212	2,519,419
Property, plant and equipment	1,290,352	1,671,802
<b>Total Non-financial assets</b>	<b>3,142,564</b>	<b>4,191,221</b>

#### Accounting Policy

The methods utilised to determine and substantiate the unobservable inputs are derived and evaluated 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 has been required to utilise 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 the OIGIS's operational requirements as well as improvements in asset design, materials and technology in determining the modern equivalent asset.

Physical depreciation and obsolescence have 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, we have considered a combination of inquiries made with relevant OIGIS staff, discussion with external suppliers / manufactures and our professional experience with such assets. For all leasehold improvement assets, the consumed economic benefit / asset obsolescence deduction is determined based on the term of the associated lease.

OIGIS engaged the services of an independent valuer, Public Private Property (PPP) to conduct a materiality review of carrying amounts for Leasehold Improvements and property, plant and equipment assets as 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. Comprehensive valuations are carried out at least once every 3 years with a comprehensive valuation conducted at 30 June 2021. PPP has provided written assurance to OIGIS that the models developed are in compliance with AASB 13.

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

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

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

	2021	2020
	\$	\$
<b>Assets expected to be recovered in:</b>		
<b>No more than 12 months</b>		
Cash and cash equivalents	228,304	221,012
Trade and other receivables	26,262,819	25,872,197
Other non-financial assets	147,272	13,121
<b>Total no more than 12 months</b>	<b>26,638,395</b>	<b>26,106,330</b>
<b>More than 12 months</b>		
Leasehold Improvements	1,852,212	2,519,419
Property, plant and equipment	1,290,352	1,671,802
Right-of-use	9,122	15,756
Intangibles	652,029	847,659
Other non-financial assets	2,026	3,184
<b>Total more than 12 months</b>	<b>3,805,741</b>	<b>5,057,820</b>
<b>Total assets</b>	<b>30,444,136</b>	<b>31,164,150</b>
<b>Liabilities expected to be settled in:</b>		
<b>No more than 12 months</b>		
Suppliers	266,086	273,695
Other payables	225,318	105,991
Leases	6,686	6,622
Employee provisions	714,168	380,490
<b>Total no more than 12 months</b>	<b>1,212,258</b>	<b>766,798</b>
<b>More than 12 months</b>		
Leases	2,524	9,210
Employee provisions	1,013,755	1,217,887
<b>Total more than 12 months</b>	<b>1,016,279</b>	<b>1,227,097</b>
<b>Total liabilities</b>	<b>2,228,537</b>	<b>1,993,895</b>

# APPENDIX A: Entity resource statements and resource for outcomes

Figure 4.1: Entity Resource Statement and Resource for Outcomes 2020–21

		Actual available appropriation for 2020–21 \$'000 (a)	Payments made 2020–21 \$'000 (b)	Balance remaining 2020–21 \$'000 (a) – (b)
<b>Ordinary annual services</b>				
<b>Departmental appropriation</b>				
Prior year departmental		20,653	7,384	13,269
Appropriation <sup>1</sup>		1,909	–	12,909
Departmental appropriation <sup>2</sup>		204	–	204
S74 Relevant Agency Receipts				
<b>Total ordinary annual services</b>	<b>A</b>	<b>33,766</b>	<b>7,384</b>	<b>26,382</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>33,766</b>	<b>7,384</b>	<b>26,382</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 \$5,408,866 that was quarantined under sunset clauses and returned to the Official Public Account on the 1st July 2020.

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

**Figure 4.2: 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 2020–21 \$'000 (a)</b>	<b>Actual expenses 2020–21 \$'000 (b)</b>	<b>Variation 2020–21 \$'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>	11,902	7,223	4,679
Special appropriations	–	–	–
Special Accounts	–	–	–
<b>Total for Program 1.1</b>	<b>14,493</b>	<b>8,523</b>	<b>5,970</b>
<b>Outcome 1 Totals by appropriation type</b>			
Departmental expenses			
Departmental appropriation <sup>1</sup>	11,902	7,223	4,679
Special appropriations	–	–	–
Special Accounts	–	–	–
Expenses not requiring appropriation in the Budget year	2,591	1,300	1,291
<b>Total expenses for Outcome 1</b>	<b>14,493</b>	<b>8,523</b>	<b>5,970</b>
	<b>Budget 2020–21</b>	<b>Actual 2020–21</b>	<b>Variation 2020–21</b>
<b>Average Staffing Level (number)</b>	55	33	22

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 FIVE**

## ANNEXURES

# ANNEXURE 5.1

## IGIS SALARY SCALE

The 2020–2023 Enterprise Agreement for IGIS came into effect on 6 May 2020. Remuneration increases were to be averaged across the life of the workplace arrangement as follows:

- 2% - 6 months from commencement
- 2% - 12 months from commencement
- 2% - 24 months from commencement.

**Figure 5.1: IGIS remuneration 2020–2022**

IGIS band	APS level	Salary range	Salary range
		1 July 2020 – 5 May 2021 (\$)	6 May 2021 – 30 June 2022 (\$)
IGIS Band 4	EL2	121,831 – 144,997	124,268 – 147,896
IGIS Band 3	EL1	104,673 – 116,686	106,766 – 119,020
IGIS Band 2	APS6	86,655 – 97,381	88,388 – 99,329
	APS5	75,931 – 82,367	77,450 – 84,014
	APS4	68,210 – 74,215	69,574 – 75,699
IGIS Band 1	APS3	61,346 – 66,064	62,573 – 67,385
	APS2	53,622 – 59,628	54,694 – 60,820
	APS1	48,854 – 52,337	49,831 – 53,383



# ANNEXURE 5.2

## KEY MANAGEMENT PERSONNEL

IGIS had 5 executives who meet the definition of KMP. Their names and length of term as KMP are summarised below:

**Figure 5.2: IGIS KMP 2020-21**

Name	Position	Term as KMP
Margaret Stone	Inspector-General (CEO)	Part year – until 23 August 2021
Christopher Jessup	Inspector-General (CEO)	Part year – from 18 January 2021
Jake Blight	Deputy Inspector-General	Full year
Bronwyn Notzon-Glenn	Acting Deputy Inspector-General	Full year
Stephen McFarlane	Assistant Inspector-General	Full year
Bradley Fallen	Acting Assistant Inspector-General	Part year – from 24 August 2020 to 17 January 2021 and 1 February to 30 June 2021

In the notes to the financial statements for the period ending 30 June 2020, IGIS disclosed the following KMP expenses. In accordance with the PGPA Rule, this information now needs to be further disaggregated in the annual report as follows:

## Key management personnel (KMP)

Name Position title	Short-term benefits		Post-employment benefits		Long-term benefits		Termination benefits	Total remuneration (\$)
	Base salary¹ (\$)	Other benefits and allowances² (\$)	Superannuation contributions (\$)	Long service leave³ (\$)	Other long-term benefits			
<b>Margaret Stone</b> Inspector-General (1 July 2020 to 21 August 2020)	64,855	6,719	5,926	54,490	–	–	–	131,990
<b>Christopher Jessup</b> Inspector-General (18 January 2021 to 30 June 2021)	201,513	26,686	10,847	4,948	–	–	–	243,995
<b>Jake Blight</b> Deputy Inspector-General (1 July 2020 to 30 June 2021)	158,043	16,783	47,258	6,136	–	–	–	228,220
<b>Bronwyn Notzon-Glenn</b> Acting/Deputy Inspector-General (1 July 2020 to 30 June 2021)	243,957	25,917	42,346	6,136	–	–	–	318,356
<b>Steve McFarlane</b> Assistant Inspector-General (1 July 2020 to 30 June 2021)	200,124	25,917	48,355	4,766	–	–	–	279,162
<b>Brad Fallen</b> Acting/Assistant Inspector-General (1 July 2020 to 30 June 2021)	192,951	223	28,763	5,136	–	–	–	227,072

<sup>1</sup> Base salary includes leave taken and the movement in annual leave provision—i.e. 4 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. 9 days accrued per annum less long service leave taken.

All IGIS senior executives are KMP. No KMP or other highly paid staff received bonuses or termination benefits during the period.

# ANNEXURE 5.3

## 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.

### WORK HEALTH AND SAFETY

The following information is provided in accordance with Schedule 2, Part 4 of the *Work Health and Safety Act 2011* (WHS Act).

The Office encourages cooperation with workers and health and safety representatives to promote and develop strategies to ensure health, safety and welfare at work. Workplace health and safety matters are addressed at the Executive Committee meetings, Senior Officers Meetings, Audit Committee meetings and, as the need arises, directly with the Inspector-General through SES, Directors and the Workplace Health and Safety Representative.

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.

### 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.

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 takes into account 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 5.4

## Requirements for annual reports

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.	Mandatory	iv
17AJ(b)	Annexures	Alphabetical index.	Mandatory	127–134
17AJ(c)	Preliminaries	Glossary of abbreviations and acronyms.	Mandatory	vii
17AJ(d)	Annexures	List of requirements.	Mandatory	117
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	2
<b>17AD(b)</b>	<b>Overview of the entity</b>			
17AE(1)(a)(i)	Section 1	A description of the role and functions of the entity.	Mandatory	5
17AE(1)(a)(ii)	Section 1	A description of the organisational structure of the entity.	Mandatory	7
17AE(1)(a)(iii)	Section 1	A description of the outcomes and programmes administered by the entity.	Mandatory	7

PGPA Rule Reference	Part of report	Description	Requirement	Page
17AE(1)(a)(iv)	Section 1	A description of the purposes of the entity as included in corporate plan.	Mandatory	8
17AE(1)(aa)(i)	Section 2	Name of the accountable authority or each member of the accountable authority.	Mandatory	12
17AE(1)(aa)(ii)	Section 2	Position title of the accountable authority or each member of the accountable authority.	Mandatory	12
17AE(1)(aa)(iii)	Section 5	Period as the accountable authority or member of the accountable authority within the reporting period.	Mandatory	113
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 2	Annual performance statement in accordance with paragraph 39(1)(b) of the Act and section 16F of the Rule.	Mandatory	12
<b>17AD(c)(ii)</b>	<b><i>Report on financial performance</i></b>			
17AF(1)(a)	Section 4	A discussion and analysis of the entity's financial performance.	Mandatory	108–109
17AF(1)(b)	Section 4	A table summarising the total resources and total payments of the entity.	Mandatory	108–109

PGPA Rule Reference	Part of report	Description	Requirement	Page
17AF(2)	n/a	If there may be significant changes in the financial results during or after the previous or current reporting period, information on those changes, including: the cause of any operating loss of the entity; how the entity has responded to the loss and the actions that have been taken in relation to the loss; and any matter or circumstances that it can reasonably be anticipated will have a significant impact on the entity's future operation or financial results.	If applicable, Mandatory.	n/a
<b>17AD(d)</b>	<b>Management and accountability</b>			
	<b><i>Corporate governance</i></b>			
17AG(2)(a)	Section 3	Information on compliance with section 10 (fraud systems).	Mandatory	75
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 3	An outline of structures and processes in place for the entity to implement principles and objectives of corporate governance.	Mandatory	70–75

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><i>Audit Committee</i></b>				
17AG(2A)(a)	Section 3	A direct electronic address of the charter determining the functions of the entity's audit committee.	Mandatory	71
17AG(2A)(b)	Section 3	The name of each member of the entity's audit committee.	Mandatory	72–73
17AG(2A)(c)	Section 3	The qualifications, knowledge, skills or experience of each member of the entity's audit committee.	Mandatory	72–73
17AG(2A)(d)	Section 3	Information about the attendance of each member of the entity's audit committee at committee meetings.	Mandatory	72–73
17AG(2A)(e)	Section 3	The remuneration of each member of the entity's audit committee.	Mandatory	72–73
<b><i>External scrutiny</i></b>				
17AG(3)	Section 3	Information on the most significant developments in external scrutiny and the entity's response to the scrutiny.	Mandatory	76
17AG(3)(a)	Section 3	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	76
17AG(3)(b)	Section 3	Information on any reports on operations of the entity by the Auditor-General (other than report under section 43 of the Act), a Parliamentary Committee, or the Commonwealth Ombudsman.	If applicable, Mandatory	76
17AG(3)(c)	Section 3	Information on any capability reviews on the entity that were released during the period.	If applicable, Mandatory	76



PGPA Rule Reference	Part of report	Description	Requirement	Page
<b><i>Management of Human Resources</i></b>				
17AG(4)(a)	Section 2, Section 3	An assessment of the entity's effectiveness in managing and developing employees to achieve entity objectives.	Mandatory	68, 77–79
17AG(4)(aa)	Section 3	Statistics on the entity's employees on an ongoing and nonongoing basis, including the following: <ul style="list-style-type: none"> <li>• statistics on full-time employees</li> <li>• statistics on part-time employees</li> <li>• statistics on gender</li> <li>• statistics on staff location.</li> </ul>	Mandatory	77–78
17AG(4)(b)	Section 3	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 full-time employees</li> <li>• statistics on part-time employees</li> <li>• statistics on gender</li> <li>• statistics on staff location</li> <li>• statistics on employees who identify as Indigenous.</li> </ul>	Mandatory	77–78
17AG(4)(c)	Section 3	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	77
17AG(4)(c)(i)	Section 3	Information on the number of SES and non-SES employees covered by agreements etc identified in paragraph 17AG(4)(c).	Mandatory	77–78

PGPA Rule Reference	Part of report	Description	Requirement	Page
17AG(4)(c)(ii)	Annexures	The salary ranges available for APS employees by classification level.	Mandatory	112
17AG(4)(c)(iii)	Section 3	A description of nonsalary benefits provided to employees.	Mandatory	79
17AG(4)(d)(i)	Section 3	Information on the number of employees at each classification level who received performance pay.	If applicable, Mandatory	79
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 3	An assessment of effectiveness of assets management where asset management is a significant part of the entity's activities.	If applicable, mandatory	80
<b>Purchasing</b>				
17AG(6)	Section 3	An assessment of entity performance against the <i>Commonwealth Procurement Rules</i> .	Mandatory	80
<b>Reportable consultancy contracts</b>				
17AG(7)(a)	Section 3	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	80–81

PGPA Rule Reference	Part of report	Description	Requirement	Page
17AG(7)(b)	Section 3	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	81
17AG(7)(c)	Section 3	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	80–81
17AG(7)(d)	Section 3	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	81
<b>Reportable non-consultancy contracts</b>				
17AG(7A)(a)	Section 3	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	80–81
17AG(7A)(b)	Section 3	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	81

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 3	Additional information, in accordance with section 17AGA, about organisations receiving amounts under reportable consultancy contracts or reportable non-consultancy contracts.	Mandatory	80–81
<b><i>Australian National Audit Office Access clauses</i></b>				
17AG(8)	Section 3	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	81
<b><i>Exempt contracts</i></b>				
17AG(9)	Section 3	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	82

PGPA Rule Reference	Part of report	Description	Requirement	Page
<b>Small business</b>				
17AG(10)(a)	Section 3	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	80
17AG(10)(b)	Section 3	An outline of the ways in which the procurement practices of the entity support small and medium enterprises.	Mandatory	80
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 4	Inclusion of the annual financial statements in accordance with subsection 43(4) of the Act.	Mandatory	86–107
<b>Executive remuneration</b>				
17AD(da)	Section 3, Annexures	Information about executive remuneration in accordance with Subdivision C of Division 3A of Part 23 of the Rule.	Mandatory	78, 114

PGPA Rule Reference	Part of report	Description	Requirement	Page
<b>17AD(f)</b>	<b>Other mandatory information</b>			
17AH(1)(a)(i)	n/a	If the entity conducted advertising campaigns, a statement that <i>"During [reporting period], the [name of entity] conducted the following advertising campaigns: [name of advertising campaigns undertaken]. Further information on those advertising campaigns is available at [address of entity's website] and in the reports on Australian Government advertising prepared by the Department of Finance. Those reports are available on the Department of Finance's website."</i>	If applicable, Mandatory	n/a
17AH(1)(a)(ii)	Annexures	If the entity did not conduct advertising campaigns, a statement to that effect.	If applicable, Mandatory	115
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 3	Outline of mechanisms of disability reporting, including reference to website for further information.	Mandatory	82
17AH(1)(d)	Section 3	Website reference to where the entity's Information Publication Scheme statement pursuant to Part II of FOI Act can be found.	Mandatory	82
17AH(1)(e)	n/a	Correction of material errors in previous annual report.	If applicable, mandatory	n/a
17AH(2)	Annexures	Information required by other legislation.	Mandatory	115–116

# INDEX

## A

- AAT *See* Administrative Appeals Tribunal (AAT)
- Accountable Authority Instructions, 80, 81
- ACIC *See* Australian Criminal Intelligence Commission (ACIC)
- ACSC *See* Australian Cyber Security Centre (ACSC)
- ADF *See* Australian Defence Force (ADF)
- Administrative Appeals Tribunal (AAT), 8, 21, 30
- advertising and market research, 115
- AFP *See* Australian Federal Police (AFP)
- AGD *See* Attorney-General's Department (AGD)
- AGO *See* Australian Geospatial-Intelligence Organisation (AGO)
- AHO *See* Australian Hydrographic Office (AHO)
- AMLCTF Act *See* *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
- ANAO *See* Australian National Audit Office (ANAO)
- annual performance statement, vi, 12–68, 118
  - accountable authority statement, 12
  - analysis, 19–68
  - Objective 1: Assisting Ministers, 19
  - Objective 2: Assuring Parliament *See* assuring Parliament (Objective 2)
  - Objective 3: Informing the public *See* informing the public (Objective 3)
  - Objective 4: complaints and public interest disclosures *See* complaints (Objective 4); public interest disclosures (PIDs) (Objective 4)
  - Objective 4: Inquiries *See* inquiries (Objective 4)
  - Objective 4: Inspections *See* inspections (Objective 4)
  - Objective 5: Infrastructure and stakeholders *See* infrastructure and stakeholders (Objective 5)
  - Objective 6: High-performing workforce, 68 *See also* human resources
  - performance framework 2021–22, 18
  - results, vi, 12–18
  - annual reports, requirements for, 117–126
  - Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, 59
  - Archives Act 1983*, 5, 8, 21
  - ASD *See* Australian Signals Directorate (ASD)
  - ASIO *See* Australian Security Intelligence Organisation (ASIO)
  - ASIS *See* Australian Secret Intelligence Service (ASIS)
  - asset management, 80, 122 *See also* financial statements
  - Assistant Inspector-Generals, 7, 41, 70, 113, 114
  - assisting Ministers (Objective 1), 19
  - assumed identities, 58–59
  - assuring Parliament (Objective 2), 5, 19–21
    - Administrative Appeals Tribunal, 8, 21
    - Australian Information Commissioner, 8, 21
    - Joint Committee of Public Accounts and Audit, 20, 76
    - Parliamentary Joint Committee on Intelligence and Security (PJICIS), 3, 13, 19–20, 24, 48, 65
    - Senate Estimates hearings, 19
    - Senate Finance and Public Administration Legislation Committee, 20
  - Attorney-General, iii, 6, 9, 27, 28, 29, 31, 34, 35, 37, 45
  - Attorney-General's Department (AGD), 3, 65, 75, 115
    - Reconciliation Action Plan, 68
  - Attorney-General's Guidelines, 34, 40
  - Audit Committee, 71, 72–73, 74, 115, 120
  - Auditor-General, 26, 81, 120
    - Implementation of the Digital Continuity 2020 Policy*, 20
    - report, 84–85
  - AusTender, 81, 82, 123, 124
  - AUSTRAC *See* Australian Transaction Reports and Analysis Centre (AUSTRAC)
  - Australian Commission for Law Enforcement Integrity, 3, 66
  - Australian Criminal Intelligence Commission (ACIC), 65, 66
    - IGIS outreach, 61

- Australian Cyber Security Centre (ACSC), 10, 53
- Australian Defence Force (ADF), 10, 41, 48, 54, 56, 57, 66
  - Inspector-General, 66
- Australian Federal Police (AFP), 65, 66
  - IGIS outreach, 61
- Australian Geospatial-Intelligence Organisation (AGO), 5, 10, 20, 25
  - AUSTRAC information, access to, 60
  - Australian Hydrographic Office, 54, 56
  - COVID-19, impact of, 56
  - Director's Approvals, 56
  - functions, 54
  - human rights, 54, 55
  - inspection of activities, 54–56
  - Ministerial authorisations, 55
  - Privacy Rules, 56
- Australian Government Solicitor, 37, 45, 46
- Australian Human Rights Commission, 66
  - Australian Human Rights Commission Act 1986*, 66
- Australian Hydrographic Office (AHO), 54, 56
- Australian Information Commissioner, 3, 8, 21, 60, 66, 76, 120
- Australian National Audit Office (ANAO), 74, 76
  - access clauses, 81, 124
- Australian Privacy Foundation, 22
- Australian Public Service (APS), 18, 79
  - Code of Conduct, 75
  - Ethics Contact Officer Network, 75
  - State of the Service reports*, 82
  - Statistical Bulletin*, 82
  - Values, 75
- Australian Public Service Commissioner, 3
- Australian Secret Intelligence Service (ASIS), 5, 9, 20, 25, 57
  - assumed identities, use of, 58
  - AUSTRAC information, access to, 59
  - Australian persons, intelligence on, 44
  - compliance branch, 44
  - compliance matters, reporting of, 45–46
  - COVID-19, impact of, 41
  - functions, 41
  - human rights, 41, 42, 43
  - inspection of activities, 41–48
  - internal security investigations, 43
  - Ministerial authorisations, 44
  - Ministerial submissions, 44
  - operational files, 42–43
  - Privacy Rules, 42, 44, 45, 46–47
  - public interest disclosures, 64
  - weapons, use of, 41, 47
  - weapons guidelines, changes to, 48
- Australian Security Intelligence Organisation Act 1979*, 9, 26, 27, 28, 29, 30, 31, 32, 35, 37, 40
  - special powers, incidents relating to, 36
- Australian Security Intelligence Organisation Amendment Act 2020*, 28, 37
- Australian Security Intelligence Organisation Amendment Bill 2020, 19
- Australian Security Intelligence Organisation (ASIO), 5, 8, 9, 20, 23, 25
  - analytic rigour and integrity, 30
  - ASIO Act, incidents relating to special powers under, 36
  - assumed identities, use of, 58–59
  - AUSTRAC information, access to, 59
  - Australian government agencies, exchange of information with, 32
  - compliance incidents, review of, 33
  - compulsory questioning, 27, 28
  - data, collection, retention and deletion of, 29
  - force, use of, 29
  - foreign authorities, exchanges of information with, 32
  - foreign partner service, disclosure of information from, 37
  - functions, 26–27
  - human rights, 32
  - human source management, 29–30
  - Inquiry into Australian Security Intelligence Organisation Matter, 24
  - inspection of activities, 26–40
  - internal security, 33
  - internally authorised tracking devices, 37
  - investigative cases, 30



- Ministerial submissions, 31
- Minister's Guidelines, 9, 27, 31, 32, 38, 39, 40
- public interest disclosures, 64
- section 38 (ASIO Act), breaches of, 30–31
- security assessments, 30
- special intelligence operations, 9, 29
- taxation information, access to, 32
- Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, use of powers under, 31
- temporary exclusion orders, 31
- TIA Act *See Telecommunications (Interception and Access) Act 1979*
- warrants *See warrants*
- Australian Signals Directorate (ASD), 5, 10, 20, 25
  - AUSTRAC information, access to, 60
  - functions, 48, 53
  - human rights, 48, 49
  - Inquiry into Australian Signals Directorate matter 2018, 23
  - Inquiry into Australian Signals Directorate matter 2021, 23
  - inspection of activities, 48–54
  - legislative non-compliance, 52–54
  - Ministerial authorisations, 49–50, 54, 55
  - Ministerial submissions, 50–51
  - Privacy Rules, 51, 52, 57
  - public interest disclosures, 64
- Australian Transaction Reports and Analysis Centre (AUSTRAC), 41, 66
  - IGIS outreach, 61
  - intelligence agencies, access by, 59–60
- C**
  - Chief of Defence Force, 10, 56
  - Chief of Defence Intelligence, 57
  - Civil Society Reference Group, 22
  - Code of Conduct (APS), 75
  - Commissioner of Taxation, 32
  - Commonwealth Contracting Suite, 80, 81
  - Commonwealth Electoral Act 1918*, 115
  - Commonwealth Indigenous Procurement Policy, 80
  - Commonwealth Inspectors-General Meeting, 66
  - Commonwealth Ombudsman, 3, 28, 61, 65, 67, 76, 120
  - Commonwealth Procurement Rules, 80, 81, 122
  - complaints (Objective 4), 2, 3, 6, 61–64
    - COVID-19, impact of, 63
    - IGIS's complaints jurisdiction, 61
    - non-visa and citizenship related, 62–63
    - reviews, 63
    - statistics, 61, 62
    - visa and citizenship applications, 16, 61, 63
  - Comprehensive Review of the Legal Framework of the National Intelligence Community, 66
  - consultants, 80–81, 122–124
  - Convention on the Rights of Persons with Disabilities* (UN), 82
  - corporate governance, vi, 3, 7, 16, 70–75, 119–120
    - APS Code of Conduct, 75
    - APS Values, 75
    - Audit Committee, 71, 72–73, 74, 115, 120
    - corporate and organisational planning, 71
    - ethical standards and fraud control, iii, 74, 75, 119
    - Executive Committee, 70, 71, 115
    - executive remuneration, 75, 125
    - finance law, non-compliance with, 75
    - key management personnel, 75, 113–114
    - organisational structure, 7, 70
    - particular inquiry employment, 75
    - Performance Agreements, 75, 79
    - risk management *See risk management*
    - senior management committees, 70
    - Senior Officers Meeting, 70, 71, 115
  - Corporate Plan 2020–21, vi, 8, 12
    - performance criteria, results against, 13–18
  - Counter-Terrorism (Temporary Exclusion Orders) Act 2019*, 31
  - COVID-19 pandemic, 2–3, 14, 16
    - AGO, 56

ASIS, 41

complaints, 63

COVIDSafe app project, 3, 19, 27, 60, 66

governance framework, 3–4

human resources, 2–3, 68

informing the public, 21, 22

infrastructure and stakeholders, 67

ONI, 26

public interest disclosures, 64

travel, 3, 41, 63, 67

*Crimes Act 1914*, 58

*Criminal Code Act 1995*, 36

cross-agency inspections, 57–60

    assumed identities, use of, 58–59

    AUSTRAC information, access to, 59–60

cyber security, 10, 53, 57, 74

    Australian Cyber Security Centre, 10, 53

cybercrime, 48, 53

**D**

Defence Intelligence Organisation (DIO), 5, 10, 20, 25

    analytic integrity, 57

    AUSTRAC information, access to, 60

    functions, 56–57

    human rights, 57

    inspection of activities, 56–57

    Privacy Guidelines, 57

Department of Defence, 10, 56

Department of Home affairs, 63, 66

Deputy Inspector-General, 7, 20, 41, 66, 70, 73, 74, 103, 113, 114

DIO *See* Defence Intelligence Organisation (DIO)

Director-General of ASD, 49, 50

Director-General of ASIO, 52, 58

Director-General of ASIS, 42, 44, 45, 47, 48, 58

Director-General of ONI, 58

Director-General of Security, 27, 32, 34

Director of AGO, 55, 56

disability reporting mechanism, 82, 126

**E**

ecologically sustainable development and environmental performance, 115–116

employment frameworks, 78

Enterprise Agreement 2020–23, 77, 78, 112

*Environment Protection and Biodiversity Conservation Act 1999*, 115

environmental performance *See* ecologically sustainable development and environmental performance

ethical standards and fraud control, iii, 74, 75, 119

Ethics Contact Officer Network (APS), 75

Executive Committee, 70, 71, 115

executive remuneration, 75, 125

exempt contracts, 82, 124

external scrutiny, 76, 120

    ANAO report, 76

    Australian Information Commissioner, 76

    capability reviews, 76

    Joint Committee of Public Accounts and Audit, 20, 76

    judicial/tribunal decisions, 76

**F**

financial statements, 84–109, 118–119, 125

FIORC *See* Five Eyes Intelligence Oversight and Review Council (FIORC)

Five Eyes agencies, vii, 3, 32, 67

Five Eyes Intelligence Oversight and Review Council (FIORC), 3, 67

FOI Act *See* *Freedom of Information Act 1982*

force, use of, 29, 47

fraud control *See* ethical standards and fraud control

*Freedom of Information Act 1982*, 5, 8, 21, 56, 124, 126

    Information Publication Scheme, 82

FRR *See* Public Governance, Performance and Accountability (Financial Reporting) Rule 2015

## G

governance *See* corporate governance  
guide to report, vi

## H

high-performing workforce (Objective 6), 68  
*See also* human resources

human resources, 3–4, 77–79, 121–122

- capability framework, 68
- COVID-19, impact of, 68
- employment frameworks, 78
- high-performing workforce, 68
- organisational profile, 77–78
- Performance Agreements, 75, 79
- performance and development, 79
- performance management framework, 17, 68
- performance pay, 75, 79, 122
- Reconciliation Action Plan (AGD), 68
- recruitment, 4, 18, 63, 68, 87, 93, 100
- remuneration *See* remuneration

human rights

- AGO, 54, 55
- ASD, 48, 49
- ASIO, 32
- ASIS, 41, 42, 43
- Australian Human Rights Commission, 66
- DIO, 57
- IGIS, 5, 8, 22, 25

Human Rights Law Centre, 22

## I

IATDs *See* internally authorised tracking devices (IATDs)

ICT *See* information and communications technology (ICT)

identities, assumed *See* assumed identities

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

*Implementation of the Digital Continuity 2020 Policy* (Auditor-General), 20

Independent Intelligence Review (2017), 3, 20, 66

information and communications technology (ICT), 16, 17, 65, 73

Information Governance Framework, 65, 76

Information Publication Scheme (IPS), 82

informing the public (Objective 3), 21–22

Civil Society Reference Group, 22

COVID-19, impact of, 21, 22

IGIS website, 6, 14, 16, 21, 22, 24, 82

public outreach activities, 22

infrastructure and stakeholders (Objective 5), 65–67

Australian Commission for Law Enforcement Integrity, 3, 66

Australian Human Rights Commission, 66

Australian Information Commissioner, 3, 8, 21, 60, 66, 120

Commonwealth accountability and integrity agencies, liaison with, 65–67

Commonwealth Ombudsman, 3, 28, 61, 65, 67, 76, 120

Comprehensive Review of the Legal Framework of the National Intelligence Community, 66

COVID-19, impact of, 67

Five Eyes Intelligence Oversight and Review Council, 3, 67

IGIS role, proposed expansion of, 3, 61, 65–66, 79

Inspector-General of the Australian Defence Force, 66

Integrity Agencies Group, 3, 65

international engagement, 67

inquiries (Objective 4), 2, 3, 6, 22–24

Australian Security Intelligence Organisation Matter, 24

Australian Signals Directorate matter 2018, 23

Australian Signals Directorate matter 2021, 23

performance indicators, 23

preliminary *See* preliminary inquiries

inspections (Objective 4), 2, 3, 6, 25–60

AGO activities, 54–56

ASD activities, 48–54

ASIO activities, 26–40

ASIS activities, 41–48

cross-agency matters, 57–60

DIO activities, 56–57

ONI activities, 25–26

Inspector-General of Intelligence and Security, 70

annual performance statement *See* annual performance statement

letter of transmittal, iii, 117

review, vi, 2–4

role, vi, 5

*Inspector-General of Intelligence and Security Act 1986*, iii, vi, 2, 5, 6, 8, 12, 15, 19, 21, 22, 23, 24, 25, 62, 64, 66, 71, 75

Inspector-General of the Australian Defence Force, 66

Integrity Agencies Group, 3, 65

Intelligence and Security legislation  
Amendment (Implementing Independent  
Intelligence Review) Bill 2020, 20

Intelligence Oversight and Other Legislation  
Amendment (Integrity Measures) Bill 2020, 3,  
20, 61, 65, 66

*Intelligence Services Act 2001*, 9, 10, 15, 41, 43, 44,  
45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57

internally authorised tracking devices (IATDs),  
37

Investigatory Powers Commissioner's Office  
(UK), 67

IPS *See* Information Publication Scheme (IPS)

IS Act *See* *Intelligence Services Act 2001*

## J

Joint Committee of Public Accounts and Audit,  
20, 76

Joint Councils for Civil Liberties, 22

## K

key management personnel (KMP), 75,  
113–114

KMP *See* key management personnel (KMP)

## L

Law Council of Australia, 22

*Law Enforcement and National Security  
(Assumed Identities) Act 2010* (NSW), 58

## M

management and accountability

external scrutiny *See* external scrutiny

governance *See* corporate governance

human resources *See* human resources

purchasing and procurement *See*  
purchasing and procurement

market research *See* advertising and market  
research

memoranda of understanding, 32, 59, 65, 67

Minister for Defence, 23, 49, 50, 51, 54, 55, 56,  
57

Minister for Foreign Affairs, 9, 41, 44, 45, 46, 47

Minister for Home Affairs, 9, 31, 59

## N

National Centre for Intelligence Training and  
Education, 79

*National Disability Strategy 2010–2020*, 82

National Intelligence Community (NIC), 9, 25,  
26, 66

National Security and Intelligence Review  
Agency (Canada), 67

National Security College (ANU), 79

National Security Committee (Cabinet), 9

NIC *See* National Intelligence Community (NIC)

## O

*Office of National Intelligence Act 2018*, 9, 25, 26,  
57

Office of National Intelligence (ONI), 5, 9, 20

assumed identities, use of, 58

AUSTRAC information, access to, 60

COVID-19, impact of, 26

ensuring analytic integrity, 26

functions, 25

inspection of activities, 25–26

leading the national intelligence

- community, 26
- Open Source Centre, 26
- Open Source Collection Framework, 26
- open-source information, collection of, 26
- Privacy Rules, 26, 57
- Office of the Australian Information Commissioner *See* Australian Information Commissioner
- Office of the Commonwealth Ombudsman *See* Commonwealth Ombudsman
- Office of the Inspector-General of Intelligence and Security (NZ), 67
- Office of the Inspector General of the Intelligence Community (US), 67
- Office of the Intelligence Commissioner (Canada), 67
- ONI *See* Office of National Intelligence (ONI)
- ONI Act *See* *Office of National Intelligence Act 2018*
- organisational profile, 77–78
- organisational structure, 7, 70
- outcome and program structure, vi, 7, 109
- outreach
  - ACIC, AFP, AUSTRAC, with, 61
  - public outreach activities, 22
- overview of report, vi, 1–10
  - Inspector-General's review, 2–4
  - key activities *See* complaints (Objective 4); inquiries (Objective 4); inspections (Objective 4); public interest disclosures (PIDs) (Objective 4)
  - organisational structure, 7
  - outcome and program structure, vi, 7, 109
  - purpose of IGIS, 8, 18, 21
  - role of IGIS *See* role of IGIS
- P**
- Parliamentary Joint Committee on Intelligence and Security (PJCIS), 3, 13, 19–20, 24, 48, 65
- PBS *See* Portfolio Budget Statement (PBS)
- Performance Agreements, 75, 79
- performance results and analysis *See* annual performance statement
- PGPA Act *See* *Public Governance, Performance and Accountability Act 2013*
- PGPA Rule *See* Public Governance, Performance and Accountability Rule 2014
- PID Act *See* *Public Interest Disclosure Act 2013*
- PID scheme, 8, 16, 63, 64
- PIDs *See* public interest disclosures (PIDs) (Objective 4)
- PJCIS *See* Parliamentary Joint Committee on Intelligence and Security (PJCIS)
- Portfolio Budget Statement (PBS), 7, 12, 13, 14, 15, 16, 118
- preliminary inquiries, 6, 19, 62
  - Application of National Security Classifications, 24
- Prime Minister, 5, 6, 7, 9, 19, 25, 26, 92, 109
- Privacy Act 1988*, 60, 66
- procurement *See* purchasing and procurement
- Public Governance, Performance and Accountability Act 2013*, iii, vi, 12, 71, 75, 80, 81, 86, 92, 100, 108, 109
- Public Governance, Performance and Accountability (Financial Reporting) Rule 2015, iii, 90, 92
- Public Governance, Performance and Accountability Rule 2014, iii, vi, 80, 81, 113, 115
  - requirements for annual reports, 117–126
- Public Interest Disclosure Act 2013*, 5, 6, 8, 62, 63, 64
- public interest disclosures (PIDs) (Objective 4), 5, 6, 63–64
  - agency and conduct, by, 64
  - COVID-19, impact of, 64
  - PID scheme, 8, 16, 63, 64
  - statistics, 61, 62
- Public Service Act 1999*, 78, 121
- purchasing and procurement, 80–82, 122
  - ANAO access clauses, 81, 124
  - consultants, 80–81, 123–124
  - disability reporting mechanism, 82, 126
  - exempt contracts, 82, 124
  - information publication scheme, 82
  - purchasing, 80, 122
- purpose of IGIS, 8, 18, 21 *See also* Corporate Plan 2020–21

## R

- Reconciliation Action Plan (AGD), 68
- remuneration, 112
  - executive remuneration, 75, 125
- requirements for annual reports, 117–126
- review of reporting period, vi, 2–4
- risk management, 71, 74
  - Risk Management Policy and Framework, 74
  - Risk Register, 74
- role of IGIS, vi, 5, 20, 21, 22, 59
  - proposed expansion, 3, 61, 65–66, 79

## S

- Secretary for Defence, 10, 56
- Security Legislation Amendment (Critical Infrastructure) Bill 2020, 20
- Senate Continuing Order for Indexed File Lists, 82
- Senate Estimates hearing, 19
- Senate Finance and Public Administration Legislation Committee, 20
- Senate Standing Committee on Legal and Constitutional Affairs, 19
- senior management committees, 70
- Senior Officers Meeting, 70, 71, 115
- SIOs *See* special intelligence operations (SIOs)
- special intelligence operations (SIOs), 9, 29
- staff *See* human resources
- stakeholders *See* infrastructure and stakeholders (Objective 5)
- State of the Service reports* (APS), 82
- Statistical Bulletin* (APS), 82
- Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, 3, 20, 65, 66

## T

- Taxation Administration Act 1953*, 32
- Telecommunications Act 1997*, 38, 39, 40
- Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, 31
- Telecommunications (Interception and Access) Act 1979*, 23, 27, 28, 31, 39, 40, 45, 48
  - access to data under, 38
  - breaches of, 28, 34, 35
  - existing data authorisations, 38–40
  - incidents report (2019–20), finalisation of, 34
  - interception warrants, 33–36, 52–53
  - potential breaches, 34, 36
  - prospective data authorisations, 38
- TIA Act *See* *Telecommunications (Interception and Access) Act 1979*
- travel
  - COVID-19, impact of, 3, 41, 63, 67

## V

- Values (APS), 75
- visa and citizenship complaints, 16, 61, 63

## W

- warrants, 9, 23, 29, 30, 31, 37, 40, 45, 65, 66
  - inspection of, 27–28
  - interception warrants, 33–36, 52–53
- website, 6, 14, 16, 21, 22, 24, 82
- work health and safety, 115
- Work Health and Safety Act 2011*, 115



