



**IGIS**

INSPECTOR-GENERAL OF  
INTELLIGENCE AND SECURITY

# 2019–2020

## 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 AND PUBLIC INTEREST DISCLOSURES

Phone: (02) 6141 4555  
Email: [complaints@igis.gov.au](mailto:complaints@igis.gov.au)  
Email: [pid@igis.gov.au](mailto:pid@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 2020



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)

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



The Hon Christian Porter MP  
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 2019 to 30 June 2020.

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

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

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

As required by section 10 of the *Public Governance, Performance and Accountability Rule 2014*, I certify that my office has 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 appropriately deal with fraud relating to the agency.

Yours sincerely

Jake Blight  
Acting Inspector-General  
29 September 2020



# CONTENTS

IGIS contact information	inside cover
Letter of transmittal	i
Glossary of abbreviations and acronyms	v

## SECTION ONE

### **OVERVIEW** **1**

---

Inspector-General's review	2
Role of the Inspector-General of Intelligence and Security	4
About the Australian intelligence agencies	9

## SECTION TWO

### **ANNUAL PERFORMANCE STATEMENT** **11**

---

Entity purpose	12
Results	13
Analysis	19
<b>Objective 1:</b> Assisting Ministers	19
<b>Objective 2:</b> Assuring parliament	19
<b>Objective 3:</b> Informing the public	22
<b>Objective 4:</b> Inquiries	23
<b>Objective 4:</b> Inspections	26
<b>Objective 4:</b> Complaints and public interest disclosures	56
<b>Objective 5:</b> Infrastructure and stakeholders	64
<b>Objective 6:</b> High-performing workforce	67

## SECTION THREE

### **MANAGEMENT AND ACCOUNTABILITY 69**

---

Corporate governance	70
External scrutiny	75
Management of human resources	76
Asset management	78
Purchasing and procurement	78

## SECTION FOUR

### **FINANCIAL MANAGEMENT 81**

---

<b>Part 4.1:</b> Financial summary	82
<b>Part 4.2:</b> Financial statements	86

## SECTION FIVE

### **ANNEXURES 109**

---

<b>Annexure 5.1:</b> IGIS salary scale	110
<b>Annexure 5.2:</b> Key management personnel	111
<b>Annexure 5.3:</b> Other mandatory information	113
<b>Annexure 5.4:</b> Requirements for annual reports	115
Index	124

# ABOUT THIS REPORT

This is the annual report of the Inspector-General of Intelligence and Security for the period from 1 July 2019 to 30 June 2020.

This report has been prepared in accordance with legislative requirements. They 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 THIS REPORT

**Section One** contains the Inspector-General's review of the reporting period and outlook for 2020–21. This section also outlines the role and functions of the Inspector-General and the Office, its published outcomes and program structure as well as a brief description of each of the six intelligence agencies the Inspector-General oversees.

**Section Two** contains the Annual Performance Statement, detailing the Office's performance during the reporting period in the context of the indicators identified in the IGIS Corporate Plan 2019–20.

**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 OF ABBREVIATIONS AND ACRONYMS

AAT	Administrative Appeals Tribunal
ACIC	Australian Criminal Intelligence Commission
ACLEI	Australian Commission for Law Enforcement Integrity
ADF	Australian Defence Force
AFP	Australian Federal Police
AGO	Australian Geospatial-Intelligence Organisation
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
DIO	Defence Intelligence Organisation
FIORC	Five Eyes Intelligence Oversight and Review Council
FOI	Freedom of information
FOI Act	<i>Freedom of Information Act 1982</i>
IAG	Integrity Agencies Group
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>
IIOF	International Intelligence Oversight Forum
Inspector-General	The Inspector-General of Intelligence and Security
IS Act	<i>Intelligence Services Act 2001</i>
NIC	National Intelligence Community
OAIC	Office of the Australian Information Commissioner
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	<i>Public Governance, Performance and Accountability Rule 2014</i>
PID	Public Interest Disclosure
PID Act	<i>Public Interest Disclosure Act 2013</i>
PJCIS	Parliamentary Joint Committee on Intelligence and Security
Privacy Act	<i>Privacy Act 1988</i>
SES	Senior Executive Service
SIO	Special intelligence operations
TIA Act	<i>Telecommunications (Interception and Access) Act 1979</i>
WHS Act	<i>Work Health and Safety Act 2011</i>





# SECTION ONE

## OVERVIEW



# INSPECTOR-GENERAL'S REVIEW

Margaret Stone AO FAAL was the Inspector-General during the reporting period and prepared this review and the majority of the report prior to the end of her statutory term on 23 August 2020.

Over the past year, the most significant event to affect the operation of the Office of the Inspector-General of Intelligence and Security (IGIS) has been the COVID-19 pandemic. The security classifications of material relevant to IGIS's core inspection and inquiry activities mean that this work cannot be done remotely. As a result, during the peak of Canberra's COVID-19 restrictions some inspection, inquiry and complaint work was reduced or delayed, with the recognition that greater attention would be paid to these activities at a later stage. As restrictions eased in Canberra, compliance and inspection activities increased with a focus on completing the work which was delayed. Core corporate enabling functions continued with little or no interruption.

During this challenging period IGIS refined and developed new approaches to its activities and built staff capabilities through training and development. Four IGIS officers were seconded to agencies within the National Intelligence Community (NIC) and to other oversight agencies to fill critical vacancies. As the Office transitioned through several phases of working arrangements, officers were adaptable and flexible in response to the changing requirements.

In accordance with s 35 of the IGIS Act, this report provides details of inquiry and inspection activities during the year and on agency compliance with certain privacy rules, in addition to details of the performance and financial position of this Office. Despite the temporary pause in inspections due to COVID-19 restrictions, IGIS completed the majority of scheduled inspections by the end of the reporting period. Inspections continued to target areas assessed as at high risk of an undetected or unreported breach of the requirements of legality, propriety and human rights. During the reporting period an inquiry was also concluded. The inquiry required many in-depth interviews and the review and analysis of many thousands of classified documents. Reduced access to classified systems and material during the COVID-19 restrictions resulted in some delays in finalising the inquiry report.

There continue to be a number of legislative changes to the powers of agencies which will significantly expand IGIS oversight responsibilities. The Inspector-General has been consulted on the development of these changes and continues to contribute to the consultative processes around further proposed changes. This consultation helps ensure that features supporting effective oversight by IGIS are built into the legislation. Many of these changes have complex legal and technical aspects which have significant implications for how IGIS oversees agency activities. During 2019–20, IGIS contributed to all inquiries conducted by the Parliamentary Joint Committee on Intelligence and Security (PJICIS) that were relevant to the oversight of agencies within the Inspector-General's jurisdiction. Written submissions were provided and the Inspector-General appeared at hearings to answer questions from the Committee.

IGIS has engaged with other Australian integrity and oversight agencies throughout the year. Two IGIS officers participated in the Australian Commission for Law Enforcement Integrity (ACLEI) immersive development placement program ahead of the proposed changes to the Inspector-General's jurisdiction. Regular meetings occurred with the Office of the Commonwealth Ombudsman (OCO) at both the executive and officer level. IGIS is also cooperating with the Office of the Australian Information Commissioner (OAIC) on a project related to the COVIDSafe app to ensure the relevant agencies are acting legally and in accordance with the restrictions that have been applied to this data.

International engagement continued with Five Eyes partners throughout the year, although the annual 2020 Five Eyes Intelligence Oversight and Review Council (FIORC) conference was cancelled due to COVID-19 travel restrictions. The group has been able to conduct regular teleconferences to discuss key items and to progress joint projects.

Informing the public and providing assurances that intelligence and security matters are open to scrutiny is a key priority for IGIS. While there are some security constraints on what information can be released publicly, we seek to engage with public groups and include as much information as possible in this report and in other publications. IGIS has convened two further meetings with the Civil Society Reference Group and these meetings are now an important part of the IGIS public engagement strategy. IGIS has also updated and expanded the content on the IGIS website and more information is now available about the activities of IGIS, as well as specific inspection information for each of the agencies within the Inspector-General's jurisdiction. Complaints are important elements of IGIS's oversight of intelligence agencies and of its public assurance role. Recent improvements to the complaints process have made complaints by means of online forms on the website more accessible.

While IGIS welcomed a number of new officers over the past year, the planned expansion to 55 staff has not yet been reached. IGIS officers are required to hold the highest level of security clearance. Acquiring this level of clearance is a lengthy process that not infrequently results in a number of candidates withdrawing before it is finalised. One strategy to deal with the high withdrawal rate has been the use of the staff placement program which is discussed in Section 2 of this report. Recruitment activity remains a focus for the next year as well as developing retention strategies to provide flexibility for IGIS officers and to promote high levels of job engagement and satisfaction.

In light of the increasing size of the Office, a comprehensive review of internal governance has been conducted to design governance arrangements that will suit the expansion and ensure the Office delivers its responsibilities as a Commonwealth entity effectively. Based on the recommendations of the review, a governance and strategy team has been created for central management of governance functions such as corporate reporting, strategic planning, internal audit and risk management. Work has commenced on devolving authority to make decisions so as to increase the effective operation of the Office. Revised delegations and authorisations will link to clearly devolved accountability and responsibilities across the senior executive and executive level officers. Activities related to these and other recommendations will continue into the next reporting period and provide the platform to support the core investigation work of IGIS. In addition to these governance initiatives, two major ICT projects have been delivered this year – an electronic document management system and a new case management system that will be used to manage and track complaints related activities.

The coming year will also bring to a close my five year term as the Inspector-General, and the appointment of a new Inspector-General. It has been an honour to lead this Office and to participate in its important work.

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

The Inspector-General is an independent statutory office holder appointed by the Governor-General under the IGIS Act. The Hon Margaret Stone AO FAAL was appointed as Inspector-General for a five year term from 24 August 2015 to 23 August 2020.

IGIS is an agency within the Attorney-General's portfolio, with separate appropriation and staffing. As an independent statutory office holder, the Inspector-General is not subject to general direction from the Attorney-General, or other Ministers, on how responsibilities under the IGIS Act should be carried out.

Under the IGIS Act, the role of the Inspector-General is to assist Ministers in overseeing and reviewing the activities of the Australian intelligence agencies for legality and propriety and for consistency with human rights. This means:

*legality:* intelligence agencies operate within and comply with the legislation governing their activities, and with ministerial guidelines and directives.

*propriety:* the use of powers by intelligence agencies is reasonable and proportionate in the circumstances.

*human rights:* the activities of intelligence agencies are consistent with and respect human rights.

The Inspector-General discharges these responsibilities through a combination of inspections, preliminary inquiries, formal inquiries and investigations into complaints.

The Inspector-General also assists the Government in assuring the Parliament and the Australian public that intelligence and security agencies, including their operational activities, are open to scrutiny. Independence is fundamental to the role of IGIS and it is the policy of IGIS to make public as much information as possible about IGIS's activities as is consistent with secrecy requirements.

IGIS carries out regular inspections of the intelligence agencies that are designed to identify issues of concern at an early stage, including those in the agencies' governance, compliance and control frameworks. Early identification of such issues may avert the need for major remedial action.

The inspection role is complemented by an inquiry function. In undertaking inquiries the Inspector-General has strong investigative powers, similar to those of a royal commission. These include the power to compel persons to answer questions and produce documents and to take sworn evidence.

IGIS can also investigate complaints and public interest disclosures (PID) made by members of the public or intelligence agency staff, about the activities of intelligence agencies. Complaints or PIDs may also give rise to inquiries.

The role and functions of the Inspector-General are important elements of the overall accountability framework imposed on the intelligence agencies. The Inspector-General's oversight of operational activities of the intelligence agencies complements other oversight, including by the PJCS and the Australian National Audit Office (ANAO).

## OUR APPROACH TO OUR ROLE

### INDEPENDENT AND IMPARTIAL – we select what to look at and how to look at it

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

### ASTUTE AND INFORMED – we know what agencies are doing and why

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

### MEASURED – we focus on serious and systemic issues

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

## OPEN – we are open about our approach to oversight

We make as much as possible of our information public; however, a large part of the information that IGIS deals with is classified and cannot be released publicly. Nevertheless, in our annual report, unclassified inquiry reports, on our website and in our responses to complaints we include as much information as we can about our activities, including our oversight of intelligence agency activities. We aim to ensure that intelligence agencies provide Ministers with accurate reports of their intelligence activities; this includes reporting on their use of special powers, such as warrants, as well as reporting their non-compliance with legislative requirements.

## INFLUENTIAL – we assist agencies improve their compliance

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

## ORGANISATIONAL STRUCTURE

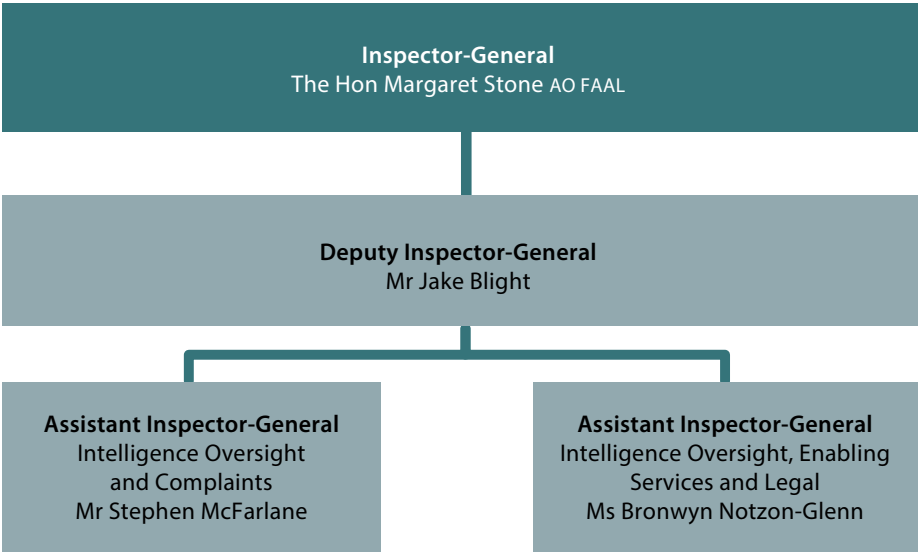
As at 30 June 2020, the Office had 33 Australian Public Service (APS) staff. The Inspector-General is supported by a Deputy Inspector-General and two Assistant Inspectors-General.

The Deputy Inspector-General is the chief operating officer and chief security officer for the agency. The Deputy Inspector-General also has significant input into IGIS investigations, governance and strategy matters, legal issues and is responsible for parliamentary matters.

The Assistant Inspector-General Intelligence Oversight and Complaints Branch manages the teams responsible for inspection programs of four agencies within the Inspector-General's current jurisdiction, as well as complaints handling.

The Assistant Inspector-General Intelligence Oversight, Enabling Services and Legal Branch manages the teams responsible for engagement with four agencies in the Inspector-General's proposed jurisdiction, two agencies within the Inspector-General's current jurisdiction, as well as corporate, legal and policy services for the Office.

Figure 1.1: IGIS organisational structure at 30 June 2020



## OUTCOME AND PROGRAM STRUCTURE

The Office has one outcome in the 2019–20 Portfolio Budget Statement (PBS).

Our 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.

## PURPOSES

The IGIS Corporate Plan 2019–20 describes the responsibilities of the Office as:

Under the IGIS Act the role of the Inspector-General is to assist Ministers in overseeing and reviewing the activities of the intelligence agencies for legality and propriety and for consistency with human rights. The Inspector-General discharges these responsibilities through a combination of inspections, inquiries and investigations into complaints.

The Inspector-General is also required to assist the Government in assuring the Parliament and the public that intelligence and security matters relating to Commonwealth agencies are open to scrutiny. Submissions to parliamentary committees and a program of public speaking are designed to address this aspect of the Inspector-General's role, as is our policy of providing as much information about our activities as is consistent with our secrecy requirements.

Section 4 of the IGIS Act sets out the objects of the Act as:

- a) to assist Ministers in the oversight and review of:
  - i. the compliance with the law by, and the propriety of particular activities of, Australian intelligence agencies; and
  - ii. the effectiveness and appropriateness of the procedures of those agencies relating to the legality or propriety of their activities; and
  - iii. certain other aspects of the activities and procedures of certain of those agencies; and
- b) to assist Ministers in ensuring that the activities of those agencies are consistent with human rights; and
- ba) to assist Ministers in investigating intelligence or security matters relating to Commonwealth agencies, including agencies other than intelligence agencies; and
- c) to allow for review of certain directions given to the Australian Security Intelligence Organisation (ASIO) by the responsible Minister for ASIO; and
- d) to assist the Government in assuring the Parliament and the public that intelligence and security matters relating to Commonwealth agencies are open to scrutiny, in particular the activities and procedures of intelligence agencies.

In addition, the *Public Interest Disclosure Act 2013* (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; and
- oversee the operation of the PID scheme in the intelligence agencies.

Under the *Archives Act 1983* (Archives Act) and the *Freedom of Information Act 1982* (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 (Information Commissioner).



# ABOUT THE AUSTRALIAN INTELLIGENCE AGENCIES

## OFFICE OF NATIONAL INTELLIGENCE (ONI)

ONI is responsible for enterprise-level management of the 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. ONI was established by the *Office of National Intelligence Act 2018* (ONI Act) and subsumed the former Office of National Assessments.

The responsible Minister for ONI is the Prime Minister.

## AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION (ASIO)

ASIO's main role is to gather information and produce intelligence that will enable it to warn the Government about activities that might endanger Australia's security.

ASIO's functions are set out in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). ASIO is also bound by Guidelines, which include requirements for the collection and handling of personal information. The Guidelines 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; 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 (ASIS)

The primary function of ASIS is to obtain and communicate intelligence not readily available by other means, about the capabilities, intentions and activities of individuals or organisations outside Australia. Further functions set out in the *Intelligence Services Act 2001* (IS Act) include communicating secret intelligence in accordance with government requirements, conducting counter-intelligence activities and liaising with foreign intelligence or security services.

Under the IS Act, ASIS's activities are regulated by a series of Ministerial Directions, Ministerial Authorisations and the Privacy Rules.

The responsible Minister for ASIS is the Minister for Foreign Affairs.

## AUSTRALIAN SIGNALS DIRECTORATE (ASD)

ASD defends Australia against global threats and advances the national interest through the provision of foreign signals intelligence, cyber security and offensive cyber operations, as directed by Government. Its functions are set out in the IS Act. The signals intelligence produced by ASD is provided to key policy makers and select government agencies with a clear and established need to know.

ASD encompasses the Australian Cyber Security Centre (ACSC) which leads the Australian Government's efforts on national cyber security. It brings together cyber security capabilities from across the Australian Government to improve the cyber resilience of the Australian community.

The responsible Minister for ASD is the Minister for Defence.

## AUSTRALIAN GEOSPATIAL-INTELLIGENCE ORGANISATION (AGO)

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 Australian Defence Force (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 the Privacy Rules.

The responsible Minister for AGO is the Minister for Defence.

## DEFENCE INTELLIGENCE ORGANISATION (DIO)

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

The responsible Minister for DIO is the Minister for Defence.

## **SECTION TWO**

### ANNUAL PERFORMANCE STATEMENT





I, Jake Blight, as the accountable authority of the Office of the Inspector-General of Intelligence and Security, present the annual performance statement of the Office of the Inspector-General of Intelligence and Security for the financial year 2019–20, 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.

Jake Blight  
Acting Inspector-General of Intelligence and Security

## ENTITY PURPOSE

The IGIS 2019–20 PBS provides a single Outcome and Program that encapsulates this purpose:

**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**

### **Program 1– Office of the Inspector-General of Intelligence and Security**

The objectives of this program are to meet the responsibilities and exercise the functions outlined in the IGIS Act and in other relevant legislation, and to conduct activities to facilitate the role of providing independent assurance as to whether Australia’s intelligence agencies are acting legally and with propriety.

---

All performance criteria in this performance statement relate to IGIS’s sole purpose.



# RESULTS

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

PERFORMANCE CRITERION AND CRITERION SOURCE  (from Corporate Plan unless indicated)	PERFORMANCE MEASURES  (from Corporate Plan unless indicated)	RESULT AGAINST PERFORMANCE CRITERION
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 of submissions made to parliamentary committees.	<b>Met</b>
	Number of appearances before parliamentary committees.	<b>Met</b>
	To the extent commensurate with our secrecy obligations, our annual report describes our 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 CRITERION AND CRITERION SOURCE (from Corporate Plan unless indicated)	PERFORMANCE MEASURES (from Corporate Plan unless indicated)	RESULT AGAINST PERFORMANCE CRITERION
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>Partially met</b> – an inquiry was finalised on 17 June 2020 and the reporting period ended on 30 June 2020. The unclassified summary was uploaded to the IGIS website in August 2020.
	IGIS has a written strategic engagement plan which includes targets for activities.	<b>Partially met</b> - IGIS has a written strategic engagement plan, however, targets for activities are still under development.
	At least 15 outreach activities completed each year to groups outside Australia's intelligence community. (PBS only)	<b>Partially met</b> – COVID-19 restrictions impacted on IGIS's ability to meet this measure.
4.1 IGIS has effective working relationships with the agencies we 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 six 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 CRITERION AND CRITERION SOURCE (from Corporate Plan unless indicated)	PERFORMANCE MEASURES (from Corporate Plan unless indicated)	RESULT AGAINST PERFORMANCE CRITERION
<p>4.2 IGIS has a well-developed and implemented inspection program.</p> <p>Inspector-General's comments on any inspection conducted under s 9A of the IGIS Act (s 35(2A) IGIS Act).</p> <p>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).</p>	Where relevant, inspections prompt changes in agency processes and agencies report on improvements.	<b>Met</b>
	An approved inspection plan is in place for agencies within the Inspector-General's jurisdiction. (Same measure appears in the PBS)	<b>Met</b>
	An interim inspection plan is in place for the four agencies expected to be added to the Inspector-General's jurisdiction by the time relevant amendments to the IGIS Act commence. (Same measure appears in the PBS)	<b>Not Applicable –</b> The IGIS Act was not amended to bring the four agencies under the Inspector-General's jurisdiction in 2019–20.
4.3 IGIS has a well-developed and implemented inquiry capability.	Program of own-motion inquiries including regular analytic integrity 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>
	A review of internal inquiry guidelines has been completed.	<b>Met</b>

PERFORMANCE CRITERION AND CRITERION SOURCE (from Corporate Plan unless indicated)	PERFORMANCE MEASURES (from Corporate Plan unless indicated)	RESULT AGAINST PERFORMANCE CRITERION
4.4 IGIS has efficient complaint and PID management processes.	90% of complaints acknowledged, triaged and allocated within five working days. (Same measure appears in the PBS)	<b>Met</b>
	85% of visa related complaints resolved within ten working days.	<b>Met</b> – Target met until 30 March 2020 when the process was amended. See Analysis section of the Annual Performance Statement for further information.
	Conduct at least one outreach activity which includes information about the PID scheme in each intelligence agency within the Inspector-General's jurisdiction each year.	<b>Partially met</b> – COVID-19 restrictions impacted on IGIS's ability to meet this measure.
5.1 Appropriate infrastructure and governance.	IGIS premises meet all applicable security accreditation standards.	<b>Met</b>
	IGIS ICT systems meet all applicable security accreditation standards.	<b>Met</b>
	Complete a review of internal governance arrangements.	<b>Met</b>





PERFORMANCE CRITERION AND CRITERION SOURCE (from Corporate Plan unless indicated)	PERFORMANCE MEASURES (from Corporate Plan unless indicated)	RESULT AGAINST PERFORMANCE CRITERION
5.2 Effective and efficient support 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>
	Implement electronic document management and complaint management systems.	<b>Partially met</b> – Implemented on the Protected system. Delivery of the new classified LAN has been delayed, including by COVID-19. The systems will be installed once delivered.
5.3 IGIS has positive relationships with other integrity agencies.	Meet at least twice per year with other integrity agencies to ensure complaint transfer and other 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.	IGIS has a performance management framework that integrates performance expectations and professional development.	<b>Met</b>
	IGIS has sufficient officers with the skills necessary to support IGIS oversight activities including inspections, inquiries and complaint management, as well as IGIS engagement with the legislative process.	<b>Met</b>



PERFORMANCE CRITERION AND CRITERION SOURCE (from Corporate Plan unless indicated)	PERFORMANCE MEASURES (from Corporate Plan unless indicated)	RESULT AGAINST PERFORMANCE CRITERION
6.2 Recruitment and training.	IGIS runs at least 10 modules of internal training per year.	<b>Met</b>
	IGIS is meeting the recruitment targets set in the IGIS strategic Human Resource (HR) plan.	<b>Partially met</b> – IGIS conducted multiple recruitment rounds in 2019–20. As at 30 June 2020, IGIS had 33 officers out of a target of 55 (not including the Inspector-General). Several additional candidates are undergoing relevant pre-employment organisational suitability and security checks.
6.3 Office culture and ethos.	IGIS officers comply with APS and security obligations.	<b>Met</b>
	IGIS officers utilise flexible working arrangements.	<b>Met</b>
	IGIS conducts a staff survey at least once every two years, the survey has at least a 90% response rate, and feedback in the survey is addressed.	<b>Met</b>



# 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 Inspector-General met these requirements for the inquiry that was conducted during 2019–20. 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 2019–20. Under s 25A of the IGIS Act, the Inspector-General may report to the responsible Minister on a completed inspection of an intelligence agency. During 2019–20, no such reports were made.

During 2019–20, 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 Inspector-General appeared before the Senate Standing Committee on Legal and Constitutional Affairs on 22 October 2019 for Supplementary Budget Estimates, and responded in writing to one question taken on notice. The Inspector-General was prepared to attend an Additional Estimates hearing on 3 March 2020, but was not called by the Committee to appear. Following both Estimates hearings, the Inspector-General responded to written questions from members of the Committee that were directed to all agencies within the Attorney-General's portfolio.

The Budget Estimates hearings originally scheduled for May 2020 were postponed due to COVID-19 restrictions and rescheduled to take place outside the reporting period.

### PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

The Inspector-General participated in six inquiries conducted by the PJICIS during the reporting period. This included four inquiries that examined existing or proposed legislation concerning Australian intelligence agencies.

- On 2 August 2019, the Inspector-General provided a written submission to the PJICIS for its inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press. The Inspector-General appeared before the Committee at a public hearing on 14 August 2019, and subsequently responded to a question taken on notice. At the end of the reporting period, the Committee was yet to table its report.



- On 2 August 2019, the Inspector-General provided a written submission to the PJCIS for its statutory review of the mandatory data retention regime prescribed by Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). The Inspector-General appeared before the Committee at a public hearing on 7 February 2020. At the end of the reporting period, the Committee was yet to table its report.
- On 25 October 2019, the Inspector-General provided a written submission to the PJCIS for its statutory review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*. The Inspector-General appeared before the Committee at a public hearing on 7 August 2020.
- On 4 May 2020, the Inspector-General provided a written submission to the PJCIS for its review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020. The Inspector-General appeared before the Committee at a public hearing on 12 May 2020, and provided a brief supplementary submission. At the end of the reporting period, the Committee was yet to table its report.

Consistent with established practices, the Inspector-General's submissions did not comment on the policy underlying the provisions, but made a number of observations in the context of IGIS's role of overseeing and reviewing the activities of the intelligence agencies for legality and propriety and for consistency with human rights.

#### REVIEWS OF THE *TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) ACT 2018*

Paragraph 29(1)(bca) of the IS Act requires the PJCIS to review, by 30 September 2020, the operation of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*. The Inspector-General's submission to the Committee's review mainly focused on Schedule 5 of the Act. This Schedule inserted provisions for voluntary assistance requests and compulsory assistance orders into the ASIO Act.

The PJCIS's statutory review follows its review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, which was completed on 5 December 2018 following a referral by the Minister for Home Affairs; and its review of the consequent Act, which was completed on 3 April 2019 following referral by the Senate. The Inspector-General's contributions to both of those reviews were discussed in the previous annual report.

Additionally, on 26 March 2019, the PJCIS referred the Assistance and Access Act to the Independent National Security Legislation Monitor (INSLM), Dr James Renwick SC, for review and report back to the Committee in order to inform its own statutory review. To assist the INSLM's review, on 29 October 2019, the Inspector-General provided a copy of her recent submission to the PJCIS's statutory review, as well as her submissions to previous PJCIS reviews. The INSLM's report was tabled in the Parliament out of session on 9 July 2020.

The Inspector-General appeared before the PJCIS for a public hearing on 7 August 2020. At the time of writing, the PJCIS's statutory review remains underway.

The Inspector-General also participated in two inquiries conducted by the PJCIS in accordance with its statutory function to review the administration and expenditure of ASIO, ASIS, AGO, DIO, ASD and ONI, 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 13 September 2019, the Inspector-General appeared before the PJCIS at a classified hearing for the Committee's review of the administration and expenditure for the 2017–18 financial year. The Inspector-General subsequently responded to one question on notice taken at the hearing. The Inspector-General's written submission for this review had been provided to the Committee during the previous reporting period (on 10 December 2018). The Committee presented its report to the Parliament on 5 February 2020. The report cited the Inspector-General's evidence on more than 20 occasions.
- On 17 February 2020, the Inspector-General provided an unclassified written submission to the PJCIS for its review of administration and expenditure for the 2018–19 financial year. The Inspector-General appeared at a classified hearing for that review on 26 February 2020, and subsequently responded to two questions on notice. In a statement published on the Committee's website and distributed to the Office on 25 June 2020, the Committee advised that COVID-19 restrictions had impacted the timeframe for its review activities and hearings with agencies. The Committee indicated that, as part of its next review of administration and expenditure for 2019–20, it will explore in detail the matters raised in evidence to the 2018–19 review.

## COMPREHENSIVE REVIEW OF THE LEGAL FRAMEWORK GOVERNING THE NATIONAL INTELLIGENCE COMMITTEE

The Inspector-General made a significant contribution to the Comprehensive Review of the Legal Framework Governing the NIC, conducted by Mr Dennis Richardson AC. In total, IGIS made seven submissions to the review, and responded to numerous requests for information. During the reporting period, this included three classified submissions in response to a Discussion Paper. The Inspector-General also met with Mr Richardson throughout the reporting period.

## 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 expert evidence concerning national security, defence, international relations and confidential foreign government communications exemptions to the AAT and the Information Commissioner.

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, they are not appropriately qualified to do so.

During the reporting period, there were two occasions where the Inspector-General received and responded to requests for evidence from the Information Commissioner in relation to Freedom of Information (FOI) exemptions. There were no requests for evidence from the AAT in relation to the review of matters relating to FOI or archives issues during the reporting period.

## OBJECTIVE 3 – INFORMING THE PUBLIC

The IGIS Act provides that it is a purpose of IGIS 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.

During 2019–20, IGIS developed a draft strategic engagement plan. The plan was developed to provide a framework for public assurance and engagement activities. The plan recognises the need to diversify engagement strategies in order to ensure an appropriate balance is achieved between general information on IGIS oversight functions, specialised and general public presentations, reference group meetings and consultative forums.

### IGIS WEBSITE

In 2019–20, as part of the draft strategic engagement plan, a project was commenced to redesign and expand the content available on the IGIS website. Ensuring that information on the role, functions and activities of IGIS is easily accessible online is a key element of providing public assurance that Australian intelligence agencies are open to scrutiny.

### PUBLIC OUTREACH ACTIVITIES

IGIS also conducts a regular program of presentations to the broader community. This includes 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 in relation to national security oversight and law reform. It also includes groups who may have broader interests across human rights, democratic principles, privacy, rule of law and current affairs. The program is designed to create greater public awareness and understanding of the role and activities of IGIS.

During 2019–20, IGIS delivered 12 major presentations at seminar and conference events, and spoke at a number of other forums to groups outside the intelligence community. This was slightly less than previous years, which reflects the cancellation of some events due to COVID-19 restrictions, and also the diversification of IGIS's public engagement strategies. The Inspector-General delivered the 2019 Sir Zelman Cowan Oration and also made various presentations to academic and legal audiences around Australia including to the New South Wales Chapter of the Australian Association of Constitutional Law seminar and at the 2019 Australian Government Solicitor National Security Law Forum. These engagements were supplemented by lectures and presentations delivered by IGIS SES officers to a range of government and non-government attendees.

## CIVIL SOCIETY REFERENCE GROUP

In June 2019, the Inspector-General convened a pilot meeting with three civil society groups with a view to establishing a regular consultative forum. The initiative was prompted in part by advice from intelligence oversight bodies from New Zealand, the United Kingdom and the United States of America on the value they derived from such meetings. There have been two further consultative meetings in 2019–20 and it is intended that Civil Society Reference Group meetings will be convened regularly. The key objectives of the meetings are 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 the discussion of legal and technical issues with groups who possess expertise in such fields.

Meetings were convened in November 2019 and May 2020. The May 2020 meeting was initially postponed and then held via VTC due to COVID-19 restrictions. On both occasions the meetings were attended by the Joint Councils for Civil Liberties, the Human Rights Law Centre, the Law Council of Australia and the Australian Privacy Foundation. A summary of discussions is published on the IGIS website.

The next meeting of the Civil Society Reference Group is scheduled for late 2020.

## 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 two inquiries from the 2018–19 reporting period and one inquiry from the current reporting period.

**Figure 2.1: Performance indicators – conducting inquiries**

SUBJECT OF INQUIRY	ASD MATTER 2018	ASIO MATTER 2018	AGENCY MATTER
Agency	ASD/ASIO	ASIO	Intelligence Agency
Source	Minister for Defence request	IGIS own motion	IGIS own motion in response to a complaint
Date initiated	30 May 2018	14 February 2018	2 August 2019
Date finalised	2 May 2019	14 June 2019	17 June 2020
Duration (days)	337 days	485 days	321 days
Number of recommendations	5	8	1
Percentage of recommendations accepted	100%	100%	100%

## INQUIRY INTO AN ASD MATTER 2018

As reported in the 2018–19 annual report, in May 2019 the Inspector-General completed an inquiry into an ASD matter pursuant to s 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 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 five recommendations aimed at reducing the risk of recurrence and improving the reporting of any future breaches of the TIA Act.

In October 2019, ASD and ASIO reported to IGIS their progress in implementing the recommendations. Whilst the implementation of one of the recommendations is ongoing, IGIS is satisfied that ASD and ASIO had so far implemented appropriate remedial action. This includes the establishment of ASD-ASIO joint warrant training and updated procedures for managing warrants and reporting incidents. Through regular inspections and engagement, IGIS will continue to monitor the actions of ASD and ASIO to implement the remaining recommendation.



## INQUIRY INTO AN ASIO 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 eight 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 eight recommendations.

On 30 September 2019, ASIO reported to IGIS 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. Key aspects of the recommendations have been implemented. IGIS considers five of the recommendations to be fully implemented and that in light of circumstances relating to COVID-19 satisfactory progress has been made in relation to the remaining three recommendations. IGIS notes that some recommendations relate to policies and procedures that will vary from time to time. The expansion and development of the compliance unit is ongoing. IGIS has included four additional inspections in the ASIO inspection program to review implementation of the inquiry recommendations. A further update will be provided in the 2020–21 annual report.

## INQUIRY INTO AN INTELLIGENCE AGENCY MATTER

During the reporting period, the Inspector-General commenced and completed an inquiry into the adequacy of mental health support provided by an intelligence agency to one of its former employees. The inquiry resulted from a PID made to IGIS in May 2019 by the former employee. It alleged there were deficiencies in the mental health support provided by the Agency while the employee was undergoing a security clearance review for cause. It is a condition of employment with the Agency that employees hold, and maintain, a security clearance.

On 2 August 2019, following a preliminary inquiry into the complainant's allegation, the Inspector-General initiated a formal inquiry under s 8 of the IGIS Act. The inquiry examined the mental health services provided by the Agency, the facts and circumstances relevant to the complainant's mental health requests and the adequacy of the Agency's response to those requests.

IGIS conducted multiple in-depth witness interviews and reviewed many thousands of the Agency's classified records relevant to the inquiry. The scope and detail of relevant material was substantial and the review process was time-consuming. Disruptions arising from the COVID-19 pandemic also delayed the process of the inquiry.



To assist the inquiry, legal advice from the office of the Australian Government Solicitor on a Commonwealth agency's duty of care obligations was provided. The *Work Health and Safety Act 2011* (Cth) (WHS Act) requires that a Commonwealth agency must exercise due diligence to ensure the health and safety of its employees in so far as is reasonably practicable. As a matter of law and propriety the employer, exercising due diligence, must be aware of the risk or it must be reasonably foreseeable.

The inquiry was completed on 17 June 2020. In regards to the matters under investigation, the inquiry found evidence contrary to the allegations made and in all the circumstances, no evidence to support the allegations made against the Agency. The Agency did not refuse any requests for support and, furthermore, there was a reasonable level of access by the complainant to psychological support. The inquiry concluded that, in the circumstances, the Agency took all reasonably practicable steps to ensure the health and safety of its employee. The inquiry highlighted the importance of intelligence agencies having a robust system of mental health and welfare support services in place, and ensuring that these are readily available to employees and subject to regular review and improvement.

The classified inquiry report made one recommendation which the Agency has accepted and undertaken to implement as soon as practicable. IGIS continues to engage with the Agency and seeks regular updates. IGIS will continue to monitor the adequacy of mental health and welfare support provided by this Agency and intelligence agencies in general.

## OBJECTIVE 4 - INSPECTIONS

IGIS regularly inspects intelligence agency activities to determine if each agency is acting in accordance with its statutory functions, is complying with any guidance provided by the responsible Minister and with its own 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 citizens detrimentally. Accordingly, the IGIS inspection program mainly focuses 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 Privacy Guidelines, and that their independence is not compromised. IGIS takes into account an agency's internal control mechanisms as well as its history of compliance and reporting.

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



## INSPECTION OF ONI ACTIVITIES

ONI is responsible for enterprise-level management of the NIC and undertakes the production of all source intelligence assessments for the Australian Government. ONI's statutory functions set out in the ONI Act include:

- leading and evaluating matters relating to the NIC
- assembling and preparing assessments and reports in accordance with the Government's requirements and matters of significance to Australia
- providing advice to the Prime Minister on NIC matters
- collecting and disseminating information that is accessible to any section of the public
- cooperation with, and assistance to, intelligence agencies and prescribed authorities.

IGIS regularly engages with ONI's Governance and Accountability Section which manages many compliance related matters in ONI, including their own review of ONI officer compliance with the *Office of National Intelligence Rules to Protect the Privacy of Australians* (Privacy Rules). This engagement addresses matters such as inspection arrangements, ensuring comprehensive building and IT access, consultation on relevant policies, reporting non-compliance and exchange of information between the Inspector-General and the ONI Director-General. ONI also briefed IGIS officers on the activities of its Open Source Centre and its progress in establishing a framework for the use of assumed identities.

During 2019–20, IGIS inspected the analytic independence and integrity of ONI assessments and ONI's compliance with its Privacy Rules. An additional inspection was scheduled in relation to ONI's open source collection function under s 7(1)(g) of the ONI Act. However, due to the COVID-19 restrictions, that inspection did not commence and has been rescheduled for the 2020–21 reporting period. Inspections of ONI are less frequent than for a collection agency given its comparatively lower risk profile as an assessment agency.

### COMPLIANCE WITH THE PRIVACY RULES

During 2019–20, IGIS conducted one inspection of ONI's compliance with its Privacy Rules. A further scheduled inspection could not be completed due to the COVID-19 restrictions.

Inspection activities identified seven ONI products where the relevant Privacy Rules were not applied. IGIS officers had been monitoring ONI reporting for references to Australian persons and this monitoring was used to identify instances of non-compliance. The inspection also identified areas where ONI could improve its compliance through ONI providing more detailed guidance in its internal policies.

ONI must advise IGIS if it identifies non-compliance with the Privacy Rules and must include information about the measures taken to protect the privacy of the affected Australian person, or of Australian persons more generally. In 2019–20, ONI reported one instance of non-compliance where the Director-General's approval was not obtained prior to ONI granting three Australian Government agencies access to reporting on Australian persons, as per the Privacy Rules.



IGIS requested further information from ONI in relation to the scale and type of reporting accessed and the remediation measures. Based on ONI's response to this request, the Inspector-General assessed that the seriousness of the non-compliance, in terms of intrusion into the privacy of Australians, was low given the type of material accessed. The prompt remediation measures undertaken by ONI were considered sufficient to manage the instance of non-compliance and to prevent similar occurrences in the future.

## ANALYTIC INTEGRITY INSPECTION

During 2019–20, IGIS conducted its first ONI analytic integrity inspection. Previously, the Inspector-General completed inquiries into the analytic independence and integrity of the Office of National Assessments (now ONI), DIO and ASIO assessments.

The Inspector-General determined that targeted inspections on specific aspects of analytic integrity were a more efficient use of finite resources and this approach was more attuned to the risk level of the agency's activities. It was determined that these inspections would be used to develop a baseline inspection process and standard for the analytic integrity of assessments across the agencies.

The inspection for ONI included a review of 40 per cent of intelligence products published by ONI from July to December 2019. IGIS officers inspected the tasking and scope of products, as well as consultation and approval requirements; the inspection focused on ONI processes being transparent and free from bias, and assessments being tested appropriately. The majority of records reviewed were of a high standard, however, there were some inconsistencies in recording key aspects related to external consultation. The inspection identified that more detailed guidance on external consultation would assist in improving the rigour and consistency of such records.

## 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
- advice about security of Ministers and Commonwealth authorities in relation to their functions and responsibilities
- furnishing security assessments to States and States authorities
- advice to Ministers and Commonwealth authorities about protective security
- collection of foreign intelligence
- cooperation with and assistance to other agencies.

During this reporting period, IGIS prioritised reviewing ASIO's intelligence collection activities, its security assessments, communication of intelligence, and advice to Ministers on security matters. There were no inspections of ASIO's advice relating to protective security.

In addition to conducting inspections, IGIS interacts frequently with members of the ASIO compliance directorate to keep abreast of developing or ongoing matters. ASIO has issued new internal guidance on proactive non-compliance reporting to IGIS and has updated its reporting templates. The directorate investigate incidents that may relate to breaches

of legislation or the Attorney-General's Guidelines, or non-compliance with ASIO internal policies and procedures. The investigation may establish that the matter in question did in fact comply with relevant requirements. When the compliance directorate investigates a matter, IGIS receives a report of its findings. IGIS independently reviews these investigation reports, and where necessary conducts its own review. In addition, the Inspector-General receives regular briefings and is provided with a copy of ASIO's periodic compliance reports.

## REGULAR INSPECTIONS OF INVESTIGATIVE CASES

Given the scale and scope of ASIO functions, IGIS implements a risk-based approach to inspection and compliance monitoring; this involves regularly sampling a number of identified activities. IGIS officers have direct access to the relevant ASIO information technology and records management systems to inspect and review all records.

Throughout 2019–20, IGIS conducted inspections using a variety of methodologies, including thematic reviews, risk-based sampling and random sampling. While COVID-19 restrictions had a minor impact on activities, most planned inspections continued unaffected. Inspections of ASIO's investigative cases 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 inspections identified instances that did not breach legislation but which were non-compliant with internal agency policy and procedure. ASIO separately identified and proactively notified IGIS of other instances of non-compliance with internal policy and procedure. IGIS found that ASIO has continued its focus on improving record keeping practices across the organisation.

During the last reporting period, ASIO increased the number of briefings provided to IGIS and this has continued over 2019–20. The briefings covered topics such as new capabilities, new initiatives and areas of risk. 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 bi-monthly meetings between the Inspector-General and senior ASIO officers; these meetings cover a variety of matters.

## ANALYTIC TRADECRAFT

ASIO produces a range of analytic products including security assessments, applications for warrants, investigative reviews and published analytic 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 Government take an action which would be prejudicial to the interests of the person such as cancelling their passport.

During the reporting period, ASIO has continued its efforts to support analysts in their professional development, including through development and delivery of a training package specifically targeted at officers with responsibility for overseeing and managing analytic functions. At ASIO's invitation, IGIS officers presented at the course and reinforced expectations regarding compliance with all relevant policies and procedures.

### FAILURE TO RECORD KEY INTELLIGENCE

In November 2019, ASIO advised IGIS it had become aware that key intelligence used as the justification for a security investigation of an individual had not been correctly recorded in ASIO's corporate records; for various reasons, at the time the issue was identified the relevant material was unable to be reobtained and recorded correctly. This placed ASIO in a position where, had it been asked to produce evidence justifying the investigation of that individual, it would not have been able to do so. ASIO advised IGIS that it had immediately suspended the investigation pending an initial compliance review, and then terminated the investigation. ASIO advised that it would delete the results of telecommunications and financial inquiries conducted by ASIO from ASIO corporate systems. ASIO's intelligence holdings were updated to remove intelligence reporting on the subject that had been based on the relevant material and ASIO circulated updated advice to remind officers of the relevant analytical integrity principles and procedures.

IGIS concluded that the incident was attributable to human error, rather than systemic weakness in analytical procedure, and that action was taken to ensure ASIO officers were aware of the relevant procedures. IGIS considers that ASIO's identification of this issue and its remedial actions were adequate, appropriate, and timely.

### HUMAN SOURCE MANAGEMENT

ASIO activities include collection of intelligence through human sources. The details of these activities are highly sensitive and cannot be disclosed in a public report. During the reporting period, IGIS reviewed ASIO human source case files and met with ASIO officers to discuss related activities.

### ASIO WARRANTS

ASIO may intercept telecommunications when authorised under warrants issued by the Attorney-General pursuant to the TIA Act. Warrants for the exercise of other intrusive powers, including searches, computer access and surveillance devices, can be issued by the Attorney-General pursuant to the provisions of the ASIO Act.

Throughout the reporting period, IGIS inspected an indicative sample of warrants through its regular inspection program. Minor compliance and record keeping errors were identified in these inspections and ASIO was advised of these issues. IGIS will continue to monitor ASIO's compliance and record keeping as part of the regular inspection program.

IGIS continues to review ASIO's response to a systemic issue relating to the authorisations of classes of persons under s 24 of the ASIO Act. The issue concerns the use of descriptions to define a class of persons for the purposes of s 24 of the ASIO Act. IGIS considered that these descriptions may be overly broad, uncertain, or not sufficiently connected to the exercise of power under the warrant. During the year, ASIO obtained legal advice and reviewed its internal guidance on these matters. IGIS has conducted a further inspection of authorisations made under s 24 and will continue to monitor this issue.

The 2018–19 annual report noted that IGIS had identified ASIO's inappropriate use of templated text to brief the Attorney-General for the purposes of s 27C(2)(b) of the ASIO Act. In response to this issue, ASIO has amended warrant application templates so that officers are prompted to provide a tailored brief on the matters identified in this subsection. IGIS is satisfied that ASIO has appropriately addressed the issue and inspections conducted during 2019–20 did not identify any similar examples of the use of generic templated text.

ASIO proactively informed IGIS of certain breaches and other issues relating to warrants issued under the TIA Act and the ASIO Act. This 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. A small number of reported breaches were attributable to mistakes made by telecommunications carriers rather than ASIO; nevertheless they required ASIO to take remedial action such as deleting information incorrectly sent by the carrier.

A detailed summary of compliance incidents reviewed by IGIS is provided below. Some of these matters remained under review by ASIO at the end of the reporting period, therefore IGIS has not finalised its consideration of the matters.

## INCIDENTS RELATING TO INTERCEPTION WARRANTS UNDER THE TIA ACT

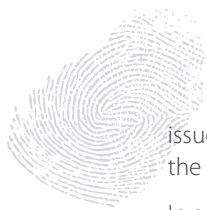
### TWO BREACHES OF SECTION 63(1) OF THE TIA ACT

Section 63(1) prevents a person from communicating, making use of, making a record of, or giving in evidence in a proceeding, lawfully intercepted information or information obtained by intercepting a communication unlawfully. In late June 2019, ASIO notified IGIS that it may have disclosed information in contravention of s 63(1) of the TIA Act. ASIO later confirmed that it had disclosed foreign intelligence information to two partner services in November 2018 without having written approval from the Attorney-General as required by s 65(2) of the TIA Act. In response to this breach, ASIO updated its foreign intelligence collection warrant application templates to prompt ASIO officers to request appropriate approvals for future warrants. IGIS has reviewed the matters and is satisfied with ASIO's assessment and subsequent remediation action.

### INTERCEPTION UNDER SECTION 11B WARRANTS

ASIO notified IGIS of an administrative error relating to interception authorised under a s 11B warrant. Section 11B provides for named person warrants to be issued for the collection of foreign intelligence. ASIO had initially intended to intercept a telecommunications service used by the subject of the warrant but decided on propriety grounds that the telecommunications service should not be intercepted. The telecommunications service was removed from the warrant but administrative errors resulted in the service being intercepted for several months. ASIO advised that on identifying the error, it ceased interception of the service, deleted all data intercepted from the service and conducted an audit to ensure no additional services were the subject of unauthorised collection. In addition, internal guidance was issued to ASIO officers reiterating the administrative procedures for s 11B warrants. While IGIS is satisfied with ASIO's response to this specific incident, IGIS has worked with ASIO to identify additional opportunities to improve its interception procedures.

Separately, ASIO notified IGIS of a potential breach relating to a s 11B warrant where services added to the warrant related to an Australian permanent resident. Having identified this



issue, ASIO immediately ceased interception of these services. ASIO is currently reviewing the matter and IGIS will assess and consider ASIO's response following its review.

In addition, ASIO notified IGIS about a propriety issue concerning a named person warrant where some data that was lawfully collected under the warrant but was intended to be deleted from ASIO holdings was not deleted. Further investigation by ASIO determined that the segregation and deletion of this data was not viable once collected. IGIS continues to liaise with ASIO on this matter.

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

In July 2019, ASIO advised IGIS that it had identified an issue regarding the application of s 11B(2) of the TIA Act. Section 11B(2) requires ASIO to advise the Attorney-General of the details of telecommunications services used by the subject of the warrant application, to the extent these are known to ASIO. The matter is currently being reviewed by ASIO and IGIS will consider ASIO's response following its review.

### BREACHES OF SECTION 16(2) OF THE TIA ACT

Section 16(2) requires ASIO, where interception of communications to or from a service are no longer required, to immediately inform an authorised representative of a telecommunications carrier, with confirmation to be given in writing as soon as practicable. In August 2019, ASIO notified IGIS of a breach of s 16(2)(d) of the TIA Act. During 2019, ASIO determined that a telecommunications service it had targeted under s 9A warrant was no longer being used by the named person. ASIO immediately ceased interception of the service but did not notify the telecommunications carrier in writing, as required by s 16(2)(d) of the TIA Act, for approximately three months. Having identified the error, ASIO provided the notification. No unauthorised collection had occurred. In response to this incident, ASIO reinforced the requirements of s 16 of the TIA Act with relevant officers. IGIS has reviewed the matter and is satisfied with ASIO's notification and response.

In the previous reporting period, ASIO had notified IGIS of a possible breach of s 16(2) of the TIA Act but had not concluded its investigation as at 30 June 2019. ASIO subsequently concluded that a breach had not occurred and provided that advice to the Inspector-General in October 2019. IGIS is satisfied with ASIO's investigation and advice.

### ERROR IN SECTION 11C WARRANT

In November 2019, ASIO advised IGIS of an error that had been identified in a warrant issued under s 11C of the TIA Act. Section 11C provides for warrants to be issued for the interception of foreign communications for the purpose of obtaining foreign intelligence. Following legal review, ASIO determined to seek a new warrant. The Inspector-General was informed of the matter and concurred with the proposed action. The Attorney-General authorised a new warrant and the original warrant was revoked.

### BREACHES IN SECTION 7(1), 13 AND 17(1) OF THE TIA ACT

Section 7(1) prohibits interception of communication passing over a telecommunications system. However, section 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 are discontinued where the grounds on which the warrant was issued cease to exist prior to the expiration of the warrant, and to advise the Attorney-General accordingly. Section 17(1) requires ASIO to provide a report to the Attorney-General within 3 months after the expiration or revocation of a warrant.





Between January and March 2020, ASIO notified IGIS of breaches concerning several related warrants issued under s 9 of the TIA Act. In the first notification, ASIO reported two instances where issues with confirming the subscriber of a telecommunications service had resulted in the unintended interception of telecommunication services likely used by Australian persons.

The first incident of erroneous interception of the service was caused by the telecommunications carrier providing incorrect subscriber details to ASIO. ASIO advised that when it detected the error, it ceased interception, deleted all relevant data and reported the issue to the Attorney-General.

The second incident resulted from the subject unsubscribing from a telecommunications service and the service being subscribed to another person. In the brief period after ASIO had confirmed the subscriber details of the telecommunications service but before ASIO applied for the warrant, the service in question was unsubscribed by the subject of ASIO's collection efforts. Despite becoming aware during the term of the warrant, ASIO did not revoke the warrant as it made the assumption that the service would not be resubscribed before the expiry of the warrant. However, the service was resubscribed to another subscriber shortly before the warrant expired. This resulted in the communications of the new subscriber being intercepted over a six day period. After detecting the error, ASIO deleted this data. In addition, ASIO advised IGIS that due to an administrative oversight, it did not report the incident to the Attorney-General in its initial report under s 17 of the TIA Act. A separate report of the incident was subsequently provided to the Attorney-General.

In response to these breaches, ASIO conducted a review of the interception operation. ASIO identified and notified IGIS of four additional incidents making a total of six warrants issued under s 11A of the TIA Act with identified breaches. These cases are discussed below and are currently being reviewed by ASIO. IGIS will consider ASIO's response following its review.

The third incident involved similar circumstances where a service was disconnected in the period between a subscriber check being undertaken and the warrant being authorised. The service was resubscribed during the period of the warrant, resulting in the communications of the new subscriber being intercepted over a four day period. ASIO advised that when it identified the error, it deleted the intercepted data and provided the Attorney-General with a supplementary warrant report.

In the fourth incident, ASIO determined that it would not seek a warrant to continue intercepting a particular service. ASIO did not inform the Attorney-General, as required by s 13 of the TIA Act, that the grounds on which the warrant had been issued had ceased to exist and ASIO did not take steps to ensure the interception of communications under the warrant was discontinued. Subsequently, due to an administrative error, interception of this service was sought and authorised under a later warrant.

The fifth incident resulted from an error made by ASIO in the identification of a subscriber, which led to a service being wrongly intercepted.

The sixth incident resulted from an administrative error whereby a subscriber check indicating that a service had been disconnected was incorrectly thought to indicate the service remained active. Accordingly, ASIO did not inform the Attorney-General that the grounds on which the warrant was issued had ceased to exist and did not take steps to discontinue the interception. This oversight resulted in continued interception being authorised under a later warrant. In addition, ASIO later identified that the service



was probably resubscribed during the warrant period resulting in a further instance of communication from the subsequent subscriber being intercepted.

ASIO identified these additional breaches in January 2020 and provided notice of intention to revoke these warrants and requested that the interception be discontinued in each case. ASIO advised IGIS that it would delete all intercepted data and report the incidents to the Attorney-General. ASIO subsequently advised that reports had been provided to the Attorney-General.

### DESCRIPTION OF SERVICES

When ASIO submits a request to the Attorney-General to obtain a named person warrant under s 9A or s 11B of the TIA Act, ASIO must include details, to the extent these are known, sufficient to identify the telecommunications services that ASIO assesses the named person is using, or is likely to use. During 2017–18, IGIS questioned whether ASIO's warrant documentation made clear the nature of the services ASIO intended to target. Following this, ASIO, in consultation with IGIS, prepared standing guidance for the Attorney-General on how it describes telecommunications services. This advice was provided to the Attorney-General in January 2020.

### FAILURE TO DELETE DATA AS INTENDED

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 unintentionally remain. During 2019–20, IGIS identified two instances where data that ASIO had advised was deleted from all systems was still available on one system. One of these instances was caused by a failure of process. The second instance, which was identified by ASIO during the inspection, was due to a technical issue affecting the collection and storage of information obtained via a certain class of surveillance device. Following the inspection, ASIO conducted an historical review to determine if this technical error affected any other warranted collection during 2018–19. ASIO confirmed to IGIS that the failure to delete all data was an isolated technical incident. ASIO rectified the technical error and revised processes governing how information from that class of surveillance device is collected and stored. IGIS is satisfied with ASIO's review and remediation response.

## INCIDENTS RELATING TO SPECIAL POWERS UNDER THE ASIO ACT

### UNLAWFUL COMMENCEMENT OF JOINT WARRANTED OPERATION

In July 2019, ASIO notified IGIS of an incident concerning a joint operation conducted with a partner foreign service targeting an Australian person of security interest. The operation was conducted in two phases. In both phases of the operation participation by the foreign service required authorisation under its own laws as well as authorisation under an Australian warrant. The foreign service mistakenly understood that, so long as the foreign service was authorised to conduct the activity under its own laws, then the first phase of the operation could be undertaken without an Australian warrant. Consequently, when the ASIO operational team sought assurance that the activities of the foreign service would not commence prior to the Australian warrant being in place, the foreign service provided this assurance on the assumption that the warrant was only required for the second phase of the operation.

Before commencing the first phase of the operation, the foreign service asked an ASIO liaison officer in that country (who was not part of the relevant ASIO operational team) for confirmation that the foreign service could proceed with the operation. This request was

intended to maintain operational coordination with ASIO, as the foreign service believed it could proceed on the basis of its own authorisation. The ASIO liaison officer was unable to consult the relevant operational team and due to the urgency of the operation, confirmed ASIO's agreement for the foreign service to proceed. IGIS has reviewed this matter and found that the liaison officer misconstrued corporate records of operational planning discussions that had been held earlier that day, and mistakenly believed that the Australian warrant that would provide the requisite authorisation of the foreign service was already in place.

Accordingly, the foreign partner commenced the first phase of the operation without authorisation under Australian law, resulting in unlawful intelligence collection. On the same day, when ASIO became aware of the foreign service's action, it obtained a warrant for the activity. ASIO formally advised the foreign service that its activities were unlawful.

In response to the incident, ASIO advised IGIS that it would develop and implement new procedures for joint operational activity to mitigate the risk of a similar incident occurring. IGIS has reviewed ASIO's records relating to this incident, and has concluded that it was caused by poor communication processes between the relevant parties. IGIS is satisfied that ASIO's response to the incident was appropriate and timely. IGIS will continue to monitor the development of new procedures for joint operational activity.

### NON-COMPLIANCE WITH SECTION 25(7)(a) OF THE ASIO ACT

Section 25(7)(a) of the ASIO Act specifies that a warrant issued under s 25 of the ASIO Act must explicitly authorise the use of any force against persons and things that is necessary and reasonable. In July 2019, ASIO advised IGIS that search activity had occurred under a warrant that was non-compliant with s 25(7)(a). On the day of the planned search activity ASIO officers realised that the required authorisation had been omitted from the warrant. ASIO prepared an urgent application requesting the Attorney-General to issue a new warrant with the requisite authorisation; however, the search commenced before the Director-General made contact with the Attorney-General. The existing warrant was replaced by a new warrant during the period of the search activity. IGIS has considered the matter and is of the view that the omission of the mandatory authorisation did not invalidate the warrant. IGIS is satisfied that ASIO's prompt actions to seek immediate reissue of the warrant were reasonable.

### POTENTIAL UNAUTHORISED ACTIVITY UNDER SECTION 25 SEARCH WARRANT

The 2018–19 IGIS annual report noted that ASIO had advised IGIS of a possible breach of s 25 of the ASIO Act, whereby a person who examined records during a search activity may not have been authorised under s 24 of the ASIO Act to do so. ASIO had not concluded its investigation into the matter during the 2018–19 reporting period.

In 2019–20, ASIO advised IGIS of the results of its investigation. In 2018–19, an ASIO search team requested at very short notice the participation of an officer of another Commonwealth agency to support the execution of a search warrant under s 25 of the ASIO Act. At the conclusion of the search, a post-activity review identified that, while certain classes of officer from that Commonwealth agency were validly authorised under s 24 to participate in the search, the officer in question did not belong to any of the classes specified. All other members of the search party were validly authorised to execute the warrant. IGIS is satisfied with the action taken by ASIO in identifying and notifying this breach.

## DISCLOSURE OF INFORMATION FROM A FOREIGN PARTNER SERVICE

ASIO notified IGIS of an incident where it had received a disclosure of information from a foreign partner service about an Australian citizen which could not have been collected lawfully by ASIO without a computer access warrant under s 25A of the ASIO Act. IGIS reviewed the circumstances of this incident and concluded that ASIO's actions in relation to the disclosure could reasonably be argued to be lawful and proper. In particular, IGIS determined that ASIO did not solicit information on the Australian citizen from the foreign partner in a manner that could reasonably be interpreted as a request to collect or disclose information in circumvention of Australian law. IGIS considered that the incident highlighted systemic issues. IGIS considers that, should these issues remain unaddressed, it could result in future breaches. IGIS will continue to monitor how ASIO has addressed the systemic issues identified.

## INCIDENTS RELATING TO PART IV OF THE ASIO ACT

### BREACHES OF SECTION 38 OF THE ASIO ACT BY COMMONWEALTH DEPARTMENTS

In certain circumstances, s 38(1) of the ASIO Act requires a Commonwealth agency 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. During the reporting period, ASIO advised IGIS of two cases where a Commonwealth department failed to provide the relevant information within the time period required by s 38(1).

ASIO also advised IGIS of an additional instance where a Commonwealth department failed to comply with s 38(6) of the ASIO Act, which requires that notice of an adverse security assessment must be sent to the subject of the assessment by registered mail or hand delivery. The department instead provided this notice by ordinary post. ASIO identified the non-compliance and subsequently worked with the department to ensure that the requirements of s 38(6) were met.

IGIS is satisfied with ASIO's actions in relation to these three cases. ASIO has since contributed to work undertaken by the department to develop policies and internal guidance to minimise the likelihood of future breaches of s 38 of the ASIO Act.

### BREACH OF SECTION 39 OF THE ASIO ACT

Section 39 of the ASIO Act prevents Commonwealth agencies that receive advice from ASIO from taking prescribed administrative action against a person unless the advice is in the form of an adverse or qualified security assessment. ASIO advised IGIS of one instance where a Commonwealth agency took action that ASIO considered may have constituted prescribed administrative action in response to preliminary advice from ASIO that was not in the form of a security assessment. ASIO intervened to ensure that the subject of the advice was not adversely affected by the action of the Commonwealth agency. ASIO then met with the relevant agency to explain the incident and improve awareness of the requirements of the ASIO Act. IGIS is satisfied that ASIO's response to the incident was adequate and appropriate.

## 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 Attorney-General's Guidelines, and must be signed by a specified eligible person.

ASIO notified IGIS of three incidents relating to prospective data authorisations under s 176 of the TIA Act.

In the first incident, the eligible person was briefed on the facts and grounds for the two telecommunications services to be subject to the authorisation. However, due to human error the authorisation instrument signed by the eligible person omitted the details of one of the services, and this omission was not identified by officers responsible for communicating the authorisation to the recipient of the notice. Consequently, the recipient was instructed to provide data for both services, one of which was unauthorised. The error was identified on the same day the authorisation notice was issued and before any data had been provided. ASIO issued a revised authorisation instrument containing details of both telecommunications services. In response to this incident, ASIO advised IGIS that it would update its administrative procedures for notices under s 176 of the TIA Act to reduce the risk of human error in the future.

In the second incident, during drafting of the necessary approval documentation, relevant checks were not conducted against three individuals to ensure the individuals were at the correct investigation level in ASIO's case management system.

The third incident occurred when the approvals that would authorise maintaining the subjects of the prospective data authorisation at the correct investigation level in ASIO's case management system were not completed by the relevant due date. This omission was identified the following day and collection was ceased immediately.

ASIO also notified IGIS of two cases where telecommunications data was obtained contrary to s 175 of the TIA Act.

The first case involved three separate incidents within the same operation involving different telecommunications carriers. 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. ASIO advised IGIS that it was working to identify the data that was outside the specified criteria and to 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.

The second case involved human error in interpreting data used as the basis for four requests. This resulted in data being obtained that was earlier than the connection date of two services and, in one instance, data being sought for the wrong service. ASIO advised that the relevant data had been deleted. Separately, ASIO reported another case that highlighted similar problems in interpreting data.

These cases are currently being reviewed by ASIO and IGIS will consider ASIO's response following their review.



## QUESTIONING AND DETENTION WARRANTS

No questioning or questioning and detention warrants were authorised or used during the reporting period.

## 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 and 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.

## SPECIAL INTELLIGENCE OPERATIONS

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 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. Details of these operations are highly sensitive and cannot be included in a public report.

Unlike warrants issued under Division 2 of the ASIO Act, there is no requirement under Division 4 for an SIO to be discontinued if the requirement for special intelligence conduct has ceased. During 2019–20, IGIS identified several instances where ASIO had made a determination that conduct authorised under an SIO had ceased, but the authority was not cancelled and substantial time elapsed before the SIO authority expired. IGIS has advised ASIO that while there is no legislative requirement to do so, as a matter of propriety where ASIO makes a determination that conduct authorised under the SIO has ceased the authority should be cancelled as soon as practicable. ASIO has reported that it has updated its procedures to ensure that all officers understand this expectation. IGIS will continue to monitor ASIO's update to procedures.

## INCIDENT RELATING TO THE CRIMES ACT

In June 2019, ASIO notified IGIS of an incident that occurred in February 2019. The incident involved possible unauthorised access to a telecommunications device that had been lawfully seized by the AFP under the *Crimes Act 1914*. At the time of the incident, ASIO had a warrant under the ASIO Act that authorised access to the device. However, an ASIO officer assisting with the investigation accessed the device but was not authorised to do so under the warrant. ASIO gave consideration to notifying IGIS in February at the time the possible breach was identified, but then did not provide notification until June.



Following notification and further details of the incident, IGIS questioned the legal basis for the information provided by ASIO in the initial notification to IGIS and the legal consequences of the incident. In June 2020, ASIO concluded that the provision of the telecommunications device to the ASIO officers and the subsequent actions taken in relation to the device were lawful and authorised under the Crimes Act. IGIS concurred with ASIO's view regarding legality.

## **TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) ACT 2018**

In December 2018, the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* granted ASIO new powers in relation to obtaining industry assistance under the Telecommunications Act 1997. ASIO is required to notify the Inspector-General formally within seven days of a request or notice being given under the relevant legislative provisions set out in Part 15 of the Act. IGIS reviewed each use of these powers through its inspection program.

In addition, the Act granted ASIO new powers under the ASIO Act in relation to computer access and access to data, and voluntary assistance. The IGIS inspection program included a review of ASIO's use of these powers during the year. IGIS will continue to monitor procedures and activities around the use of these powers.

## **TEMPORARY EXCLUSION ORDERS**

In July 2019, the *Counter-Terrorism (Temporary Exclusion Orders) Act 2019* came into effect providing for the Minister to make temporary exclusion orders preventing a person from entering Australia for a period of up to two years. Section 10(2) of the 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). IGIS has included inspection of ASIO's assessments for the purposes of temporary exclusion orders in its regular inspection program. IGIS will continue to monitor ASIO's procedures and activities around the use of these orders through regular inspection plans.

## **THE ATTORNEY-GENERAL'S GUIDELINES**

The Attorney-General's Guidelines (the Guidelines) are issued under s 8A of the ASIO Act and are to be observed by ASIO in performance of its functions. Among other things, the Guidelines require ASIO to review each of its investigations on an annual basis. In 2019–20, a small number of investigations were conducted without review for periods longer than a year. ASIO proactively reported the majority of these breaches to IGIS. ASIO also notified two instances where subjects were not raised to the correct investigation level in ASIO's case management system.

The Guidelines also require that a security investigation into an entity must be reconsidered and reapproved at least annually by an ASIO officer of a certain seniority. ASIO notified IGIS of a breach of the Guidelines where, due to administrative and human error, an investigation was reviewed annually and reapproved three times by an officer who was not sufficiently senior. During this period, no intrusive activities were undertaken that required the correct





approval of the investigation into the entity. In response to the breach, ASIO terminated the investigation and conducted remedial training on the requirements of the Guidelines. IGIS is satisfied with ASIO reporting and remediation action.

In March 2020, ASIO identified a potential breach of the 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. The matter is currently being reviewed by ASIO and IGIS will consider ASIO's response following this review.

## **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 as part of IGIS's periodic inspections.

During the reporting period, ASIO exchanged information with a number of Australian Government agencies including the Australian Criminal Intelligence Commission (ACIC), Australian Federal Police (AFP), State and Territory police services, the Department of Home Affairs, the Department of Defence and the Department of Foreign Affairs and Trade. IGIS regularly reviewed these exchanges to assess ASIO's compliance with legislation, the Attorney-General's Guidelines and ASIO policy. IGIS did not identify any concerns.

## **ACCESS TO TAXATION INFORMATION**

Section 355-70 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 tax information is further governed by a memorandum of understanding (MOU) between the Commissioner of Taxation and the Director-General of Security, the Attorney-General's Guidelines and ASIO's internal guidelines and procedures. ASIO rarely requests access to this type of information.

During the reporting period, IGIS reviewed ASIO's access to sensitive tax information in the previous financial year 2018–19. IGIS did not identify any concerns. In the next reporting period, IGIS will review ASIO's access to taxation information for the period 2019–20.

## **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 only cooperate with foreign authorities approved by ASIO's Minister. ASIO has guidelines for the communication of information on Australians and foreign nationals to approved foreign authorities.

During the reporting period, IGIS conducted an inspection of ASIO's foreign liaison arrangements to assess the effectiveness of these arrangements in promoting information exchange that is consistent with human rights. The scope of the inspection included ASIO's internal policy regarding the disclosure of information about minors. While information exchange is considered through other inspection activities conducted by IGIS, this was the first time in several years that a specific inspection into the issue had been conducted.



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. These matters are currently being addressed by ASIO. IGIS will continue to monitor ASIO's progress.

## MINISTERIAL SUBMISSIONS

IGIS reviewed 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 accurately informs the Minister on relevant matters. During the reporting period, IGIS raised an issue identified in the previous period where potentially unreliable or misleading advice was provided to the Minister. ASIO addressed the matter and provided further advice to the Minister. IGIS is satisfied with the appropriateness of information provided in other submissions.

## SECURITY ASSESSMENTS

Security assessments issued by ASIO can result in administrative decisions, such as cancelling a visa or passport, which significantly affect the liberties of the person who is the subject of the assessment. In 2019–20, IGIS reviewed a sample of cases where ASIO issued prejudicial (adverse or qualified) security assessments. IGIS did not identify any issues during the reporting period.

## INSPECTION OF ASIS ACTIVITIES

The functions of ASIS are set out in s 6 of the IS Act. Under the IS Act ASIS can only perform these functions in the interests of Australia's national security, foreign relations or national economic wellbeing, and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia.

In performance of these functions ASIS undertakes a number of activities which are subject to IGIS oversight. The activities are categorised as follows:

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

During 2019–20, IGIS conducted a range of inspections of ASIS's activities. These inspections included the review of operational files, advice to the Minister for Foreign Affairs, weapons related matters and access to sensitive financial information. Inspections were conducted using a risk-based approach with priority given to operational file reviews. The approach

IGIS takes to each inspection varies, but usually it involves review of official ASIS records, discussions with officers from the agency and any other elements relevant to the particular inspection. 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. All inspections are followed by a letter from the Inspector-General to the Director-General of ASIS summarising IGIS's findings.

IGIS also conducts other review and oversight related activities. These other activities are an important part of the oversight of ASIS, and provide additional assurance that its activities are legal and proper. IGIS reviews all ASIS reports of legislative non-compliance or other significant matters. IGIS is also consulted on the legality and propriety of certain ASIS proposals and draft internal policies prior to finalisation; this allows IGIS to identify any concerns before action is taken. Normally, the Inspector-General and IGIS officers visit ASIS officers outside its Canberra headquarters, however, this did not occur in the reporting period due to the COVID-19 pandemic.

Inspections and other oversight activities are supplemented by awareness briefings on various matters throughout the year, either as IGIS requests, or as are provided proactively by ASIS. 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 ASIS as well as bi-monthly meetings between the Inspector-General and senior ASIS officers; these meetings cover a variety of matters. The COVID-19 restrictions limited IGIS's ability to carry out some inspections. However, some review and engagement activities did continue and IGIS officers were able to recommence normal inspection activities prior to the end of the financial year.

## INSPECTION OF OPERATIONAL FILES

IGIS officers regularly visited ASIS premises during 2019–20 to inspect ASIS's operational case files. Generally these inspections occur monthly, however, not all scheduled operational file inspections could occur as planned, primarily due to restrictions relevant to the COVID-19 pandemic.

Inspections of operational files involve reviewing a sample of files, focusing on higher risk areas as determined by IGIS. ASIS activities 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. Considerations applied in the inspections of operational files include the appropriate application of the Privacy Rules; compliance with internal guidelines, policies, and procedures; and human rights requirements such as conventions relating to the prohibition of torture and other cruel, inhumane or degrading treatment.

For a given overseas location, source or operation these inspections typically focus on records created in the previous two years. During the reporting period, IGIS inspected files relating to ASIS's operational activities in a number of countries, covering a wide variety of themes.

The sensitive nature of ASIS's operational activities means that specific details of inspection topics, and the matters identified cannot be provided in a public report. At the conclusion of these inspections, IGIS is satisfied that ASIS is appropriately identifying and considering legality and propriety risks associated with operational activities. No significant concerns regarding legality, propriety or human rights were detected and ASIS achieved a very high level of compliance.

It is a breach of s 15(5) of the IS Act for ASIS to communicate intelligence information concerning an Australian person other than in accordance with the Privacy Rules. An inspection identified an instance where ASIS communicated intelligence information on an Australian person to another Australian Government agency without first applying the Privacy Rules. This appears to have been an isolated case as on other occasions relating to this matter the Privacy Rules were clearly considered, correctly applied and appropriately documented. Moreover, it should be noted that in the isolated case the information would have met the requirements of the Rules had they been applied. Other inspections identified a number of record keeping issues which were minor in nature. IGIS is satisfied with ASIS processes and the remediation action taken.

## MINISTERIAL SUBMISSIONS

Through its bi-monthly inspections IGIS generally inspects and reviews all ministerial submissions sent by ASIS to the Minister for Foreign Affairs. IGIS reviews submissions to ensure that ASIS is appropriately and accurately informing the Minister on relevant ASIS matters. Due to work restrictions and disruptions resulting from the impact of the COVID-19 pandemic, IGIS could not conduct all the planned inspections of ministerial submissions. The majority of the submissions reviewed during the reporting period related to Ministerial Authorisations to produce intelligence on Australian persons; these are discussed below.

ASIS consulted IGIS on several proposed ministerial submissions with potential issues connected to legality and propriety. These submissions were primarily regarding proposed updates to requirements involving the production of intelligence on Australian persons. The Inspector-General provided comments and suggestions as appropriate, and having reviewed the submissions sent to the Minister, is satisfied that in each instance the Minister was accurately informed.

## MINISTERIAL AUTHORISATIONS TO PRODUCE INTELLIGENCE ON AUSTRALIAN PERSONS

ASIS is a foreign intelligence collection agency and intelligence activities it conducts on Australian persons attract IGIS scrutiny. During 2019–20, IGIS reviewed all Ministerial Authorisations obtained by ASIS from the Minister for Foreign Affairs up to February 2020 when this inspection was disrupted by the impact of COVID-19 restrictions.

The inspections conducted did not identify any breaches of legislation. IGIS identified one issue of propriety regarding the timeliness of advice to the Minister in relation to a Ministerial Authorisation whose grounds had ceased to exist. ASIS had appropriately ceased all activity as soon as the grounds ceased to exist but, due to an administrative error, ASIS did not advise the Minister in a timely manner. While the time within which the Minister is to be provided submissions to cancel Ministerial Authorisations will vary according to the facts of each case, in this instance IGIS considered that the Minister should have been advised sooner. IGIS is satisfied with ASIS processes and concluded that this was an isolated case and not indicative of a systemic issue.



## EMERGENCY MINISTERIAL AUTHORISATIONS

There were no emergency Ministerial Authorisations sought during the reporting period.

## THE ASIS COMPLIANCE BRANCH

The ASIS Compliance Branch aims to ensure that ASIS operates legally and in accordance with established authorisations and policies, develops internal policies and procedures, provides compliance and risk related advice and training to ASIS officers, and conducts investigations into matters of concern. The ASIS Compliance Branch works to develop and promote an agency culture of compliance.

When ASIS conducts an investigation into a matter of concern, IGIS receives a copy of the investigation report. IGIS independently 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.

## REPORTING OF COMPLIANCE MATTERS

During 2019–20, ASIS provided IGIS with seven reports related to activities in breach of the IS Act. Some reports covered more than one specific breach. All but one breach involved communications not in accordance with the Privacy Rules; this case is discussed below. Separate to these reports, ASIS undertook reviews into other matters of concern related to internal policies and procedures and reported to IGIS as appropriate. The number of breaches of the Privacy Rules and investigation reports provided to IGIS were generally consistent with the numbers in the previous reporting period. ASIS self-identified the majority of breaches and reported them to IGIS. IGIS is satisfied with ASIS reporting, investigation and remediation in these matters.

One of the compliance reports referred to above related to a failure to obtain a Ministerial Authorisation in breach of s 8 of the IS Act. This case involved ASIS being engaged in activities for the purpose of producing intelligence on an overseas Australian person who was likely involved in terrorism related activities. These activities occurred without a Ministerial Authorisation in place, or a written notice under s 13B of the IS Act. The case also involved two breaches of the Privacy Rules and a number of issues of administrative non-compliance. There was also a significant delay between the identification of this incident and notification to IGIS. The case was brought to the attention of the ASIS Compliance Branch following a compliance training session and subsequently the ASIS Compliance Branch notified IGIS and kept IGIS informed as the ASIS investigation progressed. ASIS advised IGIS that it was planning to use the scenario as part of its ongoing compliance training, and would update its internal Privacy Rules policy to minimise the risk of future similar breaches. IGIS reviewed the ASIS investigation report and raised additional matters, including further suggested changes to internal policy. As at 30 June 2020, these updates had not yet been implemented. IGIS will continue to engage with ASIS and monitor these changes.



## PROTECTING THE PRIVACY OF AUSTRALIAN PERSONS

During 2019–20, ASIS self-reported a total of 17 breaches of the Privacy Rules in the seven compliance reports referred to above. Seven of these breaches occurred between 2012 and 2015, which ASIS identified during 2019–20. An additional two breaches were identified by IGIS during inspection and other review work. Human error was the cause of the breach in the majority of cases. The errors included officers missing key information when reviewing a report prior to publication, failing to accurately interrogate a key ASIS database that contains information indicating a person's nationality, or not updating that database as required.

Noting the total volume of reporting that ASIS produced on Australian persons during 2019–20, the incidence of Privacy Rules breaches was rare. IGIS found no indication of systemic failings with ASIS's compliance controls or training. 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.

In its compliance reports ASIS identified some areas for improvement in record keeping or compliance, and IGIS identified some additional matters in its inspection and review work. IGIS will continue to monitor ASIS's application of the Privacy Rules closely as well as the implementation of areas identified for improvement. IGIS is satisfied with ASIS reporting procedures in these matters.

Under the Privacy Rules ASIS is also required to advise IGIS when it obtains information which leads to the overturning of the initial presumption that a person overseas is not an Australian person. If the initial presumption was reasonable, such incidences are not recorded as a breach of legislation or the Privacy Rules. In 2019–20, ASIS reported three occasions where such a 'presumption of nationality' was overturned. In all cases ASIS's initial presumption was reasonable and in accordance with the Privacy Rules as it initially had no evidence that the individuals, who were located outside Australia, were Australian. One case related to the s 8 compliance incident discussed earlier. Timely notification of this incident was not provided to IGIS or to other relevant intelligence agencies. IGIS is however satisfied with the basis of the initial presumption of nationality and will continue to monitor these matters and the timing of the notifications that should be made to IGIS.

## 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 except in the limited circumstances permitted by the IS Act. The IS Act provides for ASIS to equip its officers with weapons, and to train them to use weapons and self-defence techniques in certain circumstances, particularly in order to protect themselves or certain other people.

Schedules 2 and 3 of the IS Act require the Minister and the Director-General of ASIS to provide certain documentation relating to the use of force and weapons to the Inspector-General. This includes approvals for weapons and self-defence training; copies of the Director-General guidelines issued for the purpose of weapons and self-defence; approvals in specific circumstances where the Minister approves the use of force; and notification of officers or agents using weapons or self-defence techniques other than in training or approved scenarios. During 2019–20, the Director-General of ASIS issued new guidelines under Schedule 3 of the IS Act relating to the use of force or threats of the use of force, and updated guidelines made under Schedule 2 relating to the use of weapons and self-defence techniques. The Inspector-General was consulted during the drafting of



these documents, and the final versions did not raise any legality or propriety concerns. As required under the IS Act, the Inspector-General briefed the PJCS on these changes.

In the 2019–20 reporting period, the Minister and the Director-General of ASIS provided the reports required under the IS Act. The Inspector-General 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 in order 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 non-compliance with the Director-General's internal guidelines on weapons. In one case the Minister provided an approval for certain ASIS staff members to protect a number of persons in accordance with Schedule 2, Clause 1(3) of the IS Act.

IGIS examined ASIS weapons and self-defence policies, guidelines and training records during an inspection. No significant issues were identified. IGIS identified a record keeping error relating to how ASIS applied part of its guidelines issued under Schedule 2. IGIS is satisfied with ASIS processes and reporting, and its remediation of the record keeping error.

## INSPECTION OF ASD ACTIVITIES

The functions of ASD are set out in s 7 of the IS Act. ASD undertakes a number of activities in exercise of these functions. The activities which are subject to IGIS oversight 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.

IGIS inspection of ASD activities is facilitated by strong working relationships with ASD's Oversight, Compliance and Legal teams, and regular 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, and proactive reviews of areas of risk or sensitivity. IGIS also reviews selected ASD existing and proposed policies to ensure they are appropriate, implemented and effective.

During 2019–20, IGIS inspected a number of ASD activities, including:

- applications for Ministerial Authorisation to produce intelligence on Australian persons
- ASD's compliance with the Rules to *Protect the Privacy of Australians* (Privacy Rules)
- compliance incident reports
- ASD's access to sensitive financial information.

While COVID-19 restrictions had a minor effect on activities, most planned inspections were able to be conducted. Inspections were supplemented by briefings on various matters across the year, regular meetings with the ASD Oversight and Compliance teams, engagement with ASD Legal officers, and visits to ASD officers posted outside Canberra. The Inspector-General and the Director-General of ASD met formally on a quarterly basis to discuss oversight matters and developments.

## MINISTERIAL AUTHORISATIONS TO PRODUCE INTELLIGENCE ON AUSTRALIAN PERSONS

The IS Act requires that ASD obtain authorisation from the Minister for Defence before conducting certain activities, including the production of intelligence on Australian persons. During 2019–20, IGIS inspected the majority of ASD's applications for Ministerial Authorisation. These applications were generally of a high standard, and no significant issues were identified by IGIS officers, with the exception of the ministerial submission instances discussed below.

The 2018–19 IGIS annual report noted that IGIS had identified several instances where ASD did not include the appropriate administrative 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 2019–20 reporting period, IGIS identified further instances where appropriate administrative restrictions were not in place. ASD conducted an internal audit in September 2019 and to mitigate this risk of continued occurrence published further guidance for its officers in April 2020. There was some delay from initial identification of the issue to ASD taking remedial action and additional instances occurred over that time, however, IGIS has now seen a reduction in the number of instances identified. IGIS will continue to monitor the effectiveness of ASD's remedial actions.

## EMERGENCY MINISTERIAL AUTHORISATIONS

Situations may arise where, as a matter of urgency, ASD requires a Ministerial Authorisation to undertake certain activities. Emergency authorisations may be provided orally by the Minister for Defence, other select Ministers where the Minister for Defence is unavailable or, if the Ministers are not readily available the Director-General of ASD can authorise such activities. Emergency authorisations are valid for 48 hours after which a new authorisation is required if ASD is to continue the activity. ASD did not seek any emergency Ministerial Authorisations during the reporting period.

## MINISTERIAL SUBMISSIONS

During the reporting period, IGIS conducted a quarterly review of the submissions ASD provided to the Minister for Defence. In conducting these reviews IGIS considers whether the Minister for Defence is provided timely and accurate information about critical ASD issues.

In August 2019, ASD advised IGIS that it had conducted an audit of ministerial submissions prepared in support of all active Ministerial Authorisations. This audit was conducted at the Minister for Defence's direction following an incident where ASD had provided incorrect information to the Minister in a submission in support of a Ministerial Authorisation. ASD identified over one third of the submissions audited contained unclear or inaccurate advice. ASD assessed that none of the identified errors affected the grounds upon which the Ministerial Authorisations were sought or granted. At the Minister for Defence's request, 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. ASD has also undertaken to report quarterly to the Minister for Defence on its remedial actions. Based on IGIS's initial review of the matter it appears that these issues were the result of an insufficient quality assurance process. IGIS will continue to monitor this issue and the effectiveness of ASD's remedial actions.

Separate to the above, during the reporting period ASD notified IGIS of one instance where a warrant application contained incorrect information and one instance where a ministerial submission contained incorrect information. ASD has since strengthened its internal procedures to mitigate the likelihood of recurrence. IGIS reviewed the circumstances of each incident and was satisfied that ASD's remedial actions were appropriate to ensure the accuracy of submissions provided to Ministers.

## PROTECTING THE PRIVACY OF AUSTRALIANS

The Minister for Defence issues written rules (Privacy Rules) to regulate the basis on which ASD may communicate and retain intelligence information about Australian persons. The IS Act prohibits ASD from communicating intelligence information concerning an Australian person other than in accordance with those rules. The rules are publicly available on the ASD website.

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

ASD reported to IGIS cases where ASD, in accordance with the guidance set out in the rules, had initially presumed that an individual was not an Australian person, but where the presumption was subsequently overturned and the person shown to be Australian. ASD's reports included details of the measures taken to protect the privacy of that person including, as a propriety measure, informing other relevant intelligence agencies of overturned presumptions of nationality.

If the initial presumption was reasonable, such incidents do not breach legislation or the Privacy Rules. IGIS reviewed these cases and found that ASD's initial presumptions of nationality were reasonable given the information available to ASD at the time. IGIS found that ASD's actions were appropriate and in accordance with the Privacy Rules. IGIS is satisfied with ASD's compliance with Privacy Rules and reporting processes.



## LEGISLATIVE NON-COMPLIANCE

When ASD identifies breaches of legislation and significant or systemic matters of non-compliance with ASD policy, it proactively provides written notification of these issues to IGIS. ASD then undertakes an investigation of the incident and provides its findings to IGIS which reviews these reports and where necessary undertakes further independent investigation of the incidents.

### TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979

#### INCIDENT REPORTS

The TIA Act prohibits agencies from intercepting communications passing over a telecommunications system, except in limited circumstances, including where there is a warrant in place allowing interception.

The 2018–19 IGIS annual report stated that ASD had notified IGIS in May 2019 that it may have breached s 7 of the TIA Act. In June 2019, ASD confirmed that this incident did constitute a breach of s 7, as it had enabled interception without an appropriate warrant. In three instances, telecommunications ‘devices’ were specified for interception under warrants that could only lawfully authorise interception of telecommunications ‘services’. Although these telecommunications devices were targeted for interception no communications were intercepted as a result. This problem arose from ASD officers incorrectly believing that the telecommunications devices specified were telecommunications services. In November 2019, ASD provided IGIS the related compliance incident report. IGIS independently reviewed the circumstances of this incident and was satisfied that ASD had sufficiently sought to understand the novel technical elements of the incident, and had implemented appropriate remedial action.

In August 2019, ASD confirmed that it had breached s 63 of the TIA Act by communicating information that had been intercepted without an appropriate warrant. This information had been provided to ASD by a partner agency that, at the time, believed that the information had been lawfully obtained. In November 2019, ASD provided IGIS the related compliance incident report. IGIS reviewed this incident and found that ASD’s response and the remedial actions taken, including deleting the relevant information, were appropriate in the circumstances.

In February 2020, ASD notified IGIS that it may have breached s 7 of the TIA Act by intercepting communications without an appropriate warrant. ASD investigated this incident and in June 2020 confirmed that the activity was a breach of the TIA Act. As of 30 June 2020, ASD was conducting an internal investigation. IGIS will independently review ASD’s investigation and report in the 2020–21 annual report.

In addition to advising IGIS of confirmed breaches of legislation, ASD also advises IGIS of ‘potential breaches’, that is where it is technically possible that there was a breach but this cannot be proven. ASD categorises an incident as a potential breach when it is unclear, due to data limitations or the absence of essential details, whether a breach has occurred. IGIS reviews these matters in the same manner as it reviews confirmed breaches. During the reporting period, ASD reported one potential breach.

The 2018–19 IGIS annual report noted that ASD had notified IGIS in June 2019 that it may have breached s 7 of the TIA Act. ASD investigated this incident, and in late June 2019, confirmed that this issue constituted potential breaches of s 7(1)(a) and s 63 of the TIA Act, as ASD had likely intercepted and communicated certain information without an appropriate warrant. ASD also confirmed that it had breached s 7(1)(c) of the TIA Act as it

had enabled interception, regardless of whether interception had occurred. In this instance, an unanticipated change in the use of technology resulted in communications likely being intercepted that were outside the authority of a warrant. The information obtained from the interception was then likely communicated to partner agencies. Due to the technical nature of the incident, ASD could not confirm that interception or communication had occurred. Following ASD providing the related compliance incident report in November 2019, IGIS independently reviewed ASD's investigation. IGIS found that the technological adaptation could not have been reasonably foreseen by ASD, whose actions would otherwise have been entirely consistent with legislation. IGIS is satisfied with reporting and the mitigation measures enacted by ASD.

### OTHER INCIDENT REPORTS

In July 2019, ASD confirmed a legislative breach as a result of an electronic signals intelligence activity. In August 2019, ASD provided IGIS the related compliance incident report. A key issue which led to the incident was a lack of understanding about how a particular capability operated, a problem compounded by the pressure of a time sensitive operation. IGIS has independently reviewed this breach and determined that ASD's remedial actions, which included increased training to relevant areas and revised procedures to mitigate recurrence, were appropriate in the circumstances.

### INSPECTION OF AGO ACTIVITIES

The functions of AGO are set out in s 6B of the IS Act. In performance of these functions AGO undertakes a number of activities which are subject to IGIS oversight. The activities are categorised as follows:

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

During the 2019–20 reporting period, IGIS officers conducted inspections of the following AGO activities:

- applications for Ministerial Authorisations to produce intelligence on Australian persons
- Director's approvals and post activity reporting
- AGO's compliance with the AGO Privacy Rules
- AGO's access to sensitive financial information, which is discussed later in the report.

IGIS officers received briefings from AGO teams in Canberra, which gave IGIS a better understanding of the agency's functions and made it better equipped to identify emerging issues. These briefings also assisted IGIS to enhance relationships with AGO and to pursue issues observed during inspections.

The Inspector-General had three meetings with the Director of AGO during the reporting period. Among other matters the meetings discussed key issues and arrangements for oversight.

Based on inspection and review activities, IGIS is satisfied that AGO met the majority of its statutory obligations under the IS Act during the 2019–20 reporting period. IGIS is also satisfied that AGO continues to enhance its systems and processes to encourage compliance with legislation and internal procedures.

## **MINISTERIAL AUTHORISATIONS TO PRODUCE INTELLIGENCE ON AUSTRALIAN PERSONS**

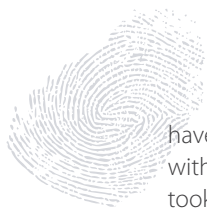
The IS Act requires AGO to obtain authorisation from the Minister for Defence before conducting certain activities, including the production of intelligence on an Australian person. This authorisation is ordinarily requested in conjunction with ASD. During 2019–20, IGIS officers reviewed a majority of the Ministerial Authorisation applications made by AGO. During the reporting period, AGO proactively reported one instance where it produced an intelligence product that included information relating to an Australian person, without obtaining a Ministerial Authorisation. IGIS officers reviewed this matter and the Inspector-General agreed with AGO's assessment that the incident did not comply with s 9 and s 15 of the IS Act. The Inspector-General was satisfied with the remedial action AGO took in response to the incident, including informing the Minister for Defence of the non-compliance. Additionally, AGO implemented measures to mitigate the likelihood of future non-compliance in similar circumstances. IGIS did not identify any other concerns relating to AGO's applications for Ministerial Authorisation, renewals, or circumstances in which AGO sought to cancel an authorisation.

## **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. The Director of AGO is also required to provide the Minister with quarterly reports on the activities conducted in accordance with such approval. The accuracy of these and other reports provided to the Minister for Defence were reviewed by IGIS during the reporting period and no issues were identified. At the conclusion of approved activities, AGO officers prepare a post-activity compliance report for the Director, which IGIS examines. During 2019–20, no significant issues with these reports were identified.

## **AGO COMPLIANCE WITH PRIVACY RULES**

The Minister for Defence issues written rules (Privacy Rules) to regulate AGO's communication and retention of intelligence information concerning Australian persons. During the 2019–20 reporting period, IGIS conducted an in-depth inspection to review AGO's application of the Privacy Rules, using a sample of AGO products published between July 2018 and October 2019. IGIS officers identified 16 products where a privacy rule was not correctly applied. It should be noted that in these instances the information would



have met the requirements of the Privacy Rules had they been applied. IGIS, in cooperation with AGO, identified the factors that led to the non-compliance, and AGO subsequently took remedial action to make future recurrence less likely. This included implementing compliance checklists, additional training, and specific prompts in approval templates, which will assist in preventing similar non-compliance. IGIS is satisfied with AGO's remedial actions.

Additionally, IGIS identified five products produced under a Director's approval where a privacy rule was not applied. AGO found that this non-compliance resulted from a misunderstanding within a particular team about the application of the rules, and subsequently provided additional training and compliance support to the team. IGIS is satisfied that AGO took appropriate actions to address the non-compliance.

## AUSTRALIAN HYDROGRAPHIC OFFICE

In October 2017, the AHO functions were transferred from the Royal Australian Navy to AGO. This transfer meant that IGIS assumed oversight of the functions of the AHO in relation to any intelligence collection or application of the AGO Privacy Rules. The AHO has fully incorporated IS Act requirements into its daily workflows and has received relevant compliance training. However, due to current differences in task tracking and recording in separate systems, IGIS has not yet reviewed any AHO products. In the 2019–20 reporting period, IGIS was unable to conduct planned outreach and inspection activities at the Wollongong site due to the COVID-19 restrictions. Pending the finalisation of infrastructure upgrades at the Wollongong site, IGIS officers will conduct outreach and inspection activities during the 2020–21 reporting period. Given the nature of AHO work, IGIS assesses that the risk of non-compliance is low.

## INSPECTION OF DIO ACTIVITIES

DIO is part of the Department of Defence and is mandated to support:

- the planning and conduct of ADF operations
- Defence Organisation policy, planning and decision-making
- the development and sustainment of Defence capability
- wider government planning and decision-making on defence and national security issues.

DIO is not subject to direction in regard to the judgments in its intelligence assessments.

To fulfil its role, DIO is mandated to provide:

- assessment, advice and services to support the planning, command and conduct of current and potential operations by the ADF
- timely assessments of countries and foreign organisations relevant to Australia's security and strategic environment, including 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.

Given its lower risk profile as an assessment agency, in comparison with a collection agency, inspections of DIO are less frequent. IGIS focused its inspection resources on the key areas of legality and propriety risks for DIO.



Oversight of DIO activities is facilitated by strong working relationships with DIO's Governance Team, and IGIS access to required information and systems. In the 2019–20 reporting period, IGIS conducted inspections of DIO's compliance with the *Guidelines to Protect the Privacy of Australian Persons* (Privacy Guidelines). IGIS officers also reviewed DIO's access to sensitive financial information from AUSTRAC, which is discussed later in this report.

In addition to these inspection activities, IGIS officers attended relevant compliance and analytical training facilitated by DIO, and monitored the percentage of DIO personnel that have completed mandatory compliance training requirements. DIO personnel proactively briefed IGIS about new activities and capabilities; this is of valuable assistance to IGIS's understanding of DIO's operating environment.

In the reporting period, the Inspector-General and senior IGIS officers met with DIO senior leaders to discuss key issues and arrangements for oversight. Additionally, the Inspector-General conducted an outreach session to DIO officers covering the role and functions of the Inspector-General, and IGIS's approach to the performance of its functions.

In the reporting period, restrictions relevant to the COVID-19 pandemic compromised the ability for IGIS to conduct inspections and reviews at DIO. A planned analytical integrity inspection was not able to be conducted due to this restricted access and is now planned for 2020–21.

## COMPLIANCE WITH DIO'S PRIVACY GUIDELINES

IGIS reviewed DIO's compliance with the Privacy Guidelines once during the reporting period. The second inspection for the reporting period was not undertaken due to COVID-19 restrictions; this inspection is now scheduled for the 2020–21 reporting period. The Privacy Guidelines, which are available on the DIO website, are similar to the privacy rules established under s 15 of the IS Act for ASIS, ASD and AGO. They allow DIO to perform its role while respecting the privacy of Australians. IGIS did not identify any significant issues or concerns in this reporting period, and there was no evidence that DIO failed to comply with the Privacy Guidelines.

## 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* 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 Act.

The legislation also imposes reporting, administration and audit regimes on those agencies using assumed identities. Section 15LG of the *Crimes Act 1914* requires ASIO, ASIS and ONI to conduct six monthly audits of assumed identity records and s 15LE requires that each agency provide the Inspector-General with an annual report containing information on the



assumed identities created and used during the year. During 2019–20, the Director-General of Security, 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 2018–19 reporting period. There was nothing in the reports to suggest that ASIO, ASIS or ONI were not complying with their legislative responsibilities or which otherwise caused significant concern. Agency reports covering the period 2019–20 will be submitted during 2020–21.

### ACCESS TO SENSITIVE FINANCIAL INFORMATION BY INTELLIGENCE AGENCIES

The *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (AML/CTF Act) provides a legal framework in which designated agencies are able 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 AML/CTF Act.

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

In overseeing the agencies' use of AUSTRAC information, IGIS officers check that there is a demonstrated intelligence purpose pertinent to the agencies' functions, that access is appropriately limited, searches are focused, and that information passed to both Australian agencies and foreign intelligence counterparts is correctly authorised. In 2019–20, as it does each year, IGIS prepared a statement summarising compliance monitoring in respect of each of the intelligence agencies concerning their access to, and use of, AUSTRAC information in the preceding financial year and provided this to relevant Ministers and the AUSTRAC Chief Executive Officer.

In the 2019–20 reporting period, IGIS conducted an inspection of ASIS's 2018–19 records concerning AUSTRAC information, as well as reviewing ASIS's use of AUSTRAC material during routine inspections. The inspections found that ASIS's governance and record keeping in relation to AUSTRAC information continued to be effective and there were no instances of non-compliance observed with this material during the period.

Separately, IGIS reviewed the access to, and use and protection of, sensitive financial information by ASD, AGO and DIO in 2018–19. These inspections revealed no instances of non-compliance by these agencies regarding the access to, and use and protection of, AUSTRAC information. ASD, AGO and DIO 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. All three agencies have effective procedures in place for handling this information.

IGIS also inspected ASIO's use of AUSTRAC material during 2018–19. The overall standard of ASIO's use of AUSTRAC material has improved when compared with previous reporting periods, particularly in its compliance with the dissemination and communication requirements of the AML/CTF Act. The inspection identified record keeping issues relating to policy and procedures, including issues relating to the record keeping requirements set out in the MOU between ASIO and AUSTRAC. ASIO is currently revising internal policies and procedures which, together with increased training for ASIO officers in handling AUSTRAC information and the establishment of a central internal compliance directorate, will assist ASIO to address the deficiencies identified during this period.

## COVIDSAFE APP PROJECT

On 16 May 2020, Part VIIIA was introduced into the *Privacy Act 1988* (Privacy Act); it sets out privacy protections that relate specifically to personal information collection via the COVIDSafe app.

Part VIIIA introduced offences for the collection, use and disclosure of COVIDSafe app data. This new Part has implications for intelligence agencies under the jurisdiction of the Inspector-General, in particular in respect of the incidental collection of COVIDSafe app data amongst lawfully intercepted material. Part VIIIA provides exceptions to certain offences that relate to incidental collection of COVIDSafe app data during the collection of other data under a warrant. No offence is committed if the COVIDSafe app data is deleted as soon as practicable after the agency becomes aware that it has been collected, and that it has otherwise not been used, accessed or disclosed after it has been collected.

A project was established within IGIS that aims to identify those agencies under the Inspector-General's jurisdiction that are most likely to be at risk of incidentally collecting COVIDSafe app data, and to determine if these agencies are taking the necessary steps to comply with Part VIIIA of the Privacy Act.

Given the intersecting areas of oversight that Part VIIIA creates, this project is being undertaken in cooperation with the Office of the Australian Information Commissioner (OAIC). The OAIC is the agency responsible for compliance with the Privacy Act, and also regulation of the COVIDSafe app. An unclassified report will be shared with the OAIC at the completion of the initial assurance activities undertaken by IGIS which will allow for completion of their obligations under the Privacy Act to be satisfied.

Inspection activities of intelligence agencies under the Inspector-General's jurisdiction related to the project is planned to continue until use of the COVIDSafe app is discontinued by government and all related COVIDSafe app data is deleted.

## ACTIVITIES RELATING TO ACIC, AFP, AUSTRAC AND THE DEPARTMENT OF HOME AFFAIRS

### PROPOSED EXPANSION OF IGIS ROLE

The *2017 Independent Intelligence Review* recommended far-reaching changes to Australia's intelligence bodies. One recommendation of that Review is that the jurisdiction of the Inspector-General be expanded to include the intelligence functions of the ACIC, AFP, AUSTRAC and the Department of Home Affairs. While the final form and timing of any expanded jurisdiction remains a matter for the Government and Parliament, IGIS has continued to build the relationships and understanding of the activities of these four agencies, and is developing interim inspection plans accordingly.

### OUTREACH

During 2019–20, IGIS continued to engage with key contacts and senior managers within the ACIC, AFP, AUSTRAC, and the Department of Home Affairs, 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, specific operational and capability briefings, observation of inspections by OCO officers and regional visits. Outreach activities have also focused on explaining the role of the Inspector-General and IGIS's approach to the role. In addition, some IGIS officers have

been placed with the agencies to assist in building a detailed and practical understanding of their intelligence functions and the internal policies and procedures that support those functions. The immersive development placement program is discussed further in Objective 6 of this report.

## OBJECTIVE 4 – COMPLAINTS AND PUBLIC INTEREST DISCLOSURES

### ABOUT COMPLAINTS

For practical purposes, communications received by IGIS expressing a grievance are categorised either as ‘contacts’ or ‘complaints’. Contacts are communications raising grievances that fall outside the jurisdiction of the Inspector-General, or which otherwise cannot be progressed for various reasons, including that they are clearly not credible or not intelligible.

IGIS categorises a matter as a complaint if it raises an initially credible allegation of illegal or improper conduct or an abuse of human rights in relation to an action, or alleged action, of an intelligence agency within the jurisdiction of the Inspector-General. Complaints can be made orally or in writing and they may be made anonymously.

Each communication is assessed to determine the most appropriate course of action and whether it falls within the PID scheme. Matters which fall within the PID scheme are managed with the requirements of that scheme. Complaints are usually handled administratively in the first instance. In most cases, complaints and other matters can be resolved quickly and efficiently by IGIS officers contacting the relevant agency or reviewing their records. This approach can determine whether a particular matter is within jurisdiction and reduce the procedural burden of an inquiry. Administrative resolution usually gives the complainant a timely response, and information sought from agencies in this way can help the Inspector-General determine whether to conduct an inquiry for more serious or complex matters.

Each person who contacts IGIS with a complaint is given advice about actions taken in response to their concerns and the outcomes, to the extent possible within IGIS security obligations.



## QUANTITATIVE PERFORMANCE MEASURES

**Figure 2.2: Timeliness of response to complaints**

COMPLAINT TYPE	TOTAL NUMBER OF COMPLAINTS	COMPLAINTS ACKNOWLEDGED WITHIN FIVE BUSINESS DAYS (TARGET: 90%)	AVERAGE BUSINESS DAYS TO ACKNOWLEDGE COMPLAINTS	VISA/ CITIZENSHIP-RELATED COMPLAINTS RESOLVED WITHIN TWO WEEKS (TARGET: 85%)
Visa/ citizenship-related	300	99%	1.4	96%
Other IGIS Act complaints	35	80%	3.4	N/A
Public Interest Disclosures	2	100%	3	N/A
TOTAL	337	97%	1.6	

\*Total includes weighted averages.

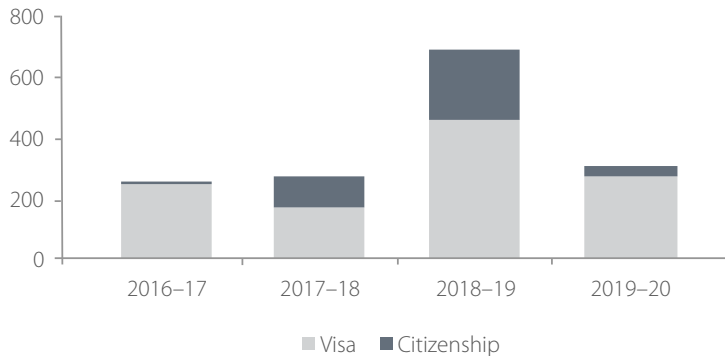
## COMPLAINTS ABOUT VISA AND CITIZENSHIP APPLICATIONS

The Department of Home Affairs processes visa and citizenship applications. There are occasions when applications will be referred to other government agencies to conduct necessary background checks. When asked to do so by the Department of Home Affairs, ASIO may make a security assessment or provide advice in support of the visa process. IGIS's role in reviewing ASIO's conduct is to ensure standards of legality and propriety are met.

Complaints to IGIS about visa and citizenship are almost invariably related to an application taking longer than the applicant anticipated. The last three years of investigating visa and citizenship complaints have revealed no instances of illegality or impropriety in the way ASIO managed the applications. As a result, in March 2020, the Inspector-General changed the way this category of complaint is handled. Each complaint continues to be individually assessed and acknowledged upon receipt. Complaints meeting identified criteria are referred to the inspection team for incorporation in the inspection program. Relevant inspection criteria have been established to ensure the IGIS inspection program identifies any concerns about the legality or propriety of ASIO's handling of these cases when conducting security assessments and providing advice. The results of inspections are passed to a complaints officer so that any trends or anomalies can be identified. Complex cases which go beyond the usual concerns about processing are considered promptly by inspection team officers, outside the routine inspection program. The inspection team takes responsibility for any further investigation and correspondence relating to a complex case.

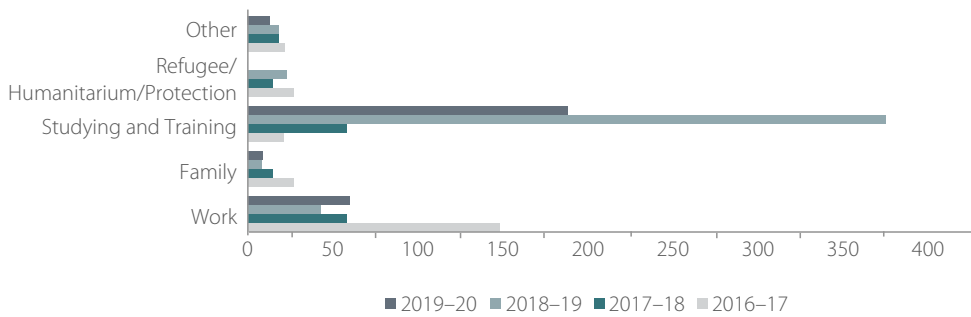
In 2019–20, IGIS received 300 complaints about visa or citizenship applications, a notable 60% drop from 2018–19 (Figure 2.3), and more in line with the two preceding years. There was also a reduction in these type of complaints received in the final quarter of 2019–20 (44 complaints compared to the quarterly average of 75). This period coincided with COVID-19 and could reflect global uncertainty and travel restrictions.

**Figure 2.3: Visa and citizenship complaints received per year 2016–17 to 2019–20**



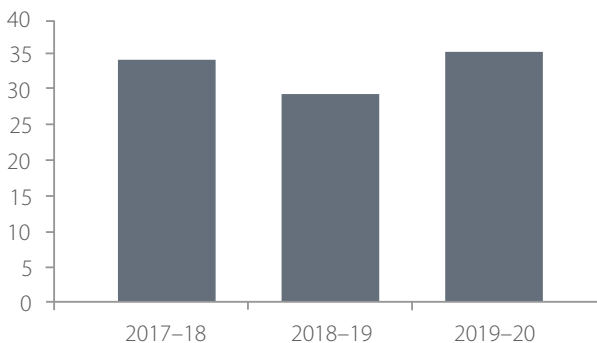
Of the 300 visa and citizenship related complaints received, 90% concerned the time taken to finalise visa applications, and 10% concerned citizenship applications (Figure 2.3). Of the complaints about visa processing delays, over two thirds related to visa applications to study or train in Australia while one fifth concerned work related visas (Figure 2.4). One complaint concerned a person in detention, but unlike previous years, there were no complaints lodged in 2019–20 regarding refugee/humanitarian/protection visa applications. There was an 89% reduction on the previous period in complaints about delays in processing citizenship applications, from 283 complaints in 2018–19 to 30 in 2019–20.

After an initial review, twenty five complaints about visa and citizenship matters were assessed as falling outside the jurisdiction of the Inspector-General. Of the 275 complaints within jurisdiction, no instances of illegality or impropriety were identified. IGIS identified only one complaint where a processing error had occurred, and the agency rectified the oversight after it was brought to its attention.

**Figure 2.4: Visa complaint trends 2016–17 to 2019–20**

## OTHER COMPLAINTS MADE UNDER THE IGIS ACT

IGIS received 35 other complaints in the reporting period (excluding PID matters), and four requests for a review of a complaint. One complaint received in 2018–19 was carried into the 2019–20 reporting period, while at the end of 2019–20 three complaints remained open. The average time taken to acknowledge complaints was three business days. IGIS officers responded to 80% of such complaints within five business days, below the performance measure of 90%. In three of the seven complaints affected by a delay in acknowledgement, the delay was attributed to restrictions implemented in response to COVID-19. Delay in the remaining four cases was attributed to competing priorities and available resources. Four complainants sought a review because they were dissatisfied either with the IGIS officer's handling of their complaint or with the outcome of their complaint. In each of these cases, a review of all relevant information by a more senior IGIS officer found no reason to take any further action.

**Figure 2.5: Other complaint statistics 2017–18 to 2019–20**

**Figure 2.6: Breakdown of complaint by agency and allegation 2019–20**

ALLEGATIONS	ASIO	ASIS	ASD
Access to records	1		
Breach of privacy	1		
Communication issues	2		
Conflict of interest	1		
Delay – personal security clearance	8		
Detriment arising from agency action	6		
Employment - management action or security related	2	3	1
Employment - recruitment	4	1	
Warrant – conduct, return of property seized	3	2	
TOTAL	28	6	1

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, and where possible, to facilitate a resolution to complaints. IGIS officers have established effective relationships with agency staff which ensures most matters are able to be resolved in a timely manner.

On finalisation, 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.

The majority of complaints (28) were about ASIO, while six were about ASIS and one concerned ASD. No complaints were received about AGO, DIO or ONI.

The complaints covered a wide range of matters, including allegations related to:

- security assessments for employment
- return of property seized under warrant
- employment issues including recruitment processes, and management or security related action
- detriment arising from agency action.

Eight of the complaints in 2019–2020 were related to delays by ASIO in undertaking an assessment of suitability for an individual to be granted a security clearance for employment purposes. This compares with eleven such cases in the previous reporting period. In several cases, a member of the public had complained more than once. These cases had been with ASIO for some time and had previously been the subject of scrutiny by IGIS.

IGIS sought advice from ASIO on each case and reviewed a sample of relevant ASIO holdings. IGIS considered the eight complaints regarding the time taken by ASIO to complete security assessments, and information gained in previous reporting periods. Based on this, IGIS is satisfied that ASIO's processing of security assessments for personal security clearances is systematic, with cases prioritised on the basis of any externally-set priorities as well as the age of referrals.

In addition to the above, it should be noted that ASIO conducts thorough assessment of all cases, including giving proper attention to complications, particularly where the circumstances could lead to a prejudicial outcome. No concerns were identified in the reporting period about the legality or propriety of ASIO's handling of these cases. In cases where complainants held particular concerns about delay, IGIS suggested the complainant seek prioritisation through their employer.

Six complaints about ASIO were broadly classified as alleging detriment arising from agency action. The type of detriment claimed to have been suffered included a breach of privacy, and difficulties in personal circumstances due to inaction or lack of support or the conduct of an officer. IGIS's response when matters such as these are brought to its attention includes reviewing relevant ASIO records and briefings, and referral to ASIO for it to investigate and consider management action, if appropriate. IGIS identified no illegality or impropriety by ASIO in the matters raised with us in 2019–20.

Five of the complaints were about warrant operations. Four of these concerned property that was either seized or misplaced during the operation. Another made serious claims about the conduct of an operation, including ASIO's alleged use of force. ASIO has certain obligations regarding any use of force, including reporting its use to IGIS. The complaint was referred to IGIS inspection officers for a search of relevant ASIO records. No illegality or impropriety by ASIO was identified by IGIS. We note that ASIO may conduct warrant operations with assistance from relevant Commonwealth or State police services. Other agencies also conduct their own warrant operations. A complainant may not always identify the correct agency responsible for the issues of concern and for matters outside IGIS jurisdiction the complainant is advised to contact the relevant agency.

## 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 is quite general in nature which can be frustrating for them.

Four complainants sought a review of their complaint because they were dissatisfied either with the IGIS officer's handling of their complaint or with the outcome of their complaint. A more senior IGIS officer reviewed the complaints and no concerns were identified through these reviews. Requests for these reviews largely arose because information could not be provided to complainants.

## ABOUT PUBLIC INTEREST DISCLOSURES

The PID Act is intended to promote integrity and accountability within the Commonwealth public sector. This includes by encouraging PIDs by public officials, providing appropriate support to disclosers to ensure they are not subject to adverse consequences as a result of their disclosures and ensuring that disclosures by public officials are properly investigated and addressed.

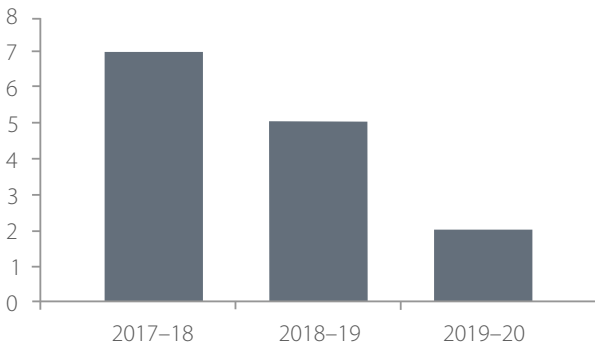
## IGIS'S HANDLING OF PUBLIC INTEREST DISCLOSURES

IGIS has key responsibilities under the PID scheme, 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 12 authorised officers under the PID scheme in addition to a principal officer (the Inspector-General). These officers are accessible to intelligence agency staff due to their regular attendance at agencies for routine activities such as inspections and briefings. IGIS authorised officers are also contactable via classified email and phone.

**Figure 2.7: Number of PIDs received 2017–18 to 2019–20**



**Figure 2.8: PIDs by agency and outcome in 2019–20**

AGENCY	ASIO	ASIS
Number of PIDs	1	1
Acknowledged within 5 business days	Y	Y
Disclosable conduct	Maladministrtrtion	Maladministrtrtion
Outcome	No evidence to support claims	Closed without investigation in accordance with 48(1) of the PID Act

IGIS received two PIDs concerning intelligence agencies during the reporting period, continuing a downward trend across the last three periods. No disclosable conduct was reported in relation to IGIS.

Both PIDs raised allegations of maladministration. One concerned allegations that a senior officer interfered in HR related matters. This disclosure was investigated in accordance with the IGIS Act rather than the PID Act to enable use of IGIS inquiry powers if required. No evidence was found to substantiate the claim.

The second concerned allegations of inadequate support to officers in a high risk environment. In accordance with s 48(1)(h) of the PID Act, the Inspector-General exercised her discretion not to investigate the disclosure. The discloser did not want investigation of the disclosure to be pursued, and the Inspector-General was satisfied that there were no matters that warranted investigation.

Separately, in May 2019, IGIS received a PID from a former intelligence agency employee. Following preliminary investigations, in August 2019 the Inspector-General decided to conduct an inquiry under s 8 of the IGIS Act. Although the inquiry was triggered by a PID made under the PID Act, it was decided that the matter would be more appropriately investigated under s 8 of the IGIS Act to enable the use of IGIS inquiry powers if required. The details of this matter are included in the Inquiries section of this report.

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

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

Agency staff engaged regularly with IGIS to notify when a PID had been received. During the reporting period IGIS was advised of four PIDs received by the intelligence agencies. The agencies advised of the actions taken in each matter, including when the matter was being investigated under a 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 also has a role in meeting annual reporting obligations by collecting and collating the intelligence agencies' responses to the OCO's annual PID survey. IGIS performs this role to ensure the protection of classified details relating to the intelligence agencies. The results of these are reported in the Ombudsman's annual report.

## OTHER CONTACTS

In 2019–20, IGIS also received contacts from approximately 180 individuals seeking advice or expressing concern about matters affecting them that were assessed to be either outside the jurisdiction of the Inspector-General or as not requiring action. This represents around 10% fewer than the previous reporting period, however, as many contacted IGIS on multiple occasions, the impact of the reduction was not noticeable.

When IGIS is contacted about matters it cannot pursue, IGIS officers provide written or oral advice about the Inspector-General's jurisdiction and alternative action that can be taken to resolve concerns. This includes reference to other complaint-handling bodies, police and

the National Security Hotline where appropriate. In cases where there has been previous contact about matters that have already been assessed, IGIS takes no further action unless substantially new and credible information is provided.

## OBJECTIVE 5 – INFRASTRUCTURE AND STAKEHOLDERS

### INFRASTRUCTURE AND GOVERNANCE

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

In mid-2020, the Office implemented its new case management system, and an electronic records management system on the Protected system. The installation of the classified LAN has been delayed. The electronic records management system and case management systems will be installed on the classified LAN in the next reporting period. The case management system has been designed to meet the particular work requirements of IGIS.

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

An internal governance review was conducted to design governance arrangements that will suit the increased size of the Office. The recommendations of the review will be implemented through 2020.

### LIAISON WITH DOMESTIC ACCOUNTABILITY AND INTEGRITY AGENCIES

IGIS regularly liaises with other accountability and integrity agencies in Australia, to discuss matters of mutual interest such as oversight processes, administrative improvements, implementation of legislative changes, and significant developments in relevant domestic and global issues. The Inspector-General also attends the twice yearly Integrity Agencies Group (IAG) meeting which brings together the heads of the integrity agencies and other relevant Commonwealth departments. The purpose of the IAG is to lead coordination, enhancement and promotion of institutional integrity across the Commonwealth.

Recommendations of the *2017 Independent Intelligence Review* included that the jurisdiction of the Inspector-General be extended to include the intelligence functions of the ACIC, AFP, AUSTRAC and the Department of Home Affairs. As noted in the 2018–19 annual report, IGIS has engaged with other accountability and integrity agencies on measures to ensure that future changes to oversight processes are complementary and avoid overlap wherever possible. It was reported that agreement-in-principle has been reached and set out in a Statement of Cooperation. The Statement of Cooperation will be finalised following legislation to extend the jurisdiction of the Inspector-General.



## AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

During the reporting period, IGIS continued to strengthen the relationship with ACLEI ahead of proposed changes to the Inspector-General's jurisdiction. Two IGIS officers completed immersive development placements with ACLEI to enhance understanding of their activities, practices and procedures.

## AUSTRALIAN HUMAN RIGHTS COMMISSION

The Australian Human Rights Commission is required by s 11(3) of the *Australian Human Rights Commission Act 1986* to refer human rights and discrimination matters relating to an act or practice of the intelligence security agencies to the Inspector-General. During 2019–20, no such matters were referred by the Australian Human Rights Commission.

## INSPECTOR-GENERAL OF THE AUSTRALIAN DEFENCE FORCE

There was continued liaison with the Inspector-General of the ADF in areas of common interest.

## OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER

IGIS continued to engage with the OAIC in developing a shared understanding of the complementary roles of IGIS and OAIC. As described in Section Two of this report, IGIS has been cooperating with the OAIC to ensure effective oversight of the COVIDSafe app.

## OFFICE OF THE COMMONWEALTH OMBUDSMAN

During the reporting period, IGIS continued to engage regularly at various levels within the OCO. In the course of this engagement IGIS officers have observed elements of OCO inspections of agencies that are within the scope of the proposed expansion of the Inspector-General's jurisdiction. In some respects the responsibilities of the OCO and IGIS are complementary; a memorandum of understanding between the two offices provides guidance for handling complaints that fall within the overlapping jurisdiction of each office. During 2019–20, an IGIS officer completed an immersive development placement at OCO.

## INTERNATIONAL ENGAGEMENT WITH ACCOUNTABILITY AND INTEGRITY AGENCIES

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

## FIVE EYES INTELLIGENCE OVERSIGHT AND REVIEW COUNCIL

In 2019–20, the Inspector-General continued her engagement with the FIORC. The FIORC is comprised of the following intelligence oversight, review and security entities of the Five Eyes countries: the Office of the Inspector-General of Intelligence and Security of Australia; the Office of the Intelligence Commissioner and the National Security and Intelligence Review Agency of Canada; the Commissioner of Intelligence Warrants and the Office of the Inspector-General of Intelligence and Security of New Zealand; the Investigatory Powers Commissioner's Office of the United Kingdom; and 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; explore areas where cooperation on reviews and the sharing of results is permitted and appropriate. They encourage transparency to the greatest extent possible to enhance public trust, and they maintain contact with political offices, oversight and review committees, and non Five Eyes countries as appropriate. FIORC meets in person at least once each year; in 2019 the meeting took place in the United Kingdom and was attended by the Deputy Inspector-General Mr Jake Blight, Assistant Inspector-General Ms Bronwyn Notzon-Glenn, and a senior IGIS officer.

At the conclusion of the forum, the FIORC agreed to establish working level committees on three topics: automated data processing and AI; 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 2019–20, IGIS completed work to support the working committee on methods to mitigate risks of mistreatment from sharing information with foreign entities. This involves considering how intelligence and security agencies may mitigate risks of human rights abuses by foreign entities when agencies share information with these entities, and how to improve coherence across the Five Eyes countries when overseeing agencies for such purposes. IGIS has developed a paper on the legal framework applicable to Australian intelligence and security agencies, policies and procedures, reporting arrangements, and oversight trends observed by IGIS regarding sharing information across borders, and associated safeguards.

In consultation with Australia's intelligence agencies IGIS is continuing to work towards a set of principles that encapsulates the Inspector-General's expectations around the passage of information to foreign entities. These principles will reflect Australia's high standards in relation to the prohibition on torture, cruel or inhuman treatment and punishment, and unlawful killing.

During the 2019–20 reporting period, FIORC also liaised via regular teleconferences to discuss topics of mutual interest or priority. The 2020 FIORC meeting, scheduled to be hosted by New Zealand in October 2020, was cancelled due to the COVID-19 pandemic. Teleconferences have enabled the FIORC members to continue to liaise and progress the work of the three working committees.

## INTERNATIONAL INTELLIGENCE OVERSIGHT FORUM

Directly before the October 2019 FIORC meeting, the Deputy Inspector-General and a senior IGIS officer attended the International Intelligence Oversight Forum (IIOF) in London. This was the fourth iteration of the conference series which since 2016 has been hosted under the mandate of the Special Rapporteur on the right to privacy.

## BILATERAL ENGAGEMENT

In August 2019, the Inspector-General met the Canadian Assistant Chief Defence Intelligence at National Defence, Marie-Hélène Chayer. Canadian Defence Intelligence is comparable to DIO. Ms Chayer is responsible for Defence Intelligence policy, oversight and analysis. The meeting covered how the IGIS office operates, in particular how

oversight of the Australian Defence intelligence agencies work. Ms Chayer also briefed the Inspector-General on her role and oversight responsibilities, which includes reporting on Defence Intelligence oversight to the Canadian National Security and Intelligence Committee of Parliamentarians.

In January 2020, an IGIS officer travelled to Wellington to meet New Zealand's acting Inspector-General of Intelligence and Security and her office. The purpose of the visit was to establish working relationships and make preparations for a three-month exchange of officers between the Canberra and Wellington IGIS offices. Discussions covered general office structure and methodologies, proposed work programs for the exchange, and other logistical arrangements. The IGIS officer also conducted an outreach session to relevant Australian personnel based in Wellington. Because of travel restrictions during the COVID-19 pandemic, the exchange program has not taken place during the reporting period.

## OBJECTIVE 6 – HIGH-PERFORMING WORKFORCE

### OVERVIEW

The Office maintains a strategic human resource management plan to ensure it recruits, develops and retains a workforce that effectively supports the Inspector-General in current activities as well as preparing for the anticipated expansion of jurisdiction. In striving to meet its recruitment target, the Office initiated seven recruitment rounds in 2019–20. One of those rounds commenced in late June 2020 and will be completed in 2020–21. From the completed rounds a number of candidates are undergoing relevant pre-employment suitability and security checks. The Office welcomed seven new officers during the reporting period.

In 2019–20, the Office continued its program of internal professional development in job-specific skills and knowledge including recent changes to legislation, complaints handling and security awareness. There were continued opportunities for IGIS officers to attend training courses and seminars relevant to their role as well as special guest presenters at internal training sessions. Also relevant to professional development is the IGIS Enterprise Agreement 2016–2019 which provides a study assistance scheme for employees who pursue studies relevant to the work of the Office.

Eight officers (24%) utilised formal flexible working arrangements in 2019–20. In addition, other officers utilised temporary or adhoc flexible working arrangements with the agreement of their supervisor. The Office adopted work from home arrangements during COVID-19 restrictions in Canberra and in some instances has continued to utilise these arrangements for officers in the high risk category and to provide greater flexibility to officers.

The Office conducts regular staff surveys to seek feedback on the Office's performance management and training arrangements. In 2019–20, the Office conducted two staff surveys, one on the management of COVID-19 arrangements and the other a productivity pulse survey. The surveys covered matters relevant to communication, workplace flexibility, safety management and support to employees, and professional development.



## STAFF PLACEMENTS

During 2019–2020, this Office has undertaken immersive development placements with the following Commonwealth Government agencies: ACLEI, ACIC, AFP, AUSTRAC, and the OCO. The arrangements for these placements were agreed in an MOU with each host agency, and further tailored to each individual placement. Placements have primarily been undertaken by newly recruited staff who are in the process of obtaining the security clearance for IGIS roles.

As mentioned earlier, these placements are designed to improve the expertise of this Office ahead of the anticipated expansion of the Inspector-General's jurisdiction. They also enable the Office to enhance its understanding of the host agencies' internal policies, procedures and organisational structures. The placements have likewise provided host agencies with an understanding of the organisational structure of this Office and its approach to oversight.

Placements in the ACIC, AFP and AUSTRAC have also improved our understanding of the intelligence functions of those agencies, and developed the skills and capabilities of IGIS officers in relation to those functions. The placement of IGIS officers with other oversight bodies (ACLEI and OCO) has assisted this Office in its work to prepare for the deconfliction of oversight when the expanded jurisdiction commences.

## **SECTION THREE**

### MANAGEMENT AND ACCOUNTABILITY



# CORPORATE GOVERNANCE

## ORGANISATIONAL STRUCTURE

Senior positions occupied during 2019–20 were as follows:

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

The Honourable Margaret Stone AO FAAL, appointed on 24 August 2015 and concluded on 23 August 2020.

### **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 originally appointed as the SES Band 1 deputy under the previous organisational structure in January 2012. Mr Blight was Acting Inspector-General on some occasions during the reporting period.

### **Assistant Inspectors-General of Intelligence and Security (SES Band 1)**

Mr Stephen McFarlane, appointed 8 February 2018; and Ms Bronwyn Notzon-Glenn, appointed 28 February 2019.

## SENIOR MANAGEMENT COMMITTEES

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

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

The Senior Officers' Meeting is held weekly and comprises of the Inspector-General, Deputy Inspector-General, the two 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 OPERATIONAL PLANNING

The Office's corporate and operational planning processes are straightforward, reflecting the small size and specialist function of the Office.

The Office addresses these matters through:

- an annual forward planning process to set strategic priorities and a mid-cycle review
- weekly meetings between the Inspector-General and senior IGIS officers to review and document operational priorities

- monthly meetings between the Inspector-General and all IGIS officers during which current operational matters, internal guidelines, and procedures and governance issues 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).

## PROTECTIVE SECURITY

The Australian Government's Protective Security Policy Framework (PSPF) provides a structure for Australian Government agencies to manage security risks proportionately and effectively, and provides the necessary protection for the government's people, information and assets.

The governance arrangements and core policies in the PSPF describes the higher level protective security outcomes and identifies mandatory compliance requirements which IGIS must meet.

How agencies assess their compliance with PSPF requirements has changed from compliance statements against 36 mandatory requirements, to a maturity model. In the last PSPF reporting period the Office recorded a maturity assessment of Embedded, which means:

*All PSPF core and supporting requirements are implemented, effectively integrated and exceeding security outcomes. Entity's implementation of better-practice guidance drives high performance. The entity's security maturity provides comprehensive protection of the entity's people, information and assets.*

Throughout the reporting year the Office continued to participate in whole of government security management forums and cross-agency security management activities.

## INTERNAL AUDIT AND RISK MANAGEMENT

IGIS has an internal risk management framework which establishes the IGIS Audit Committee, provides risk assessments, risk tolerance and acceptance thresholds, and includes business continuity plans.

In February 2020, the Office reviewed its business continuity plan to respond to the COVID-19 global pandemic and in March 2020 implemented a specific pandemic emergency management plan. This plan is scalable and adaptable to a broad range of pandemic and other emergency situations.

In late 2019–20, two internal audits were initiated; one relates to assurance concerning the agency's wage compliance and the other relates to administration of employee leave liabilities.

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>. Mr Trevor Kennedy (Attorney-General's Department) was the Chair of the Committee until 22 July 2019; no meeting was held with Mr Kennedy as Chair during the reporting period. During 2019–20, the IGIS Audit Committee membership comprised of:

MEMBER NAME	QUALIFICATIONS, KNOWLEDGE, SKILLS OR EXPERIENCE	NUMBER OF MEETINGS ATTENDED/ TOTAL NUMBER OF MEETINGS	TOTAL ANNUAL REMUNERATION
Ms Sarah Vandenbroek (Chair from 23 July 2019)	Ms Vandenbroek holds a Bachelor of Information Management, a Post-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 currently the First Assistant Secretary for the Territories Division in the Department of Infrastructure, Transport, Regional Development and Communications.	3/3	\$0
Ms Lynda Waugh	Ms Waugh holds a Bachelor of Arts, a Post-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.	2/3	\$0
Mr Jake Blight	Mr Blight holds a BA/LLB and Graduate Diploma in Legal Practice from ANU and is a graduate of the Australian Institute of Company Directors course. He has been on the IGIS Audit Committee for seven years, as well as having been on the audit committee for two other Commonwealth agencies. Mr Blight is the only internal member of the IGIS Audit Committee and brings a deep knowledge of IGIS operations, having been the Deputy Inspector-General for eight years.	3/3	\$0

The Inspector-General may attend the meetings as an observer.



The Audit Committee meets on a periodic basis to consider matters including:

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

The Committee reviews the Risk Management Plan annually based on its assessment of the office risk performance over the period. The Risk Management Plan includes controls designed to mitigate risks across the following categories:

- personnel related
- accidental or intentional loss of information
- segregation of duties
- failure or compromise of information technology systems
- physical security of the office and facilities
- corporate liability
- fraud prevention, detection and management
- corporate compliance requirements.

Through its various mitigation strategies, the residual risk accepted by the Office is maintained in the low-medium levels in each of the categories.

## ETHICAL STANDARDS AND FRAUD CONTROL

During 2019–20, 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:

- modelling of appropriate behaviours by the agency's Senior Executive
- implementation of organisational suitability assessments
- a requirement that all IGIS officers maintain a high level security clearance
- annual declaration of known interests by the Senior Executive 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.

During the reporting year there were no detected or alleged internal cases of fraud or breaches of the APS Code of Conduct. There was one detected instance of external fraudulent activity involving an agency credit card. The incident was identified through the agency's controls. The matter was pursued and resolved using financial institution processes and all unauthorised funds were recovered by the financial institution.

The Office has established and maintains appropriate systems of risk oversight, management and internal controls in accordance with s 16 of the PGPA Act and the Commonwealth Risk Management Policy.

The Risk Management Plan includes controls designed to mitigate risks including: personnel related risks; accidental or intentional loss of information; segregation of duties; failure or compromise of information technology systems; physical security of the office and facilities; fraud prevention, detection and management; and corporate compliance requirements.

Regular monitoring of risks is undertaken and considered by the management team and reported to the Audit Committee.

## EXECUTIVE REMUNERATION DISCLOSURES

The Inspector-General is a statutory office holder. In addition, the Office has three SES positions: one SES Band 2 position and two 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 s 24(1) determinations and are based broadly on SES remuneration within the Attorney-General's Department. Each s 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

Section 35(2AA) of the IGIS Act requires the annual report to comment on the employment under s 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. No person was employed under that provision during 2019–20.

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

There were no significant issues relating to non-compliance with the finance law during 2019–20 that would be reportable to the responsible Minister under paragraph 19(1)(e) of the PGPA Act.



## EXTERNAL SCRUTINY

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

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 and is currently implementing.

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 the reporting period, 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.

In April 2020, the Fair Work Commission approved the Office of the Inspector-General of Intelligence and Security Enterprise Agreement 2020–2023.

### CAPABILITY REVIEWS

No capability reviews of the Office were released during 2019–20.



# MANAGEMENT OF HUMAN RESOURCES

## ORGANISATIONAL PROFILE

At 30 June 2020, the Office had 33 ongoing APS employees located in the Australian Capital Territory. The Inspector-General is a statutory officer and therefore not an employee. Five APS employees worked part-time. No APS employee was employed on a non-ongoing basis in 2019–20 or 2018–19.

At 30 June 2019, the Office had 32 ongoing APS employees located in the Australian Capital Territory (not including the Inspector-General). Four APS employees worked part-time.

No employees identified as Indigenous in 2019–20 or 2018–19.

At the end of 2019–20, five APS employees had individual flexibility agreements for part-time work, under the Office of the IGIS Enterprise Agreement 2016–2019 and continued under the Office of the IGIS Enterprise Agreement 2020–2023.

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

**Figure 3.1: Organisational Profile as at 30 June 2020 (by employment level and status)**

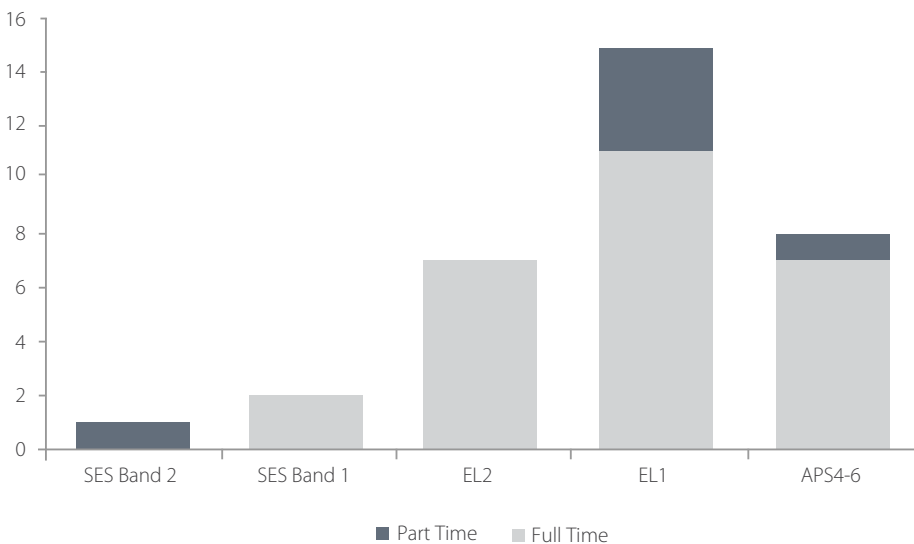
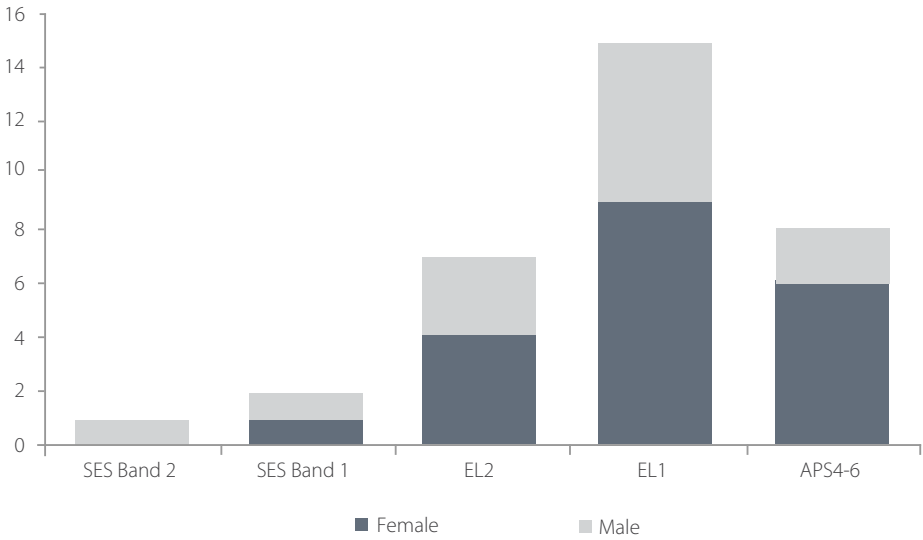


Figure 3.2: Gender Balance as at 30 June 2020 (by employment level and status)



## EMPLOYMENT FRAMEWORKS

All IGIS officers are employed under the *Public Service Act 1999*. From 6 February 2017 to 5 May 2020, all non-SES officers' salaries and conditions were made under the Office of the IGIS Enterprise Agreement 2016–2019 and since 6 May 2020 under the Office of the IGIS Enterprise Agreement 2020–2023. Three SES officers are presently employed in accordance with individual determinations under s 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 \$1,159.

## MANAGING AND DEVELOPING EMPLOYEES

Objective 6 of the IGIS Corporate Plan 2019–20 relates to managing and developing IGIS officers to achieve IGIS outcomes. An assessment of the effectiveness of these measures is in the Annual Performance Statement.

### PERFORMANCE PAY

The Office does not have a performance pay scheme.

## ASSET MANAGEMENT

Management of the Office's assets is 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 and reported in the financial statements. The Office's fixed assets include office fit outs, purchased software and leasehold improvements.

## PURCHASING AND PROCUREMENT

### PURCHASING

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, [www.finance.gov.au/procurement](http://www.finance.gov.au/procurement).

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

All procurement and purchasing activities conducted by the Office were in accordance with the Commonwealth Procurement Rules.

### CONSULTANTS

During 2019–20, four new consultancy contracts were entered into, involving total actual expenditure of \$65,700 (GST exclusive). In addition, two ongoing consultancy contracts were active during the period, involving total actual expenditure of \$58,252.29 (GST exclusive).

The Office maintains internal policies and procedures which require selection and engagement of all consultants to be conducted in accordance with the Commonwealth Procurement Rules. The main purpose for which consultants were engaged in 2019–20 was to obtain specialist expertise not available within the Office due to its small size.

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

## ANAO ACCESS CLAUSES

No contracts for greater than \$100,000 were entered into during the reporting period that did not provide for the Auditor-General to have access to the contractor's premises.

## EXEMPT CONTRACTS

No contracts were entered into during the reporting period that have been exempt from publishing on AusTender.

## 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 Council of Australian Governments. 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

Entities 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 FOI Act and as such the IPS does not apply.

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





## PART 4.1

### FINANCIAL SUMMARY

#### SUMMARY OF IGIS FINANCIAL PERFORMANCE AND RESOURCES FOR OUTCOMES (PGPA ACT)

The Office received an unqualified audit report from the Australian National Audit Office for its 2019–20 financial statements. A summary of our financial performance follows.

The Office operated within available resources in 2019–20 and ended the year with a surplus of \$4,866,087. The summary of financial performance is based on the original budget figures as published in the Portfolio Budget Statements 2019–20.

The increase in appropriation funding levels in 2019–20 reflected the Office's planned growth from the previously budgeted 42 to 55 staff during the year. Other Income remained constant from the previous year.

In relation to expenditure, the most significant variance against original budget figures related to employee expenses which were \$4,341,752 underspent due largely to recruitment on boarding delays associated with the lengthy security clearance process together with staff turnover. As a result security clearance assessment fees were also significantly below budget. Finally, depreciation expenses were significantly below budget mainly due to delays in the deployment of ICT systems and completion of intangible assets. These delays were partly attributable to the impact of the COVID-19 pandemic on priorities and resourcing.

Total equity increased from \$21,821,168 in 2018–19 to \$29,170,255. Movements in equity included a \$4,866,087 increase in retained surplus. Contributed Equity also increased from \$12,371,167 in 2018–19 to \$14,854,167 with capital funding totalling \$2,483,000 in the current year.

The following tables show:

Figure 4.1 – Entity Resource Statement and Resource for Outcomes 2019–20

Figure 4.2 – Expenses and Resources for Outcome 1.

IGIS has one outcome and one program.

Figure 4.1: Entity resource statement and resources for outcomes 2019–20

	ACTUAL AVAILABLE APPROPRIATION FOR 2019–20 \$'000 (A)	PAYMENTS MADE 2019–20 \$'000 (B)	BALANCE REMAINING 2019–20 \$'000 (A) – (B)
<b>Ordinary Annual Services</b>			
<b>Departmental Appropriation</b>			
Prior year departmental appropriation	17,940	7,288	10,652
Departmental appropriation	14,839	-	14,839
S74 Relevant Agency Receipts	350	-	350
<b>Total</b>	<b>33,129</b>	<b>7,288</b>	<b>25,841</b>
<b>Administered expenses</b>	-	-	-
<b>Total</b>	-	-	-
<b>Total ordinary annual services A</b>	<b>33,129</b>	<b>7,288</b>	<b>25,841</b>
<b>Other services</b>			
Departmental non-operating	-	-	-
<b>Total</b>	-	-	-
<b>Total other services B</b>	-	-	-
<b>Total available annual appropriations</b>	<b>33,129</b>	<b>7,288</b>	<b>25,841</b>
<b>Special appropriations</b>	-	-	-
<b>Total special appropriations C</b>	-	-	-
<b>Special accounts</b>	-	-	-
<b>Total special accounts D</b>	-	-	-
<b>Total resourcing A + B + C + D</b>	<b>33,129</b>	<b>7,288</b>	<b>25,841</b>
Less appropriations drawn from annual or special appropriations above and credited to special accounts and/or payments to corporate entities through annual appropriations	-	-	-
<b>Total net resourcing and payments for agency</b>	<b>33,129</b>	<b>7,288</b>	<b>25,841</b>

Figure 4.2: Expenses for Outcome 1

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	BUDGET 2019–20 \$'000	ACTUAL EXPENSES 2019–20 \$'000	VARIATION 2019–20 \$'000
	(A)	(B)	(A)-(B)
<b>Program 1.1: Office of the Inspector-General of Intelligence and Security</b>			
Departmental expenses			
Departmental appropriation <sup>1</sup>	12,356	12,356	-
Special appropriations	-	-	-
Special Accounts	-	-	-
Expenses not requiring appropriation in the Budget year	2,353	(4,796)	7,149
<b>Total for Program 1.1</b>	<b>14,709</b>	<b>7,560</b>	<b>7,149</b>
<b>Outcome 1 Totals by appropriation type</b>			
Departmental expenses			
Departmental appropriation <sup>1</sup>	12,356	12,356	-
Special appropriations	-	-	-
Special Accounts	-	-	-
Expenses not requiring appropriation in the Budget year	2,353	(4,796)	7,149
<b>Total expenses for Outcome 1</b>	<b>14,709</b>	<b>7,560</b>	<b>7,149</b>
	<b>Budget 2019–20</b>	<b>Actual 2019–20</b>	
<b>Average Staffing Level (number)</b>	55	32	23

<sup>1</sup> Departmental appropriation combines ordinary annual services (Appropriation Act Nos 1, 3 and 5) and retained revenue receipts under section 74 of the *Public Governance, Performance and Accountability Act 2013*.

## TRENDS IN FINANCE

Significant changes to the finances of the Office during 2019–20 included:

- A \$2,714,000 increase in Revenue from Government.
- A \$562,115 increase in employee expenses arising largely due to recruitment activity associated with the expansion of the Office.
- A \$188,246 decrease in supplier expenses. This decrease partly reflects the higher than usual expenditure in the previous year associated with the relocation of the Office and associated construction expenditure. The COVID-19 pandemic also impacted on expense items such as travel. Increases in expenditure included \$252,184 in ICT expenses, \$44,831 in legal expenses and \$30,045 increase in staff training expenses. These were offset by decreases including \$343,926 in consultancy expenses, \$48,973 in minor equipment purchases, \$18,675 in travel expenses and \$26,304 associated with staff accommodation placements which ceased during the year.
- A \$624,998 increase in depreciation expenses representing the full year expense related to assets capitalised during the final two quarters of the last financial year.

**Figure 4.3: Trends in finance**

		2019–20 OUTCOME 1 \$	2018–19 OUTCOME 1 \$	CHANGE FROM PREVIOUS YEAR
Revenue from Government		12,356,000	9,642,000	+29%
Other Income		70,774	72,470	-2%
<b>TOTAL INCOME</b>		<b>12,426,774</b>	<b>9,714,470</b>	
Employee expenses		5,006,248	4,444,133	+13%
Supplier expenses		1,631,263	1,819,509	-10%
Other expenses		923,176	297,990	+310%
<b>TOTAL EXPENSES</b>		<b>7,560,687</b>	<b>6,561,632</b>	
<b>OPERATING RESULT</b>		<b>4,866,087</b>	<b>3,152,838</b>	
Financial assets	A	26,093,209	18,437,104	+41%
Non-financial assets	B	5,070,941	5,738,199	-12%
Liabilities	C	1,993,895	2,354,135	-15%
<b>NET ASSETS = A + B - C</b>		<b>29,170,255</b>	<b>21,821,168</b>	

## 4.2

### FINANCIAL STATEMENTS



## INDEPENDENT AUDITOR'S REPORT

### To the Attorney-General

#### Opinion

In my opinion, the financial statements of the Office of the Inspector-General of Intelligence and Security ('the Entity') for the year ended 30 June 2020:

- (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 2020 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 2020 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.

#### 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 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.

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

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

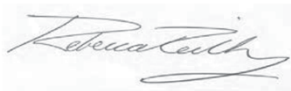
My objective is to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes my opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that 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  
23 September 2020



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

In my opinion, the attached financial statements for the year ended 30 June 2020 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.



Jake Blight  
Acting Inspector-General of  
Intelligence and Security

23 September 2020

**OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY**  
**STATEMENT OF COMPREHENSIVE INCOME**  
*for the year ended 30 June 2020*

	Notes	2020 \$	2019 \$	Original Budget \$
<b>NET COST OF SERVICES</b>				
<b>Expenses</b>				
Employee benefits	2A	5 006 248	4 444 133	9 348 000
Suppliers	2B	1 631 263	1 819 509	3 035 000
Depreciation	5	922 988	297 990	2 326 000
Finance costs		188	-	-
<b>Total expenses</b>		<u>7 560 687</u>	<u>6 561 632</u>	<u>14 709 000</u>
<b>Own-Source Income</b>				
<b>Own-source revenue</b>				
Revenue from contracts with customers	3A	31 266	19 155	-
Other revenue	3B	39 508	53 315	27 000
<b>Total own-source income</b>		<u>70 774</u>	<u>72 470</u>	<u>27 000</u>
<b>Net cost of services</b>		<u>7 489 913</u>	<u>6 489 162</u>	<u>14 682 000</u>
Revenue from Government		<u>12 356 000</u>	<u>9 642 000</u>	<u>12 356 000</u>
<b>Surplus /(deficit) on continuing operations</b>		<u>4 866 087</u>	<u>3 152 838</u>	<u>(2 326 000)</u>
<b>OTHER COMPREHENSIVE INCOME</b>				
<b>Items not subject to subsequent reclassification to net cost of services</b>				
Changes in asset revaluation surplus		-	-	-
<b>Total comprehensive income/(loss)</b>		<u>4 866 087</u>	<u>3 152 838</u>	<u>(2 326 000)</u>

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

**OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY**  
**STATEMENT OF FINANCIAL POSITION**  
*as at 30 June 2020*

	Notes	2020 \$	2019 \$	Original Budget \$
<b>ASSETS</b>				
<b>Financial Assets</b>				
Cash and cash equivalents		221 012	306 265	200 000
Trade and other receivables	4	25 872 197	18 130 839	8 788 000
<b>Total financial assets</b>		<u>26 093 209</u>	<u>18 437 104</u>	<u>8 988 000</u>
<b>Non-Financial Assets<sup>1</sup></b>				
Property, plant and equipment	5	5 054 636	5 646 110	10 347 000
Other non-financial assets	6	16 305	92 089	-
<b>Total non-financial assets</b>		<u>5 070 941</u>	<u>5 738 199</u>	<u>10 347 000</u>
<b>Total Assets</b>		<u>31 164 150</u>	<u>24 175 303</u>	<u>19 335 000</u>
<b>LIABILITIES</b>				
<b>Payables</b>				
Suppliers	7A	273 695	783 065	100 000
Other payables	7B	105 991	41 158	61 000
<b>Total payables</b>		<u>379 686</u>	<u>824 223</u>	<u>161 000</u>
<b>Interest Bearing Liabilities</b>				
Leases	8	15 832	-	-
<b>Total interest bearing liabilities</b>		<u>15 832</u>	<u>-</u>	<u>-</u>
<b>Provisions</b>				
Employee provisions	9	1 598 377	1 529 912	2 058 000
<b>Total provisions</b>		<u>1 598 377</u>	<u>1 529 912</u>	<u>2 058 000</u>
<b>Total Liabilities</b>		<u>1 993 895</u>	<u>2 354 135</u>	<u>2 219 000</u>
<b>Net Assets</b>		<u>29 170 255</u>	<u>21 821 168</u>	<u>17 116 000</u>
<b>EQUITY</b>				
Contributed equity		14 854 167	12 371 167	14 868 000
Reserves		21 623	21 623	22 000
Retained surplus		14 294 465	9 428 378	2 226 000
<b>Total Equity</b>		<u>29 170 255</u>	<u>21 821 168</u>	<u>17 116 000</u>

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

- Right-of-use assets are included in Property, plant and equipment.

**OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY**  
**STATEMENT OF CHANGES IN EQUITY**  
*for the period 30 June 2020*

	2020 \$	2019 \$	Original Budget \$
<b>CONTRIBUTED EQUITY</b>			
Opening balance as at 1 July	12 371 167	12 109 283	12 385 000
<b>Transactions with Owners</b>			
Contributions by Owners			
Return of Equity	-	(13 116)	
Departmental Capital Budget	2 483 000	275 000	2 483 000
<b>Total Transactions with Owners</b>	2 483 000	261 884	2 483 000
<b>Closing balance as at 30 June</b>	<b>14 854 167</b>	<b>12 371 167</b>	<b>14 868 000</b>
<b>RETAINED EARNINGS</b>			
Opening balance as at 1 July			
Balance carried forward from previous period	9 428 378	6 275 540	4 552 000
<b>Adjusted opening balance</b>	<b>9 428 378</b>	<b>6 275 540</b>	<b>4 552 000</b>
<b>Comprehensive Income</b>			
Surplus/deficit for the period	4 866 087	3 152 838	(2 326 000)
<b>Total comprehensive income</b>	4 866 087	3 152 838	(2 326 000)
<b>Closing balance as at 30 June</b>	<b>14 294 465</b>	<b>9 428 378</b>	<b>2 226 000</b>
<b>ASSET REVALUATION RESERVE</b>			
Opening balance as at 1 July			
Balance carried forward from previous period	21 623	21 623	22 000
<b>Comprehensive Income</b>			
Other Comprehensive Income	-	-	-
<b>Total comprehensive income</b>	-	-	-
<b>Closing balance as at 30 June</b>	<b>21 623</b>	<b>21 623</b>	<b>22 000</b>
<b>TOTAL EQUITY</b>			
Opening balance			
Balance carried forward from previous period	21 821 168	18 406 446	16 959 000
Adjustment for change in accounting policies	-	-	-
<b>Adjusted opening balance</b>	<b>21 821 168</b>	<b>18 406 446</b>	<b>16 959 000</b>
<b>Comprehensive Income</b>			
Surplus/deficit for the period	4 866 087	3 152 838	(2 326 000)
Other comprehensive income	-	-	-
<b>Total comprehensive income</b>	4 866 087	3 152 838	(2 326 000)
<b>Transactions with Owners</b>			
Contributions by Owners			
Return of Equity	-	(13 116)	-
Departmental Capital Budget	2 483 000	275 000	2 483 000
<b>Total Transactions with Owners</b>	2 483 000	261 884	2 483 000
<b>Closing balance as at 30 June</b>	<b>29 170 255</b>	<b>21 821 168</b>	<b>17 116 000</b>

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

#### 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 to contributed equity in that year.

**OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY**  
**CASH FLOW STATEMENT**  
*for the year ended 30 June 2020*

	Notes	2020 \$	2019 \$	Original Budget \$
<b>OPERATING ACTIVITIES</b>				
<b>Cash received</b>				
Appropriations		6 925 682	5 759 654	11 856 000
Net GST received		127 621	585 149	-
Other cash received		367 273	575 026	27 000
<b>Total cash received</b>		<u>7 420 576</u>	<u>6 919 829</u>	<u>11 883 000</u>
<b>Cash used</b>				
Employees		(4 665 766)	(4 130 812)	(8 848 000)
Suppliers		(2 536 690)	(2 172 315)	(3 035 000)
Interest payments on lease liabilities		(188)	-	-
Section 74 receipts transferred to OPA		(350 418)	(510 224)	-
<b>Total cash used</b>		<u>7 553 062</u>	<u>(6 813 351)</u>	<u>(11 883 000)</u>
<b>Net cash from/(used by) operating activities</b>		<u>(132 486)</u>	<u>106 477</u>	<u>-</u>
<b>INVESTING ACTIVITIES</b>				
<b>Cash used</b>				
Purchase of property, plant and equipment		(309 125)	(5 838 030)	(2 481 000)
<b>Total cash used</b>		<u>(309 125)</u>	<u>(5 838 030)</u>	<u>(2 481 000)</u>
<b>Net cash from/(used by) investing activities</b>		<u>(309 125)</u>	<u>(5 838 030)</u>	<u>(2 481 000)</u>
<b>FINANCING ACTIVITIES</b>				
<b>Cash received</b>				
Contributed equity		363 104	5 838 030	2 481 000
<b>Total cash received</b>		<u>363 104</u>	<u>5 838 030</u>	<u>2 481 000</u>
<b>Cash used</b>				
Principal payments of lease liabilities		(6 746)	-	-
<b>Total cash used</b>		<u>(6 746)</u>	<u>-</u>	<u>-</u>
<b>Net cash from financing activities</b>		<u>356 358</u>	<u>5 838 030</u>	<u>2 481 000</u>
<b>Net increase/(decrease) in cash held</b>		<u>(85 253)</u>	<u>106 477</u>	<u>-</u>
Cash and cash equivalents at the beginning of the reporting period		306 265	199 788	200 000
<b>Cash and cash equivalents at the end of the reporting period</b>		<u>221 012</u>	<u>306 265</u>	<u>200 000</u>

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

#### Major Budget Variances for 2020

The following table provides high level commentary of major variances between budgeted information for the OIGIS published in the 2019-20 Portfolio Budget Statements (PBS) and the 2019-20 final outcome as presented in accordance with Australian Accounting Standards for the OIGIS.

The Budget is not audited. Major variances are those deemed relevant to an analysis of OIGIS' performance and are not focused merely on numerical differences between the budget and actual amounts. Explanations of major variances are as follows:

Explanation of major variances	Affected line items (and statements)
<p>Employee Benefits – \$4,341,752 below budget. The variance reflects delays in on boarding activities, partly associated with the lengthy security clearance process.</p> <p>Employee Provisions - \$459,623 below budget. The variance reflects the actual versus budgeted staffing numbers.</p>	<p>Impacted:</p> <p>Statement of Comprehensive Income: Employee expenses</p> <p>Statement of Financial Position: Appropriations receivable Employee provisions Other payables Retained surplus</p> <p>Cashflow Statement: Cash used - operating activities</p>
<p>Suppliers expenses – \$1,403,737 below budget. The most significant variances related to security clearance fees and recruitment related consultancy fees. Both expenditure items were lower due to recruitment delays. Other variances include underspends in expenses driven by the number and scope of inquiry work, including legal and travel expenses. The COVID-19 pandemic also impacted on expense items including staff training and overseas travel.</p> <p>Suppliers payable - \$173,695 above budget. The variance represents in part a timing difference with property related outgoings included as accrued expenses. The variance is also partly due to staff leave liability transfers for departed staff which were not included in the budget.</p>	<p>Impacted:</p> <p>Statement of Comprehensive Income: Supplier expenses</p> <p>Statement of Financial Position: Appropriation receivable Suppliers payables Employee provisions Retained surplus</p> <p>Cashflow Statement: Cash used - operating activities</p>
<p>Property, Plant and Equipment – capital expenditure was approximately \$5,292,364 below budget due to lower than expected capital works. Part of the variance is the subject of an approved Movement of Funds request.</p>	<p>Impacted:</p> <p>Statement of Comprehensive Income: Depreciation</p> <p>Statement of Financial Position: Property, plant and equipment Appropriations receivable</p> <p>Cashflow Statement: Cash used - investing activities</p>



### 1.1 Basis of Preparation of the Financial Statements

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:

- *Public Governance, Performance and Accountability (Financial Reporting) Rule 2015* (FRR); and
- 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 and values are rounded to the nearest dollar.

### 1.2 Significant Accounting Judgments and Estimates

In the process of applying the accounting policies listed in this note, OIGIS has made judgments in relation to leave provisions that have a significant impact on the amounts recorded in the financial statements. Leave provisions involve assumptions on the likely tenure of existing staff, future salary movements and future discount rates.

The uncertainty associated with the existing COVID-19 pandemic may impact on the reliability of these judgements. The potential impact is currently unquantifiable.

### 1.3 New Australian Accounting Standards

The following new standards were applicable for the first time in the current reporting period:

#### **Application of AASB 15 Revenue from Contracts with Customers/AASB 1058 Income of Not-for-Profit Entities**

OIGIS adopted AASB 15 and AASB 1058 using the modified retrospective approach, under which the cumulative effect of initial application is recognised in retained earnings at 1 July 2019. Accordingly, the comparative information presented for 2019 is not restated, that is, it is presented as previously reported under the various applicable AASBs and related interpretations.

Under the new income recognition model OIGIS shall first determine whether an enforceable agreement exists and whether the promises to transfer goods or services to the customer are ‘sufficiently specific’. If an enforceable agreement exists and the promises are ‘sufficiently specific’ (to a transaction or part of a transaction), OIGIS applies the general AASB 15 principles to determine the appropriate revenue recognition. If these criteria are not met, OIGIS shall consider whether AASB 1058 applies.

In relation to AASB 15, OIGIS elected to apply the new standard to all new and uncompleted contracts from the date of initial application. OIGIS is required to aggregate the effect of all of the contract modifications that occur before the date of initial application.

In terms of AASB 1058, OIGIS is required to recognise volunteer services at fair value if those services would have been purchased if not provided voluntarily, and the fair value of those services can be measured reliably.

#### **Impact on transition**

There was no material impact upon transition.



#### Application of AASB 16 Leases

OIGIS adopted AASB 16 using the modified retrospective approach, under which the cumulative effect of initial application is recognised in retained earnings at 1 July 2019. Accordingly, the comparative information presented for 2019 is not restated, that is, it is presented as previously reported under AASB 117 and related interpretations.

As a lessee, OIGIS previously classified leases as operating or finance leases based on its assessment of whether the lease transferred substantially all of the risks and rewards of ownership. Under AASB 16, OIGIS recognises right-of-use assets and lease liabilities for all of its current leases.

On adoption of AASB 16, OIGIS recognised a right-of-use asset and lease liability in relation to the lease of one motor vehicle, which had previously been classified as an operating lease.

The lease liabilities were measured at the present value of the remaining lease payments, discounted using OIGIS's incremental borrowing rate as at 1 July 2019.

The right-of-use asset was measured as the carrying value that would have resulted from AASB 16 being applied from the commencement date of the lease.

Impact on transition

On transition to AASB 16, OIGIS recognised a right-of-use asset and lease liability recognising the difference to retained earnings. The impact on transition is summarised below:

	1 July 2019
	\$
Right-of-use asset – property, plant and equipment	22 390
Lease liabilities	22 390

The following table reconciles the minimum lease commitments disclosed in OIGIS's 30 June 2019 annual financial statements to the amount of lease liabilities recognised on 1 July 2019:

	1 July 2019
	\$
Minimum operating lease commitment at 30 June 2019	20 698
Plus: adjustments to lease commitments and inclusion of applicable GST	2 070
Less: short-term leases not recognised under AASB 16	-
Less: low value leases not recognised under AASB 16	-
Plus: effect of extension options reasonable certain to be exercised	-
<b>Undiscounted lease payments</b>	<b>22 768</b>
Less: effect of discounting using the incremental borrowing rate as at the date of initial application	(378)
<b>Lease liabilities recognised at 1 July 2019</b>	<b>22 390</b>

**1.4 Taxation**

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

Revenues, expenses and assets are recognised net of GST except:

- where the amount of GST incurred is not recoverable from the Australian Taxation Office; and
- for receivables and payables.

**1.5 Revenue from Government**

Amounts appropriated for departmental appropriations for the year (adjusted for any formal additions and reductions) are recognised as Revenue from Government when OIGIS gains control of the appropriation. Appropriations receivable are recognised at their nominal amounts.

**1.6 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.

## Note 2 – Expenses

	2020 \$	2019 \$
<u>Note 2A – Employee Benefits</u>		
Wages and salaries	3 873 085	3 354 324
Superannuation:		
Defined benefit plans	275 486	239 787
Defined contribution plans	409 763	329 297
Leave and other entitlements	447 914	520 725
<b>Total employee benefits</b>	<b>5 006 248</b>	<b>4 444 133</b>

## Accounting Policy

Accounting policies for employee related expenses are contained in Note 9.

	2020 \$	2019 \$
<u>Note 2B – Suppliers</u>		
<b>Goods and services supplied or rendered</b>		
Consultants	123 952	467 878
ICT support	395 186	143 002
Legal expenses	48 996	4 165
Printing publications	17 468	13 352
Resources received free of charge	39 508	39 545
Stationery	7 777	32 183
Training	50 086	20 041
Travel	83 945	102 620
Security Vetting Expenses	95 011	76 587
HR Support Services	77 300	88 045
Minor Assets	9 350	58 323
Scribe Services	16 011	24 522
Occupancy Expenses	573 679	587 801
Accommodation - Placements	24 073	50 377
Other	54 912	90 452
<b>Total goods and services supplied or rendered</b>	<b>1 617 254</b>	<b>1 798 893</b>
<b>Other suppliers</b>		
Motor Vehicle Lease – minimum lease payments <sup>1</sup>	-	8 555
Variable lease payments	-	-
Workers compensation premiums	14 009	12 061
<b>Total other supplier</b>	<b>14 009</b>	<b>20 616</b>
<b>Total supplier</b>	<b>1 631 263</b>	<b>1 819 509</b>

1 The above lease disclosures should be read in conjunction with accompanying notes 1.3.

**Note 3 – Own-Source Revenue**

	2020 \$	2019 \$
<u>Note 3A – Revenue from Contracts with Customers</u>		
Rendering of services – provision of staff car parking facilities	31 266	19 155
<b>Total revenue from contract with customers</b>	<u>31 266</u>	<u>19 155</u>
	2020 \$	2019 \$
<u>Note 3B – Other Revenue</u>		
Other	-	13 770
Resources Received Free of Charge:		
Australian National Audit Office	35 000	35 000
Australian Signals Directorate	4 508	4 545
<b>Total other own-source revenue</b>	<u>39 508</u>	<u>53 315</u>

**Accounting Policy****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.

**Resources Received Free of Charge**

Resources received free of charge are recognised as revenue when, and only when, a fair value can be reliably determined and the services would have been purchased if they had not been donated. Use of those resources is recognised as an expense. Resources received free of charge are recorded as either revenue or gains depending on their nature.

The main resources received free of charge in 2019-20 are the provision of audit services (from the ANAO) and the installation and maintenance of the OIGIS owned internal secure computer network (from Australian Signals Directorate).

**Note 4 – Financial Assets**

	2020 \$	2019 \$
<u>Trade and other receivables</u>		
Appropriations receivable	25 840 404	17 939 771
GST receivable from the Australian Taxation Office	15 436	67 739
Other receivables	16 357	123 329
<b>Total trade and other receivables (net)</b>	<u>25 872 197</u>	<u>18 130 839</u>

All receivables are expected to be recovered in less than 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.

#### **Note 5 – Non-Financial Assets**

##### Reconciliation of the Opening and Closing Balances of Property, Plant and Equipment

Item	Property, plant & equipment \$	Leasehold Improvements \$	Intangibles \$	Total \$
<b>As at 1 July 2019</b>				
Work in progress	530 000	-	754 739	1 284 739
Gross book value	1 280 416	3 392 088	-	4 672 504
Accumulated depreciation and impairment	(104 362)	(206 771)	-	(311 133)
<b>Total as at 1 July 2019</b>	<b>1 706 054</b>	<b>3 185 317</b>	<b>754 739</b>	<b>5 646 110</b>
Additions				
by purchase	46 485	15 260	247 380	309 125
right-of-use assets	22 390	-	-	22 390
Disposals	-	-	-	-
Depreciation expense	(235 197)	(681 158)	-	(916 355)
Depreciation on right-of-use assets	(6 634)	-	-	(6 634)
<b>Total as at 30 June 2020</b>	<b>1 533 098</b>	<b>2 519 419</b>	<b>1 002 119</b>	<b>5 054 636</b>
<b>Total as at 30 June 2020 represented by:</b>				
Work in progress	557 955	-	1 002 119	1 560 074
Gross book value	1 321 335	3 407 348	-	4 728 683
Accumulated depreciation and impairment	(346 193)	(887 929)	-	(1 234 122)
<b>Total as at 30 June 2020</b>	<b>1 533 098</b>	<b>2 519 419</b>	<b>1 002 119</b>	<b>5 054 636</b>
Carrying amount of right-of-use assets	15 756	-	-	15 756

#### 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.

Leased right-of-use 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.

##### Asset Recognition Threshold

Purchases of 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).

### Fair Value Measurement

The fair values of property plant and equipment are determined using either the market selling price or depreciated replacement cost. The valuation of property plant and equipment at 30 June 2020 included \$4,035,307 Level 2 assets (including office equipment and furniture, software and leasehold improvements) and \$1,455 Level 3 assets (including office furniture).

The unobservable inputs (Level 3 fair value hierarchy) used to determine the fair value, include historical actual cost information and costing guides to estimate the current replacement cost. Useful life profiles have been applied to the replacement cost to reflect the expended life of the asset.

### Revaluations

Following initial recognition at cost, property plant and equipment (excluding right-of-use 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 do not differ materially from the assets' fair values as at the reporting date. The regularity of independent valuations depends 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 reverses 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 reverse 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 Materiality Review was undertaken by Jones Lang LaSalle Public Sector Valuations Pty Ltd (JLL) as at 30 June 2020. The outcome of the Materiality Review was an assessment by JLL that the carrying amounts of all property, plant and equipment assets (including assets under construction) were not materially different to the fair value of the assets as reported at 30 June 2020.

All assets were examined for indicators of impairment during the stocktake completed on 30 June 2020. The right-of-use asset included in Property, plant and equipment was also assessed for impairment at the reporting date. No indicators of impairment have been identified.

### Depreciation

Depreciable property plant and equipment assets are written-off to their estimated residual values over their estimated useful lives to OIGIS using, in all cases, the straight-line method of depreciation.

Depreciation rates (useful lives), residual values and methods are reviewed at each reporting date and necessary adjustments are recognised in the current, or current and future reporting periods, as appropriate.

Depreciation rates of depreciable assets are based on useful lives of:

Property – Plant & Equipment 1 – 11 years (2019: 1 – 11 years)  
Leasehold Improvements 5 years (2019: 5 years)

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



### 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

Intangibles comprise internally developed software for internal use. These assets are carried at cost less accumulated amortisation and accumulated impairment losses. Software is amortised on a straight-line basis over its anticipated useful life. The useful lives of OIGIS's software are 3 years. All software assets were assessed for indicators of impairment as at 30 June 2020.

#### **Note 6 – Other Non-Financial Assets**

	2020 \$	2019 \$
Prepayments	16 305	92 089
<b>Total other non-financial assets</b>	<b>16 305</b>	<b>92 089</b>

#### **Note 7 – Payables**

	2020 \$	2019 \$
7A - Suppliers		
Trade creditors and accruals	273 695	783 065
<b>Total suppliers</b>	<b>273 695</b>	<b>783 065</b>

Supplier payables expected to be settled in no more than 12 months.

### Accounting Policy

OIGIS' financial liabilities comprise trade and other payables and are recognised at amortised costs. Liabilities are recognised to the extent that the goods or services have been received (and irrespective of having been invoiced).

	2020 \$	2019 \$
7B - Other Payables		
Salaries and wages	78 797	31 210
Superannuation	10 492	4 874
Other	16 702	5 074
<b>Total other payables</b>	<b>105 991</b>	<b>41 158</b>

Other Payables are expected to be settled in no more than 12 months.

### Accounting Policy

### Superannuation

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

**Note 8 – Interest Bearing Liabilities**

	2020 \$	2019 \$
<u>Leases</u>		
Lease liability – motor vehicle	15 832	-
<b>Total leases</b>	<b>15 832</b>	<b>-</b>

Total cash outflow for leases for the year ended 30 June 2020 was \$7,173.84 (GST inclusive)

**Accounting Policy**

OIGIS has one motor vehicle lease. The lease liability represents the present value of the remaining lease payments, discounted using OIGIS's incremental borrowing rate as at 1 July 2019. OIGIS's incremental borrowing rate is the rate at which a similar borrowing could be obtained from an independent creditor under comparable terms and condition. The weighted-average rate applied was 0.97% which is considered to be the equivalent of the bond yield rate.

**Note 9 – Employee Provisions**

	2020 \$	2019 \$
<u>Employee Provisions</u>		
Leave	1 598 377	1 529 912
<b>Total employee provisions</b>	<b>1 598 377</b>	<b>1 529 912</b>

**Accounting Policy**

Liabilities for 'short-term employee benefits' and termination benefits expected within twelve months of the end of the reporting period are measured at their nominal amounts.

**Leave**

The liability for employee benefits includes provision for annual leave and long service leave. No provision has been made for personal leave as all personal leave is non-vesting and the average personal leave taken in future years by employees of OIGIS is estimated to be less than the annual entitlement for personal leave.

The leave liabilities are calculated on the basis of employees' remuneration at the estimated salary rates that will be applied at the time the leave is taken, including OIGIS's employer superannuation contribution rates to the extent that the leave is likely to be taken during service rather than paid out on termination.

The liability for long service leave has been determined by using the Short Hand Method per the Financial Reporting Rules. The estimate of the present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

**Superannuation**

Staff of OIGIS are members of the Commonwealth Superannuation Scheme (CSS), the Public Sector Superannuation Scheme (PSS), the PSS accumulation plan (PSSap) and other industry super funds held outside the Australian Government.

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



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

The PSSap is a defined contribution scheme.

#### Note 10 – 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 Chief Executive, Deputy Chief Executive and Assistant Chief Executives. Key management personnel remuneration is reported in the table below:

	2020 \$	2019 \$
<b>Short-term employee benefits:</b>		
Salary	1 047 977	901 374
Other Benefits & Allowances	125 729	110 734
<b>Total short-term employee benefits</b>	<u>1 173 706</u>	<u>1 012 108</u>
<b>Post-employment benefits:</b>		
Superannuation	164 114	125 197
<b>Total post-employment benefits</b>	<u>164 114</u>	<u>125 197</u>
<b>Other long-term employee benefits:</b>		
Long Service Leave	20 662	15 805
<b>Total other long-term employee benefits</b>	<u>20 662</u>	<u>15 805</u>
<b>Total senior executive remuneration expenses</b>	<u>1 358 482</u>	<u>1 153 110</u>

#### Accounting Policy

This note is prepared on an accrual basis. The total number of key management personnel that are included in the above table are 4 individuals (2019: 4 individuals). The 2019 figure includes one of the officers for part of the year.

#### Note 11 – Related Party Disclosures

##### Related Party Relationships

OIGIS is an Australian Government controlled entity. Related parties to OIGIS are:

- Key Management Personnel, their close family members and entities controlled or jointly controlled by either;
- the members of the Executive – key management personnel for the whole of government financial statements; and
- other Australian Government entities.

##### Transactions with Related Parties

Given the breadth of Government activities, related parties may transact with the government sector in the same capacity as ordinary citizens. Such transactions include the payment or refund of taxes, receipt of a Medicare rebate or higher education loans. These transactions have not been separately disclosed in this note.

Giving consideration to relationships with related entities, and transactions entered into during the reporting period by the entity, it has been determined that there are no related party transactions to be separately disclosed.

#### **Note 12 - Contingent Assets and Liabilities**

Contingent liabilities and contingent assets are not recognised in the statement of financial position but are reported in the relevant notes. They may arise from uncertainty as to the existence of a liability or asset or represent an asset or liability in respect of which the amount cannot be reliably measured. Contingent assets are disclosed when settlement is probable but not virtually certain and contingent liabilities are disclosed when settlement is greater than remote.

OIGIS has no contingencies to report at 30 June 2020 (2019: Nil).

#### **Note 13 – Financial Instruments**

	2020 \$	2019 \$
<u>Categories of Financial Instruments</u>		
<b>Financial Assets at amortised costs</b>		
Cash and cash equivalents	221 012	306 265
Trade and other receivables	16 357	123 329
<b>Total financial assets at amortised cost</b>	<u>237 369</u>	<u>429 594</u>
<b>Total financial assets</b>	<u>237 369</u>	<u>429 594</u>
<b>Financial Liabilities measured at amortised cost</b>		
Suppliers	273 695	783 065
<b>Total financial liabilities measured at amortised cost</b>	<u>273 695</u>	<u>783 065</u>
<b>Total financial liabilities</b>	<u>273 695</u>	<u>783 065</u>

The net fair values of the financial assets and liabilities are at their carrying amounts. OIGIS derived no interest income from financial assets in either the current and prior year.

#### Financial Assets

OIGIS classifies its financial assets as measured at amortised cost using the effective interest method. Financial assets are recognised and derecognised upon trade date.

Financial assets are assessed for impairment at the end of each reporting period based on Expected Credit Losses.

Credit terms are net 30 days (2019: 30 days).

#### Financial Liabilities

Financial liabilities are classified as other financial liabilities. Financial liabilities are recognised and derecognised upon 'trade date'.

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 net 30 days.

## Note 14 – Appropriations

### Note 14A – Annual Appropriations ('Recoverable GST exclusive')

	2020 \$	2019 \$
<b>Ordinary Annual Services</b>		
Annual Appropriation	12 356 000	9 642 000
PGPA Act – Section 74 Receipts	350 418	510 223
Annual Departmental Capital Budget <sup>1</sup>	2 483 000	275 000
<b>Total appropriation</b>	<b>15 189 418</b>	<b>10 427 223</b>
Appropriation applied (current and prior years)	7 381 940	11 491 154
<b>Variance<sup>2</sup></b>	<b>7 807 478</b>	<b>(1 063 931)</b>

- 1 Departmental Capital Budgets are appropriated through Appropriation Acts (No 1,3,5). They form part of ordinary annual services, and are not separately identified in the Appropriation Acts.
- 2 Variance between Total Appropriation and Appropriation Applied is due in part to section 74 receipts, underspends related largely to recruitment delays associated with security clearance requirements, the impact of the COVID-19 pandemic on planned activities and delayed capital expenditure.

### Note 14B: Unspent Annual Appropriations ('Recoverable GST exclusive')

	2020 \$	2019 \$
<b>Departmental</b>		
Appropriation Act (No 3) 2017-18	-	2 772 309
Appropriation Act (No 3) 2017-18 – DCB <sup>1</sup>	5 408 865	5 771 969
Appropriation Act (No 1) 2018-19	4 967 120	9 120 492
Appropriation Act (No 1) 2018-19 – DCB	275 000	275 000
Appropriation Act (No 1) 2019-20	7 372 865	-
Supply Act (No 1) 2019-20	5 333 553	-
Appropriation Act (No 1) 2019-20 – DCB	1 448 000	-
Supply Act (No 1) 2019-20 – DCB	1 035 000	-
Cash	221 012	306 265
<b>Total Departmental</b>	<b>26 061 415</b>	<b>18 246 035</b>

- 1 \$3.5 million subject to Administrative Quarantine as at 30 June 2020.

## Note 15 – Aggregate Assets and Liabilities

	2020 \$	2019 \$
<b>Assets expected to be recovered in:</b>		
No more than 12 months	26 106 330	18 523 695
More than 12 months	5 057 820	5 651 608
<b>Total assets</b>	<b>31 164 150</b>	<b>24 175 303</b>
<b>Liabilities expected to be recovered in:</b>		
No more than 12 months	766 798	1 370 142
More than 12 months	1 227 097	983 993
<b>Total liabilities</b>	<b>1 993 895</b>	<b>2 354 135</b>



## **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% - on commencement

2% - 12 months from commencement

2% - 24 months from commencement.

The timing of the initial increase has been affected by the Australian Government announcement on 9 April 2020 that general wage increases in Commonwealth agencies would be paused for six months.

IGIS BAND	APS LEVEL	SALARY RANGE 1 JULY 2019– 5 MAY 2020 (\$)	SALARY RANGE 6 MAY 2020– 30 JUNE 2020 (\$)
IGIS Band 4	EL2	119,442 – 142,153	121,831 – 144,997
IGIS Band 3	EL1	102,620 – 114,398	104,673 – 116,686
IGIS Band 2	APS 6	84,955 – 95,471	86,655 – 97,381
	APS 5	74,442 – 80,751	75,931 – 82,367
	APS 4	66,872 – 72,759	68,210 – 74,215
IGIS Band 1	APS 3	60,143 – 64,768	61,346 – 66,064
	APS 2	52,570 – 58,458	53,622 – 59,628
	APS 1	47,896 – 51,310	48,854 – 52,337

# ANNEXURE 5.2

## KEY MANAGEMENT PERSONNEL

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

NAME	POSITION	TERM AS KMP
Margaret Stone	Inspector-General (CEO)	Full year
Jake Blight	Deputy Inspector-General	Full year
Stephen McFarlane	Assistant Inspector-General	Full year
Bronwyn Notzon-Glenn	Assistant Inspector-General	Full year

In the notes to the financial statements for the period ending 30 June 2020, IGIS disclosed the following KMP expenses:

### Note 10: Key management personnel remuneration for the reporting period

	2020 \$
Short-term benefits:	
Base salary	1,047,977
Bonus	-
Other benefits and allowances	125,729
<b>Total short-term benefits</b>	<b>1,173,706</b>
Superannuation	164,114
<b>Total post-employment benefits</b>	<b>164,144</b>
Long service leave	20,662
<b>Total other long-term benefits</b>	<b>20,662</b>
Termination benefits	-
<b>Total key management personnel remuneration</b>	<b>1,358,482</b>

In accordance with the PGPA Rule, this information now needs to be further disaggregated in the annual report as follows:

Name	Position title	SHORT-TERM BENEFITS			POST-EMPLOYMENT BENEFITS	OTHER LONG-TERM BENEFITS		TERMINATION BENEFITS	TOTAL REMUNERATION
		Base salary	Bonuses	Other benefits and allowances		Superannuation contributions	Long service leave	Other long-term benefits	
Margaret Stone	Inspector-General (CEO)	427,270	-	48,228	34,108	-	-	-	509,606
Jake Blight	Deputy Inspector-General	217,253	-	25,667	40,281	7,264	-	-	290,465
Stephen McFarlane	Assistant Inspector-General	201,150	-	25,917	46,674	6,669	-	-	280,410
Bronwyn Notzon-Glenn	Assistant Inspector-General	202,304	-	25,917	43,051	6,729	-	-	278,001
<b>Total</b>		<b>1,047,977</b>	<b>-</b>	<b>125,729</b>	<b>164,114</b>	<b>20,662</b>	<b>-</b>	<b>-</b>	<b>1,358,482</b>



# 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 WHS Act.

Due to its small size, the Office does not have a separate Workplace Health and Safety Committee. Instead, workplace health and safety matters are addressed at all-staff meetings, the Executive Committee 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 year. 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.

In 2020, all employees who were required to work from home as a result of COVID-19 restrictions completed a work from home safety checklist and assessment. All employees who required additional equipment had this provided to them by the Office.

## 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 the 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	i
<b>17AD(h)</b>	<b>Aids to access</b>			
17AJ(a)	Preliminaries	Table of contents.	Mandatory	ii
17AJ(b)	Annexures	Alphabetical index.	Mandatory	
17AJ(c)	Preliminaries	Glossary of abbreviations and acronyms.	Mandatory	v
17AJ(d)	Annexures	List of requirements.	Mandatory	
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	4
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, 12



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	7, 12
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 3	Period as the accountable authority or member of the accountable authority within the reporting period.	Mandatory	111
17AE(1)(b)	n/a	An outline of the structure of the portfolio of the entity.	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>			
	<i>Annual Performance Statements</i>			
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
17AD(c)(ii)	<i>Report on Financial Performance</i>			
17AF(1)(a)	Section 4	A discussion and analysis of the entity's financial performance.	Mandatory	82-85
17AF(1)(b)	Section 4	A table summarising the total resources and total payments of the entity.	Mandatory	83-84

PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
17AF(2)	Section 4	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.	85
<b>17AD(d) Management and Accountability</b>				
<i>Corporate Governance</i>				
17AG(2)(a)	Section 3	Information on compliance with section 10 (fraud systems).	Mandatory	i
17AG(2)(b)(i)	Preliminaries	A certification by accountable authority that fraud risk assessments and fraud control plans have been prepared.	Mandatory	i
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	i
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	i
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	70-74



PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
17AG(2)(d) – (e)	Section 3	A statement of significant issues reported to Minister under paragraph 19(1)(e) of the Act that relates to non compliance with Finance law and action taken to remedy non compliance.	If applicable, Mandatory	n/a
<i>Audit Committee</i>				
17AG(2A)(a)	Section 3	A direct electronic address of the charter determining the functions of the entity's audit committee.	Mandatory	72
17AG(2A)(b)	Section 3	The name of each member of the entity's audit committee.	Mandatory	72
17AG(2A)(c)	Section 3	The qualifications, knowledge, skills or experience of each member of the entity's audit committee.	Mandatory	72
17AG(2A)(d)	Section 3	Information about the attendance of each member of the entity's audit committee at committee meetings.	Mandatory	72
17AG(2A)(e)	Section 3	The remuneration of each member of the entity's audit committee.	Mandatory	72
<i>External Scrutiny</i>				
17AG(3)	Section 3	Information on the most significant developments in external scrutiny and the entity's response to the scrutiny.	Mandatory	75
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	75
17AG(3)(b)	n/a	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	75
17AG(3)(c)	n/a	Information on any capability reviews on the entity that were released during the period.	If applicable, Mandatory	75

PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
<i>Management of Human Resources</i>				
17AG(4)(a)	Section 2	An assessment of the entity's effectiveness in managing and developing employees to achieve entity objectives.	Mandatory	68, 76-78
17AG(4)(aa)	Section 3	<p>Statistics on the entity's employees on an ongoing and non-ongoing basis, including the following:</p> <p>(a) statistics on full-time employees;</p> <p>(b) statistics on part-time employees;</p> <p>(c) statistics on gender; and</p> <p>(d) statistics on staff location.</p>	Mandatory	76-77
17AG(4)(b)	Section 3	<p>Statistics on the entity's APS employees on an ongoing and non-ongoing basis; including the following:</p> <ul style="list-style-type: none"> <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; and</li> <li>• Statistics on employees who identify as Indigenous.</li> </ul>	Mandatory	76-77
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
17AG(4)(c)(ii)	Annexures	The salary ranges available for APS employees by classification level.	Mandatory	110
17AG(4)(c)(iii)	Section 3	A description of non-salary benefits provided to employees.	Mandatory	78



PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
17AG(4)(d)(i)	n/a	Information on the number of employees at each classification level who received performance pay.	If applicable, Mandatory	n/a
17AG(4)(d)(ii)	n/a	Information on aggregate amounts of performance pay at each classification level.	If applicable, Mandatory	n/a
17AG(4)(d)(iii)	n/a	Information on the average amount of performance payment, and range of such payments, at each classification level.	If applicable, Mandatory	n/a
17AG(4)(d)(iv)	n/a	Information on aggregate amount of performance payments.	If applicable, Mandatory	n/a
<i>Assets Management</i>				
17AG(5)	Section 3	An assessment of effectiveness of assets management where asset management is a significant part of the entity's activities.	Mandatory	78
<i>Purchasing</i>				
17AG(6)	Section 3	An assessment of entity performance against the <i>Commonwealth Procurement Rules</i> .	Mandatory	78-79
<i>Consultants</i>				
17AG(7)(a)	Section 3	A summary statement detailing the number of new contracts engaging consultants entered into during the period; the total actual expenditure on all new consultancy contracts entered into during the period (inclusive of GST); the number of ongoing consultancy contracts that were entered into during a previous reporting period; and the total actual expenditure in the reporting year on the ongoing consultancy contracts (inclusive of GST).	Mandatory	78-79



PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
17AG(7)(b)	Section 3	A statement that <i>"During [reporting period], [specified number] new consultancy contracts were entered into involving total actual expenditure of \$[specified million]. In addition, [specified number] ongoing consultancy contracts were active during the period, involving total actual expenditure of \$[specified million]"</i> .	Mandatory	78-79
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	78-79
17AG(7)(d)	Section 3	A statement that <i>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."</i>	Mandatory	79
<i>Australian National Audit Office Access Clauses</i>				
17AG(8)	n/a	If an entity entered into a contract with a value of more than \$100 000 (inclusive of GST) and the contract did not provide the Auditor General with access to the contractor's premises, the report must include the name of the contractor, purpose and value of the contract, and the reason why a clause allowing access was not included in the contract.	If applicable, Mandatory	n/a



PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
<i>Exempt contracts</i>				
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	79
<i>Small business</i>				
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	78
17AG(10)(b)	Section 3	An outline of the ways in which the procurement practices of the entity support small and medium enterprises.	Mandatory	78
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
<i>Financial Statements</i>				
17AD(e)	Section 4	Inclusion of the annual financial statements in accordance with subsection 43(4) of the Act.	Mandatory	87-108

PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
<i>Executive Remuneration</i>				
17AD(da)	Section 3 and Annexures	Information about executive remuneration in accordance with Subdivision C of Division 3A of Part 2-3 of the Rule.	Mandatory	111-112
<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	113
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	79
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	79
17AH(1)(e)	n/a	Correction of material errors in previous annual report.	Mandatory	n/a
17AH(2)	Annexures	Information required by other legislation.	Mandatory	113

# INDEX

## A

abbreviations, v

accountable authority, 12

Administrative Appeals Tribunal, 8, 21–2

administrative tribunal decisions (external scrutiny), 75

advertising and market research, 113

AGO *see* Australian Geospatial-Intelligence Organisation (AGO)

ANAO *see* Australian National Audit Office

annual performance statement

accountable authority statement, 12

analysis, 19–68

results, 13–18

Objective 1: Assisting Ministers, 13, 19

Objective 2: Assuring Parliament, 13, 19–22

Objective 3: Informing the public, 14, 22–3

Objective 4: Complaints and public interest disclosures, 16, 56–64

Objective 4: Inquiries, 15, 23–6

Objective 4: Inspections, 15, 26–56

Objective 5: Infrastructure and stakeholders, 14, 16, 17, 64–7

Objective 6: High-performing workforce, 17–18, 67–8

*Anti-Money Laundering and Counter Terrorism Financing Act 2006*, 54

*Archives Act 1983*, 8, 21–2

ASD *see* Australian Signals Directorate (ASD)

ASIO *see* Australian Security Intelligence Organisation (ASIO)

ASIS *see* Australian Secret Intelligence Service (ASIS)

asset management, 78

Assistant Inspectors-General, 6, 7

assumed identities, 53–4

Attorney-General, 4, 9

ASIO reporting obligations, 31, 32, 33–4

Guidelines under ASIO Act, 29, 37, 39–40

powers, 30

requests to, 34, 35, 38

submissions to, 41

Audit Committee, 71–4, 113

Auditor-General *see* Australian National Audit Office

*audits, internal*, 71

AUSTRAC *see* Australian Transaction Reports and Analysis Centre (AUSTRAC)

Australian Commission for Law Enforcement Integrity, 3, 65, 68

Australian Criminal Intelligence Commission, 40, 55–6, 64, 68

Australian Cyber Security Centre, 10

Australian Federal Police, 40, 55–6, 64, 68

Australian Geospatial-Intelligence Organisation (AGO), 10

- AUSTRAC information access and use, 54
- Director's approvals and post activity reporting, 51
- inspections of, 50–2
- Ministerial Authorisations, 51
- PJCIS review of administration and expenditure, 21
- Privacy Rules compliance, 51–2
- role and functions, 50

Australian Human Rights Commission, 65

Australian Hydrographic Office, 50, 52

Australian Information Commissioner, 8, 21–2 *see also* Office of the Australian Information Commissioner

Australian National Audit Office, 5

- access clauses in contracts, 79
- audits, 75
- financial statements audit report, 75, 87–8

Australian Privacy Foundation, 23

Australian Secret Intelligence Service (ASIS), 9

- AUSTRAC information access and use, 54
- Compliance Branch, 44
- compliance incident reports, 44
- inspections of, 41–6
- Ministerial Authorisations, 43–4
- ministerial submissions, 43
- PJCIS review of administration and expenditure, 21
- Privacy Rules compliance, 45
- review of operational files, 42
- weapons use and issues, 45–6

Australian Security Intelligence Organisation (ASIO), 9

- analytic tradecraft, 29–30
- Attorney-General's Guidelines, 39–40
- AUSTRAC information access and use, 54
- deletion of data, 34
- failure to record key intelligence, 30
- human source management, 30
- information exchange with other agencies, 40–1



- inquiries relating to, 24, 25
- inspections of, 28–41
- investigative activities, 29
- ministerial submissions, 41
- PJCIS review of administration and expenditure, 21
- questioning and detention warrants, 38
- role and functions, 28
- security assessments, 41
- special intelligence operations, 38
- special powers, 34–6
- taxation information access, 40
- telecommunications interception and data matters, 30–4, 37, 38–9
- temporary exclusion orders, 39
- use of force, 38
- warrants, 30–1

*Australian Security Intelligence Organisation Act 1979*, 9

- breaches of, 35–7

Australian Signals Directorate (ASD), 10

- AUSTRAC information access and use, 54
- inquiries relating to, 24
- inspections of, 46–50
- legislative non-compliance, 49–50
- Ministerial Authorisations, 47
- ministerial submissions, 47–8
- PJCIS review of administration and expenditure, 21
- Privacy Rules compliance, 48
- role and functions, 46
- TIA Act incident reports, 49–50

Australian Transaction Reports and Analysis Centre (AUSTRAC), 54, 55–6, 64, 68

## B

- bilateral engagement, 66–7
- Blight, Jake, 7, 12, 66, 70, 72, 111, 112

## C

- capability reviews, 75
- case management system, 3, 64
- citizenship-related complaints, 57–8
- Civil Society Reference Group, 3, 23

- Commonwealth Indigenous Procurement Policy, 78
- Commonwealth Procurement Rules, 78
- complaints handling, 3
  - complaint reviews, 61
  - 'contacts' versus 'complaints', 56
  - IGIS function and powers, 5
  - non-visa related, 57, 59–61
  - other contacts, 63–4
  - performance results and discussion, 16, 56–64
  - statistics, 57, 58, 59, 60
  - visa or citizenship related, 57–9
  - see also* inquiries
- Comprehensive Review of the Legal Framework Governing the NIC, 21
- consultants, 78–9
- 'contacts' versus 'complaints' *see* complaints handling
- corporate and operational planning, 7, 70–1
- corporate governance, 3, 64, 70–4
- Counter-Terrorism (Temporary Exclusion Orders) Act 2019*, 39
- COVID-19 pandemic
  - COVIDSafe app, 3, 55, 65
  - impact of, 2, 3, 19, 21, 22, 23, 25, 27, 29, 42, 43, 47, 52, 53, 59, 66, 67, 82, 85
  - response to, 2, 67, 71, 113
- Crimes Act 1914*, 38–9
- cross-agency inspections, 53–5
- cyber security, 10

## D

- Defence Intelligence Organisation (DIO), 10
  - AUSTRAC information access and use, 54
  - inspections of, 52–3
  - PJCIS review of administration and expenditure, 21
  - Privacy Guidelines compliance, 53
  - role and functions, 52
- Department of Defence, 40
- Department of Foreign Affairs and Trade, 40
- Department of Home Affairs, 40, 55–6, 64
- Deputy Inspector-General, 6, 7
- detention warrants *see* questioning and detention warrants
- Digital Continuity 2020 Policy, 75
- DIO *see* Defence Intelligence Organisation (DIO)

- disability reporting, 79
- document management system, 3, 64
- documents
  - exemptions to the requirement for government agencies to provide documents, 21–2

## E

- ecologically sustainable development and environmental performance, 113–14
- employees *see* Senior Executive Service officers; staff
- enterprise agreement, 67, 75, 77, 110
- entity resource statement, 83
- ethical standards, 73–4
- Executive Committee, 70
- exempt contracts, 79
- exemptions to the requirement for government agencies to provide documents, 21–2
- expenses for outcome, 84
- external scrutiny of IGIS, 75

## F

- Fair Work Commission, 75
- finance law compliance, 74
- financial intelligence *see* sensitive financial information
- financial management summary, 82–5
- financial statements, 87–107
- firearms *see* weapons use and issues (ASIS)
- Five Eyes Intelligence Oversight and Review Council, 3, 65–6
- force, use of, 38
- foreign services
  - activities, 34–5
  - exchange of information with, 40–1
- fraud control, i, 73–4
- Freedom of information Act 1982*, 8, 21, 79
- functions *see* roles and functions

## G

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



## H

human resources management, 67, 76–8 *see also* staff  
Human Rights Law Centre, 23  
human source management, 30

## I

identities, assumed, 53–4  
imagery intelligence *see* Australian Geospatial-Intelligence Organisation (AGO)  
*Independent Intelligence Review* (2017), 55, 64  
Independent National Security Legislation Monitor, 20  
Information Publication Scheme, 79  
information security authority *see* Australian Signals Directorate (ASD)  
information technology, 3, 64  
informing the public (Objective 3), 14, 22–3  
infrastructure and stakeholders, 64–7  
inquiries, 2  
    employment of persons for a particular inquiry, 74  
    IGIS function and powers, 4, 7  
    notification and reporting requirements, 19  
    performance results and discussion, 15, 23–6  
inquiries by parliamentary committees *see* parliamentary committees  
inspections, 2, 4, 7, 26  
    AGO activities, 50–2  
    ASD activities, 46–50  
    ASIO activities, 28–41  
    ASIS activities, 41–6  
    cross-agency matters, 53–5  
    DIO activities, 52–3  
    ONI activities, 27–8  
    other agencies (ACIC, AFP, AUSTRAC, and Home Affairs), 55–6  
    performance results and discussion, 15, 26–56  
Inspector-General of Intelligence and Security  
    letter of transmittal, i  
    powers, 4  
    review of year, 2–4  
    role, 4–6, 55  
    statutory office holder, 4, 74, 76  
*Inspector-General of Intelligence and Security Act 1986*, 4, 8, 19  
Inspector-General of the Australian Defence Force, 65

Integrity Agencies Group (IAG) meetings, 64  
*Intelligence Services Act 2001*, 9, 10  
    privacy rules *see* Privacy Rules  
internal audit, 71  
international engagement, 65–7  
International Intelligence Oversight Forum, 66  
investigations, 7

## J

Joint Councils for Civil Liberties, 23  
judicial decisions, 75

## K

Key Management Personnel, 74, 111–12

## L

Law Council of Australia, 23  
legislative changes, 2  
letter of transmittal, i

## M

market research, 113  
McFarlane, Stephen, 7, 70, 111, 112  
mental health support, adequacy of (inquiry), 25–6  
Minister for Defence, 10  
Minister for Foreign Affairs, 9  
Minister for Home Affairs, 9  
ministerial and other authorisations to collect intelligence, 9, 10, 43–4, 47, 51  
Ministerial submissions, 41, 43, 47–8  
Ministers  
    assisting Ministers (Objective 1), 13, 19  
    reporting to, 19  
    requests from, 19

## N

non-salary benefits, 77

Notzon-Glenn, Bronwyn, 7, 66, 70, 111, 112

## O

*Office of National Intelligence Act 2018*, 9

Office of National Intelligence (ONI), 9

analytic integrity inspection, 28

inspections of, 27–8

PJCIS review of administration and expenditure, 21

Privacy Rules compliance, 27–8

role and functions, 27

Office of the Australian Information Commissioner, 3, 65 *see also* Australian Information Commissioner

Office of the Commonwealth Ombudsman, 3, 55, 63, 65, 68

ONI *see* Office of National Intelligence (ONI)

*organisational structure*, 6–7, 70

outcome and program, 7, 12, 84 *see also* annual performance statement

outreach program, 22, 55

## P

parliamentary committees

IGIS submissions and appearances, 2, 7, 19–21

Parliamentary Joint Committee on Intelligence and Security, 2, 5, 19–21

performance pay, 78

performance results and discussion *see* annual performance statement

personal information protection *see* Privacy Rules

personal security *see* protective security

plans and planning, 70–1

Portfolio Budget Statements, 7, 82

portfolio relationship, 4

premises, 64

Prime Minister, 9

Privacy Rules, 9, 10

compliance, 27–8, 45, 48, 51–2, 53

protective security, 71

*Public Governance, Performance and Accountability Act 2013*, i, iv, 12, 72, 74, 82, 111, 113

*Public Interest Disclosure Act 2013*, 8, 61–3

public interest disclosure matters, 5, 8, 57, 61–3  
 public outreach activities, 3, 22  
*Public Service Act 1999*, 77  
 purchasing, 78–9  
 purposes, 7–8, 12

## Q

questioning and detention warrants, 38

## R

remuneration, 110–12  
     executive, 74  
     key management personnel, 111–12  
     non-salary benefits, 77  
     performance pay, 78  
 Renwick, James, 20  
 Richardson, Dennis, 21  
 risk management, 71–3  
 roles and functions  
     IGIS, 4–6, 55, 64  
     intelligence agencies, 27, 28, 46, 50, 52  
*Rules to Protect the Privacy of Australians* *see* Privacy Rules

## S

security, protective, 71  
 security assessments by ASIO, 41  
 Senate Estimates hearings, 19  
 Senate Standing Committee on Legal and Constitutional Affairs, 19  
 Senior Executive Service officers  
     employment arrangements, 74, 77  
     remuneration, 74, 110–12  
 senior management committees, 70  
 Senior Officers' Meeting, 70  
 sensitive financial information, 54  
 signals intelligence *see* Australian Signals Directorate (ASD)  
 small business participation in procurement, 78  
 staff  
     employment arrangements, 67, 76, 77

- enterprise agreement, 67, 75, 77, 110
- ethical standards, 73–4
- high performing workforce, 67–8
- human resource management, 67
- immersive development placements, 3, 65, 68
- recruitment, 3, 67
- remuneration, 111–12
- secondments, 2
- surveys, 67
- training and development, 67
- workforce profile, 76–7
- stakeholder engagement, 55–6
- Stone, Hon Margaret, 2, 7, 70, 111, 112
- submissions to Ministers *see* Ministerial submissions
- surveillance devices, 30, 34

## T

- Taxation Administration Act 1953* (TAA), 40
- taxation information, 40
- Telecommunications (Interception and Access) Act 1979* (TIA Act), 20
  - ASD compliance, 49–50
  - ASIO compliance, 30–4, 37, 38–9
- Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, 20, 39
- Telecommunications Legislation Amendment (International Production Orders) Bill 2020, 20

## V

- values, 73
- Vandenbroek, Sarah, 72
- visa-related complaints, 57, 59–61

## W

- Waugh, Lynda, 72
- weapons use and issues, 45–6
- website, 3, 22
- whistleblower protection scheme *see* Public Interest Disclosure matters
- Work Health and Safety Act 2011*, 26
- work health and safety (IGIS staff), 113



