



IGIS

INSPECTOR-GENERAL OF
INTELLIGENCE AND SECURITY

2018–2019

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

GENERAL INQUIRIES

Phone: (02) 6141 3330
Email: info@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

Annual report:
www.igis.gov.au/publications-reports/annual-reports

ISSN: 1030-4657

© Commonwealth of Australia 2019



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

Typesetting by Typeyard Design & Advertising www.typeyard.com.au

Printed by CanPrint Communications www.canprint.com.au



The Hon Christian Porter MP
Attorney-General
Parliament House
CANBERRA ACT 2600

Dear Attorney-General

I am pleased to present my annual report for the period 1 July 2018 to 30 June 2019.

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

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

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

As required by section 10 of the Public Governance, Performance and Accountability Rule 2014, I certify that 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

The Hon Margaret Stone AO FAAL

Inspector-General

30 September 2019



CONTENTS

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

SECTION ONE

OVERVIEW	1
<hr/>	
Inspector-General’s review	2
Role of the Inspector-General of Intelligence and Security	3
About the Australian intelligence agencies	7

SECTION TWO

ANNUAL PERFORMANCE STATEMENT	9
<hr/>	
Entity purpose	10
Results	11
Analysis	18

SECTION THREE

MANAGEMENT AND ACCOUNTABILITY 67

Corporate governance	68
Management of human resources	72
Purchasing and procurement	74

SECTION FOUR

FINANCIAL MANAGEMENT 77

Part 4.1: Financial summary	78
Part 4.2: Financial statements	82

SECTION FIVE

ANNEXURES 101

Annexure 5.1: IGIS salary scale	102
Annexure 5.2: Key management personnel	103
Annexure 5.3: Other mandatory information	105
Annexure 5.4: Requirements for annual reports	107
Index	116

ABOUT THIS REPORT

This is the Inspector-General of Intelligence and Security's annual report for the period from 1 July 2018 to 30 June 2019.

This report has been prepared in accordance with legislative requirements. These include the annual reporting requirements set out in the *Public Governance, Performance and Accountability Act 2013* (the PGPA Act), the associated PGPA Rule, section 35 of the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act) and other legislation.

GUIDE TO THIS REPORT

Section One contains the Inspector-General's review of the reporting period and outlook for 2019-20. This section also outlines the role and functions of the Inspector-General and her office, our published outcomes and program structure and 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 against the indicators identified in the IGIS Corporate Plan 2018-19.

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
AHRC	Australian Human Rights Commission
AIC	Australian Intelligence Community
AML/CTF Act	<i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i>
APS	Australian Public Service
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>
IGADF	Inspector-General of the Australian Defence Force
IGIS	Office of the Inspector-General of Intelligence and Security
IGIS Act	<i>Inspector-General of Intelligence and Security Act 1986</i>
ISA	<i>Intelligence Services Act 2001</i>
NIC	National Intelligence Community
OCO	Office of the Commonwealth Ombudsman
ONA	Office of National Assessments
ONI	Office of National Intelligence
ONI Act	<i>Office of National Intelligence Act 2018</i>
PGPA Act	<i>Public Governance, Performance and Accountability Act 2013</i>
PGPA Rule	Public Governance, Performance and Accountability Rule 2014
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PID	Public interest disclosure
PID Act	<i>Public Interest Disclosure Act 2013</i>
SES	Senior Executive Service
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

This year saw the Office of the Inspector-General of Intelligence and Security (IGIS) operate at a higher tempo than in 2017-18. The office concluded three complex inquiries whilst maintaining a program of agency inspections. The number of complaints received by this office relating to visa and citizenship applications nearly tripled in volume. Concurrent with its oversight activities, the office conducted several recruitment rounds to build the office's workforce in line with plans to expand to 55 full-time equivalent staff by 2020-21. In the course of this recruitment the office welcomed a second Assistant Inspector-General to the team and realigned its organisational structure accordingly. While the planning and design of the new office premises was time consuming, relocation of the office premises was a complete success with minimal interruption to the operations of the office.

The higher tempo was driven in part by significant change for intelligence agencies. The Australian Signals Directorate (ASD) commenced operation as a statutory agency and the Office of National Intelligence (ONI) began operating with its expanded mandate. The Australian Security Intelligence Organisation (ASIO) received new powers to request or require cooperation from telecommunications providers or other persons, often with the effect of granting civil immunity. Certain restrictions on use of force by Australian Secret Intelligence Service (ASIS) staff were removed. Many of these changes were accompanied by measures to ensure that the oversight provided by this office remains effective. To ensure that the legality and propriety risks of unprecedented activities are identified early and managed, agencies have been diligent in consulting the office before exercising new powers. The Parliamentary Joint Committee on Intelligence and Security also routinely sought the views of the office when considering these matters, providing ample opportunity for the office to provide public comment on the nature and practice of intelligence oversight. I note in passing that the past year has also seen intelligence agency heads more frequently and openly engaging directly with the Australian public. While there will always be a need for the independent and impartial view of agency activities provided by this office, the public is increasingly in a position to compare IGIS's statements about the propriety of agency activities with words from agencies themselves. Whether transparency and public messaging is promoted by IGIS or agencies themselves, both bolster the confidence that the public can have that Australian intelligence agencies are acting properly.

Legislation to include the intelligence functions of the Australian Transaction Reports and Analysis Centre, the Australian Criminal Intelligence Commission, the Australian Federal Police, and the Department of Home Affairs within the jurisdiction of the IGIS was not finalised in 2018-19. Nonetheless, the office used 2018-19 to deepen its engagement with these four agencies, as well as with other Commonwealth oversight and integrity agencies. The office program of staff secondments to these agencies has proved especially fruitful in building familiarity and subject matter expertise. The office also continued its engagement with international partners, in particular by hosting the annual Five Eyes Intelligence Oversight and Review Council conference in October 2018. I was also grateful for the opportunity to conduct a program of bi-lateral meetings with intelligence oversight bodies in the United Kingdom and New Zealand.

The coming year may yet bring further changes to the National Intelligence Community; in particular, the office awaits the outcomes of the Comprehensive Review of the Legal Framework Governing the National Intelligence Community, which is due to be presented to the Government at the end of 2019. Regardless of the changes that may occur in the years to come, the office is amply prepared to fulfil its mandate of assurance and independent scrutiny thanks to the continuing development in 2018-19.

Finally, this annual report is a significant milestone in the evolution of this office's implementation and formal reporting in accordance with the IGIS Corporate Plan. Measuring effectiveness is a perennially challenging task for oversight and integrity agencies, as well as for intelligence agencies. With that in mind, I am gratified that the IGIS Corporate Plan 2018-19 has proven to contain meaningful measures of performance over the past financial year, and by pursuing these measures the office ensured that its endeavours throughout 2018-19 remained closely aligned to the mandate of the office. Lessons learned from last year's Corporate Plan have already been incorporated into the IGIS Corporate Plan 2019-20, which is now available on the IGIS website.

THE ROLE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

The Inspector-General of Intelligence and Security (the Inspector-General) is an independent statutory office holder appointed by the Governor-General under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act). The Hon Margaret Stone AO FAAL was appointed as Inspector-General for a term of five years from 24 August 2015.

The Office of the Inspector-General of Intelligence and Security (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. 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.

The IGIS carries out regular inspections of the intelligence agencies that are designed to identify issues of concern, including in the agencies' governance 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, akin to those of a royal commission. These include the power to compel persons to answer questions and produce documents, to take sworn evidence, and to enter agency premises.

The IGIS can investigate complaints, including complaints by members of the public or intelligence agency staff, about the activities of intelligence agencies.

The role and functions of the IGIS 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 oversight by the Parliamentary Joint Committee on Intelligence and Security and the Australian National Audit Office of other aspects of governance in those agencies.

OUR VALUES

INDEPENDENT AND IMPARTIAL

Independence is fundamental to the effective discharge of 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 staff 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

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 environment in which the intelligence agencies operate as well as each agency's operational planning, risk management and approach to compliance. We also need to have a sound understanding of the techniques and technology 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 accept that in the complex environment in which intelligence agencies operate there will inevitably be errors. We encourage agencies to identify and self-report breaches and potential breaches of legislation and propriety and we assist agencies to identify errors and problems. Our focus is on identifying 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 possible in the circumstances.

OPEN

Much of the information that IGIS deals with is classified and cannot be released publicly. That said, we seek to include as much information as possible about our activities and our oversight of intelligence agency activities in our annual report, unclassified inquiry reports and responses to complaints. We are also open about our approach to oversight. We seek 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

Our inspections and inquiries lead to positive changes in agency processes and foster a culture of compliance. IGIS oversight is seen as a positive contribution to agency functions and a key part of the framework within which intelligence agencies operate. We work cooperatively with other oversight bodies to avoid duplication of effort. Our program of public presentations 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

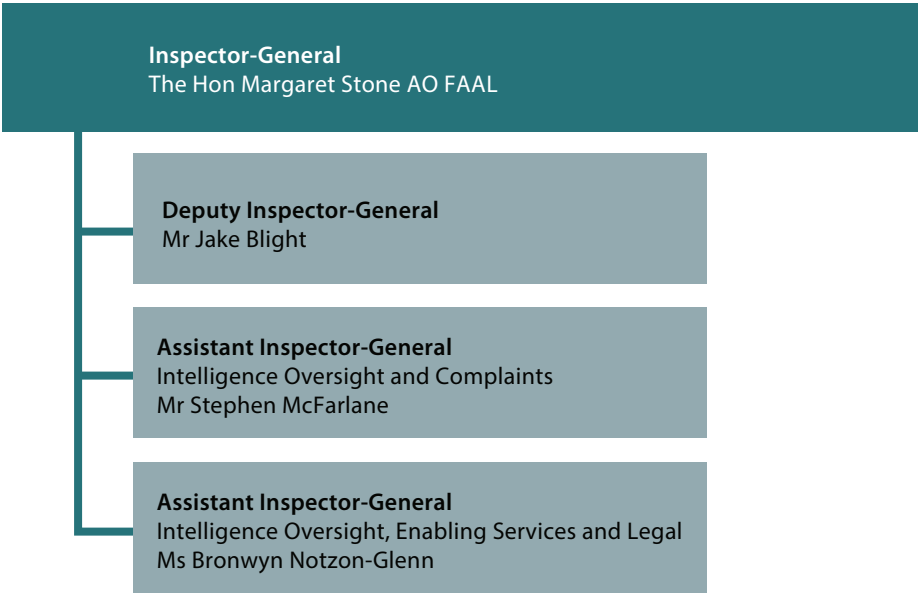
As at 30 June 2019, the office had 32 APS staff. The Inspector-General is supported by a Deputy Inspector-General and two Assistant Inspectors-General.

The Deputy Inspector-General has responsibility for legal and parliamentary matters, as well as finance and office management.

The Assistant Inspector-General Intelligence Oversight and Complaints Branch manages the teams responsible for inspection programs of six agencies within IGIS’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 the four additional agencies in IGIS’s proposed jurisdiction, as well as corporate, legal and policy services for the office.

Figure 1.1 IGIS organisational structure at 30 June 2019



OUTCOME AND PROGRAM STRUCTURE

The office has one outcome, as noted in our 2018-19 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

Consistent with the above, the IGIS Corporate Plan 2018-19 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.¹

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 and 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 ASIO by the Minister responsible for ASIO; and

¹ IGIS Corporate Plan 2018-19 p3

- 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.

ABOUT THE AUSTRALIAN INTELLIGENCE AGENCIES

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 national 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 also 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.

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* (ISA) include communicating secret intelligence in accordance with government requirements, conducting counter-intelligence activities and liaising with foreign intelligence or security services.

Under the ISA, ASIS's activities are regulated by a series of ministerial directions, ministerial authorisations and Privacy Rules.

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

AUSTRALIAN SIGNALS DIRECTORATE (ASD)

ASD is Australia's national authority on signals intelligence and information security. ASD collects foreign signals intelligence, and reports on this intelligence are provided to key policy makers and select government agencies with a clear and established need to know. The Act that established ASD as a statutory agency, the *Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Act 2018*, received Royal Assent on 11 April 2018 and commenced on 1 July 2018.

The responsible Minister for ASD is the Minister for Defence.

OFFICE OF NATIONAL INTELLIGENCE (ONI)

The Office of National Assessments was established in 1977 but following the passage of the *Office of National Intelligence Act 2018* in December 2018 was subsumed by ONI. ONI is responsible for enterprise level management of the National Intelligence Community (NIC) and ensures a single point of accountability for the NIC to the Prime Minister and National Security Committee of Cabinet. ONI produces "all source" assessments on international political, strategic and economic developments to the Government. ONI uses information collected by other intelligence and government agencies, diplomatic reporting and open sources, including the media, to support its analysis.

The responsible Minister for ONI is the Prime Minister.

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 ISA and its activities are regulated by a series of ministerial directions, ministerial authorisations and Privacy Rules.

The responsible Minister for AGO is the Minister for Defence.

DEFENCE INTELLIGENCE ORGANISATION (DIO)

DIO is the Department of Defence's all source intelligence assessment agency. Its role is to provide independent intelligence assessment, advice and services in support of: the planning and conduct of ADF operations; Defence strategic policy and wider government planning and decision making on defence and national security issues; and the development and sustainment of Defence capability.

The responsible Minister for DIO is the Minister for Defence.

SECTION TWO

ANNUAL PERFORMANCE STATEMENT





I, Margaret Stone, 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 2018-19, 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 *Inspector-General of Intelligence and Security Act 1986*. In my opinion, these annual performance statements are based on properly maintained records, accurately reflect the performance of the entity, and comply with subsection 39(2) of the PGPA Act.

The Hon Margaret Stone AO FAAL
Inspector-General of Intelligence and Security

ENTITY PURPOSE

The IGIS 2018-19 Portfolio Budget Statement 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 *Inspector-General of Intelligence and Security Act 1986* 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

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 as much information as possible about the work of the IGIS and the activities of the Australian intelligence agencies.	IGIS provides Ministers with relevant and timely information about the independent oversight activities of the IGIS.	Met – The IGIS met with Ministers as requested and provided each Minister with an information brief relevant to their portfolio following the 2019 Federal Election.
2.1 Providing the Parliament with as much information as possible about the work of the IGIS and the activities of the Australian intelligence agencies.	References to IGIS submissions (written and oral) in the reports of the PJCIS and other committees indicate that the submissions are seen as relevant and useful.	Met – PJCIS reports during 2018-19 cited evidence provided by IGIS in hearings and submissions on 45 separate occasions. Other parliamentary committees cited evidence provided by IGIS.
3.1 Providing the public with as much information about the work of the 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 and in the IGIS annual report.	Partially met - As at 30 June 2019 no inquiry conducted in 2018-19 was the subject of a public statement published separately on the IGIS website. All inquiries conducted by the office during 2018-19 are described in this report which is published on the IGIS website.
	Completion of at least 15 outreach activities each year to groups outside Australia's intelligence community. (Same measure appears in PBS).	Met – The IGIS and SES staff presented at more than 15 formal engagements. A pilot meeting for a standing Civil Society Reference Group was held in June 2019.

PERFORMANCE CRITERION AND CRITERION SOURCE (from Corporate Plan unless indicated)	PERFORMANCE MEASURES (from Corporate Plan unless indicated)	RESULT AGAINST PERFORMANCE CRITERION
	IGIS website provides an easy-to-use complaint submission process. In addition, complaints may be made by phone or in writing.	Met - The website provides a webform and complaints may be made in writing or by phone.
<p>4.1 IGIS has effective working relationships with the agencies we oversee.</p> <p>Extent to which there has been a change within the intelligence agencies as a result of activities of OIGIS (PBS).</p>	Agencies proactively disclose relevant information to IGIS in a timely way.	<p>Met - Agencies proactively notified potential breaches of law or policy. Notifications included early advice of matters later determined to be compliant.</p> <p>Further qualitative evidence is provided under Analysis (arranged agency by agency).</p>
	Agencies respond cooperatively to IGIS suggestions for improving their internal processes.	Met - Qualitative evidence is provided under Analysis (arranged agency by agency).
	The Inspector-General or SES staff meet at least every six months with SES staff from each agency to discuss key issues and arrangements for oversight.	Met - The IGIS and SES staff met frequently with senior staff from agencies throughout the year.

PERFORMANCE CRITERION AND CRITERION SOURCE (from Corporate Plan unless indicated)	PERFORMANCE MEASURES (from Corporate Plan unless indicated)	RESULT AGAINST PERFORMANCE CRITERION
4.2 IGIS has a well-developed and implemented inspection program. Range of inspection work undertaken (PBS).	Where relevant, IGIS inspection reports prompt changes in agency processes and agencies report on improvements.	Met - Qualitative evidence is provided under Analysis (arranged agency by agency).
Inspector-General's comments on any inspection conducted under s 9A of the IGIS Act (s 35(2A) IGIS Act).	An inspection plan approved by the Inspector-General is in place for each of the six agencies within current IGIS jurisdiction.	Partially met - An inspection plan approved by the IGIS or an SES officer was in place for each agency.
Inspector-General's comments on the extent of compliance by ASIS, AGO and ASD with rules made under s 15 of the <i>Intelligence Services Act 2001</i> (s 35(2B) IGIS Act).	Inspections for agencies within current IGIS jurisdiction cover at least 75% of each agency's activity categories. (Same measure appears in PBS).	Partially met - Coverage of activity categories per agency in 2018-19: <ul style="list-style-type: none"> • AGO 87% (7 of 8) • ASD 87% (7 of 8) • ASIO 85% (6 of 7) • ASIS 100% (8 of 8) • DIO 75% (3 of 4) • ONA to Dec 2018: 33% (1 of 3) • ONI from Dec 2018: 18% (2 of 11) The reason the ONA/ONI measure was not met is discussed under Analysis.
	An interim inspection plan is in place for the four agencies expected to be added to IGIS jurisdiction by the time relevant amendments to the IGIS Act commence.	Not applicable - The IGIS Act was not amended to bring the four agencies under IGIS jurisdiction in 2018-19.
	Inspection plans are reviewed at least once every six months.	Met - Inspection plans for all agencies were reviewed at least once every six months.



PERFORMANCE CRITERION AND CRITERION SOURCE (from Corporate Plan unless indicated)	PERFORMANCE MEASURES (from Corporate Plan unless indicated)	RESULT AGAINST PERFORMANCE CRITERION
4.3 IGIS has a well-developed and implemented inquiry capability. Level of acceptance by intelligence agencies of conclusions and recommendations of inquiries conducted (PBS).	Program of own-motion inquiries including regular analytic integrity inquiries and inquiries triggered by inspection findings or complaints.	Met - Three inquiries were conducted during 2018-19. Further evidence under Analysis (inquiry by inquiry).
Inspector-General's comments on any inquiry conducted in accordance with paragraph 8(1)(d) or 8(3)(c) of the IGIS Act (s 35(2) IGIS Act).	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 PBS).	Met - 100% of recommendations provided during 2018-19 were accepted.
Inspector-General's comments on the employment of any person under s 32(3) and any delegation under s 32AA of the IGIS Act (s 35(2AA) IGIS Act).	(PBS) 100% of inquiry recommendations implemented.	Met - 100% of recommendations implemented from inquiries finalised in 2017-18 were implemented. Status of implementation of recommendations from inquiries finalised in 2018-19 discussed under Analysis.
4.4 IGIS has efficient complaint and public interest disclosure management processes. Finalisation of complaints in a timely manner (PBS).	90% of complaints acknowledged, triaged and allocated within five working days. (Same measure appears in PBS).	Met - Percentage acknowledged, triaged and allocated within five working days: <ul style="list-style-type: none">• Visa-related complaints: 97%• Public Interest Disclosures: 100%• Other complaints: 93% Further details are provided under Analysis.

**PERFORMANCE CRITERION
AND CRITERION SOURCE**
(from Corporate Plan
unless indicated)

PERFORMANCE MEASURES
(from Corporate Plan
unless indicated)

**RESULT AGAINST
PERFORMANCE
CRITERION**

85% of visa-related complaints resolved within two weeks. (Same measure appears in PBS).

Met - 93% of visa-related complaints were resolved within two weeks.

Public interest disclosures are managed in accordance with statutory requirements, including timeframes.

Met - All disclosures were managed in accordance with statutory requirements, noting all disclosures were ultimately investigated under the IGIS Act not the PID Act.

5.1 Appropriate infrastructure.

IGIS premises meet all applicable security accreditation standards.

Met - IGIS previous and current premises met all applicable security accreditation standards. See Analysis for further information on office move.

IGIS classified ICT systems meet all applicable security accreditation standards.

Met - All IGIS classified ICT systems met all applicable security accreditation standards. See Analysis for further information on office move.

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.

Met - Arrangements were in place.

Plan to implement electronic document management and complaint management systems to coincide with move to new ICT systems.

Met - A plan was in place and the office is awaiting delivery of new systems.

PERFORMANCE CRITERION AND CRITERION SOURCE (from Corporate Plan unless indicated)	PERFORMANCE MEASURES (from Corporate Plan unless indicated)	RESULT AGAINST PERFORMANCE CRITERION
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.	<p>Met - ACLEI, IGADF, OCO each met at least twice per year.</p> <p>IGIS hosted the FIORC conference in October 2018.</p> <p>Bilateral meetings held with UK and NZ intelligence oversight agencies.</p> <p>Further details are provided under Analysis.</p>
	Exchange of information with other integrity agencies leads to improvements in our processes.	<p>Met - Liaison with other Australian integrity agencies provided greater insight into complaint trends and handling of issues that are within jurisdiction of two or more agencies. Liaison with other intelligence oversight bodies helped in considering the launch of a pilot Civil Society Reference Group.</p>
6.1 High performing professional staff.	IGIS has a performance management framework that integrates performance expectations and professional development.	<p>Met - IGIS performance management framework integrates these considerations.</p>
	All IGIS staff have performance plans in place and these are reviewed in accordance with the performance management framework.	<p>Met - All IGIS staff had plans in place in accordance with the framework.</p>

PERFORMANCE CRITERION AND CRITERION SOURCE (from Corporate Plan unless indicated)	PERFORMANCE MEASURES (from Corporate Plan unless indicated)	RESULT AGAINST PERFORMANCE CRITERION
	IGIS has sufficient staff with the skills necessary to support IGIS oversight activities including inspections, inquiries and complaint management, as well as IGIS engagement with the legislative process.	Met - IGIS has staff with the skills necessary to support IGIS oversight activities.
6.2 Recruitment and training.	IGIS runs at least 10 modules of internal training per year.	Met - 10 internal training modules were conducted.
	IGIS is meeting the recruitment targets set in the IGIS strategic HR plan.	Partially met - IGIS conducted multiple recruiting rounds and as at 30 June 2019 the office had 32 out of a target of 42 staff. A number of additional candidates were undergoing relevant pre-employment organisational suitability and security checks.
6.3 Office culture and ethos.	IGIS staff comply with APS and security obligations.	Met - No breaches of APS obligations occurred. No major security incidents were detected.
	IGIS staff utilise flexible working arrangements.	Met - All requests for flexible working arrangements were agreed.
	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.	Met - A staff survey was undertaken in 2019 with a response rate of 90%. Feedback from a staff survey in 2018 has been addressed.



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 draft copy of an inquiry report must be provided to the responsible Minister for comment, and a copy of the final report must be provided. IGIS met these requirements for all inquiries conducted during 2018-19. The IGIS Act also provides that IGIS 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 2018-19. Under section 25A of the IGIS Act, the IGIS may report to the responsible Minister on a completed inspection of an intelligence agency. During 2018-19 no such reports were made.

The office responded promptly to all requests from Ministers during 2018-19 for information or briefings about the independent oversight activities of the office. Each Minister responsible for an intelligence agency was proactively provided an information brief upon assuming or reassuming office following the 2019 Federal Election.

During 2018-19 no requests were made by Ministers or the Prime Minister for the IGIS 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 23 October 2018 for Supplementary Budget Estimates, and on 19 February 2019 during the 2018-19 Additional Estimates hearing. The Inspector-General was prepared to attend Budget Estimates on 9 April 2019 but was not called by the Committee to appear.

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

The Inspector-General participated in six inquiries conducted by the Parliamentary Joint Committee on Intelligence and Security (the PJCIS) during the reporting period:

- Review of the Office of National Intelligence Bill 2018 and Office of National Intelligence (Consequential and Transitional Provisions) Bill 2018;
- Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018;
- Review of the Intelligence Services Amendment Bill 2018;
- Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*;

- Review of the Counter-Terrorism (Temporary Exclusion Orders) Bill 2019; and
- Review of Administration and Expenditure No. 17 (2017-2018).

The Inspector-General's contributions to the PJCIS's legislation inquiries provided information about the oversight implications of proposed changes to agencies' governing legislation, and in some instances, about the efficiency and effectiveness of the performance of oversight functions.

During the PJCIS inquiries into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill (the Bill) in 2018 and the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Act) in 2019, the Inspector-General provided six separate submissions and appeared before the Committee on three separate occasions. The Inspector-General gave evidence about a range of technical concerns including identifying areas of ambiguity in the legislation and suggestions to improve clarity.

The PJCIS's report on the Bill was tabled on 6 December 2018, and included recommendations to strengthen oversight of the new powers. Amendments responding to the PJCIS's recommendations were introduced on 7 December 2018, and the amended Bill was passed on the same day. Following this, the Committee commenced a separate review of the Act. The PJCIS presented its second report on 2 April 2019, and made a number of recommendations including those relating to the need for adequate resourcing of oversight bodies. During the reporting period, the Committee commenced a third review of the Act, and the Inspector-General will report on engagement with that review in the next annual report.

The Inspector-General also provided evidence to the PJCIS review of agencies' administration and expenditure for the 2017-18 financial year. IGIS regularly participates in this review, providing a public submission and classified oral evidence when requested by the Committee. In the period under review by the Committee, the Inspector-General provided an overview of oversight responsibilities and functions exercised.

Broadly, the three other inquiries involved proposals to amend legislation relating to, amongst other things, ASIO, ASIS and ONI functions or powers. The Inspector-General provided comments on the oversight implications of these proposals.

SENATE LEGAL AND CONSTITUTIONAL AFFAIRS COMMITTEE

The Inspector-General participated in two inquiries conducted by the Senate Legal and Constitutional Affairs Committee during the reporting period:

- Review of Defence Amendment (Call Out of the Australian Defence Force) Bill 2018 (the Defence Bill); and
- National Integrity Commission Bill 2018 (No. 1), and National Integrity Commission Bill 2018 (No. 2).

The Inspector-General provided submissions to both inquiries.

In respect of the Defence Bill, the Inspector-General provided evidence to the Committee noting, among other things, that the proposed amendments would not amend the scope of her oversight. The Committee's report was presented in September 2018, recommending that the Bill be passed with amendments clarifying the purpose of making a call out of the Australian Defence Force. The Bill was passed on 27 November 2018.

The National Integrity Commission Bills were a package of private Member and private Senator Bills which, broadly, sought to establish a federal independent public sector anti-corruption commission. The Inspector-General provided evidence relating to, among other things, the potential for overlap between the functions of the proposed commission and the existing jurisdiction of the Office of the Inspector-General of Intelligence and Security. The Committee's report was presented in April 2019 and did not recommend the Bills' passage.

SENATE FINANCE AND PUBLIC ADMINISTRATION COMMITTEE

During the reporting period the Senate Finance and Public Administration Committee conducted a review of the Intelligence Services Amendment (Enhanced Parliamentary Oversight of Intelligence Agencies) Bill 2018.

The Bill was a private Senator's Bill, and proposed amendments to extend parliamentary scrutiny over the activities of Australia's national security and intelligence agencies. The Inspector-General made a submission to the review and appeared before the Committee at a public hearing on 26 October 2018. The Inspector-General gave evidence, amongst other things, relating to the Bill's proposed imposition of additional mandatory functions on the Office of the Inspector-General of Intelligence and Security. The Committee's report was presented on 12 November 2018 and did not recommend the passage of the Bill.

COMPREHENSIVE REVIEW OF THE LEGAL FRAMEWORK GOVERNING THE NATIONAL INTELLIGENCE COMMUNITY

The Inspector-General is participating in the Comprehensive Review of the Legal Framework Governing the National Intelligence Community being conducted by Mr Dennis Richardson AC. The office provided submissions in response to the issues papers prepared by the Review and participated in workshops conducted by the Review throughout the year on a range of topics. The Inspector-General continues to work collaboratively with the Review.

OBJECTIVE 3 – INFORMING THE PUBLIC

ABOUT ENGAGEMENT WITH THE PUBLIC

The IGIS Act provides that it is a purpose of the office to assist the Government in assuring the Parliament and the public that intelligence and security matters relating to Commonwealth agencies are open to scrutiny, in particular the activities and procedures of intelligence agencies.

IGIS 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 whose interest is less specialised and extends to the whole range of current affairs as well as more eclectic groups who have a great range of intellectual interests. The program is

designed to create greater public awareness and understanding of the role and activities of this office. During 2018-19, these activities were conducted in line with a draft strategic engagement plan. The plan was developed to test whether the target audience for public engagement activities achieves an appropriate balance between being sufficiently representative of the general Australian community while aligning the office's outreach efforts to those groups mostly likely to derive a material benefit from such engagement.

PUBLIC OUTREACH ACTIVITIES

In addition to publishing material on the IGIS website and in this annual report, during 2018-19 the office delivered over 15 presentations to groups outside the intelligence community. The Inspector-General delivered presentations to academic audiences at several universities around Australia, including the 21st Geoffrey Sawer Lecture at the Australian National University Centre for International and Public Law. In April 2019 the Inspector-General addressed a public consultation workshop conducted for the Comprehensive Review of the Legal Framework Governing the National Intelligence Community. These engagements were supplemented by lectures and presentations delivered by SES staff from the office to various audiences outside the intelligence community, comprising both 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 three groups chosen for the pilot (the Joint Councils for Civil Liberties, the Human Rights Law Centre and the Law Council of Australia) were selected because they regularly make submissions to the PJCIS on a wide range of matters relating to Australian intelligence and security agencies. 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.

It is envisaged that the meetings will give civil society groups access to relevant and credible unclassified information about the work of the IGIS and Australia's intelligence and security agencies; give the IGIS an opportunity to understand the views of those who work with people directly affected by the work of intelligence and security agencies; provide a forum for discussion of differing perspectives about issues relevant to the work of IGIS; and potentially allow for the discussion of legal and technical issues with civil society groups who possess expertise in such fields.

The next meeting of the Civil Society Reference Group is scheduled for late 2019.

OBJECTIVE 4 – INQUIRIES, INSPECTIONS AND INVESTIGATION OF COMPLAINTS

Figure 2.1: Performance indicators – conducting inquiries

SUBJECT OF INQUIRY	ASD MATTER 2017	DIO ANALYTIC INDEPENDENCE	ASIS MATTER	ASD MATTER 2018	ASIO MATTER
Agency	ASD	DIO	ASIS/ASIO	ASD/ASIO	ASIO
Source	IGIS own motion	IGIS own motion	IGIS own motion	Minister of Defence request	IGIS own motion
Date initiated	2 February 2017	14 November 2016	12 July 2018	30 May 2018	14 February 2018
Date finalised	14 July 2017	8 September 2017	20 December 2018	2 May 2019	14 June 2019
Duration (days)	163 days	299 days	161 days	337 days	485 days
Number of recommendations	5	2	4	5	8
Percentage of recommendations accepted	100%	100%	100%	100%	100%
Implementation of recommendations as at 30 June 2019	100% fully implemented	100% fully implemented	100% fully implemented	0% completed but in progress	0% completed but in progress

INQUIRY INTO AN AUSTRALIAN SIGNALS DIRECTORATE MATTER 2017

As reported in the 2017-18 annual report, in July 2017 this office completed an inquiry into an Australian Signals Directorate (ASD) matter pursuant to section 8(2) of the IGIS Act. The Inquiry Report included five classified recommendations designed to ensure that the situation would not arise in the future and to streamline ASD's communications with Ministers and with the IGIS. ASD accepted all five recommendations, and provided reports to the IGIS regarding implementation progress in December 2017 and June 2018, by which point it had fully implemented three of the recommendations. In August 2018 ASD confirmed that it had finalised the remaining two. This office reviewed ASD's advice and considers that ASD has sufficiently implemented all Inquiry recommendations.

INQUIRY INTO THE ANALYTIC INDEPENDENCE AND INTEGRITY OF THE DEFENCE INTELLIGENCE ORGANISATION

In September 2017, the IGIS completed a third inquiry into the analytic independence and integrity of the Defence Intelligence Organisation (DIO). This was a routine Inquiry, not prompted by any particular concern. The Inquiry did not find any evidence of interference with the independence of DIO assessments; generally the analytical integrity of the DIO process for producing reports is sound, although some areas for continuing improvement were highlighted. The Inquiry made two recommendations relating to analytic tradecraft policy and record keeping and several suggestions for improvement, which DIO accepted. A detailed unclassified summary of this Inquiry can be found on the IGIS website www.igis.gov.au/publications-reports/public-reports.

In November 2018, DIO released an updated end-noting and sourcing policy, which completed recommendation one of the Inquiry. In December 2018 DIO advised this office that an identified technical change had been implemented, satisfying recommendation two of the Inquiry.

The next analytic independence and integrity inquiry is scheduled to be conducted in 2020.

INQUIRY INTO AUSTRALIAN SECRET INTELLIGENCE SERVICE MATTER

On 12 July 2018 this office commenced an inquiry into allegations that ASIS officers engaged in misconduct and fraud. The allegations were made by a former ASIS officer. Although lacking detail, the serious nature of the allegations warranted the Inspector-General initiating a formal inquiry as soon as possible.

At the time, the resources of the office were not sufficient to commit to an inquiry on an urgent basis. Consequently, the Inspector-General identified Mr Bruce Miller AO as having the appropriate expertise and security clearance and invited Mr Miller to lead the Inquiry. In accordance with section 32(4) of the IGIS Act, approval of Mr Miller's appointment was obtained from the Minister for Foreign Affairs. Pursuant to section 32AA of the IGIS Act, the Inspector-General delegated to Mr Miller, in writing, the functions and powers required for him to lead the Inquiry. Mr Miller led the Inquiry supported by IGIS staff.

The Inquiry Report was completed on 20 December 2018 and the Inspector-General adopted the Inquiry Report as her own. The Inquiry found no evidence to support the allegations, either in the records reviewed or through interviews of those in a position to know the facts. The Inquiry did, however, find areas where ASIO and ASIS could improve communication and collaboration.

The Report included four recommendations, all of which were accepted. All recommendations have now been implemented and ASIO and ASIS have provided this office with details of the implementation.

INQUIRY INTO AUSTRALIAN SIGNALS DIRECTORATE MATTER 2018

In May 2018 the Inspector-General began an inquiry into the unauthorised interception of telecommunications by ASD. The Inquiry was requested by the then Minister for Defence, at the suggestion of the Director-General Designate of ASD. The Minister expressed concern with the timeliness and adequacy of reporting to her and the Inspector-General, noting similar inadequacies were identified during a 2017 IGIS Inquiry. ASD cooperated fully with the Inquiry.

The Inquiry related to an operation to collect communications of foreign intelligence value. The operation was facilitated by warrants sought by ASIO under the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Intercepting a communication under such a warrant is only lawful if the person who takes the action has been authorised to do so by an instrument made under section 12 of the TIA Act. Individual staff members of ASD are routinely authorised to intercept communications under these warrants.

In June 2017, ASD advised the Inspector-General that as a result of an error in preparing the relevant authorisation under section 12 for certain warrants, some ASD staff who were not authorised had intercepted telecommunications; in the absence of authorisation the collection was unlawful. That advice did not give any indication of the scale of the issue. By July 2017, five months after the warrants were signed, ASD staff were aware that a significant number of unlawful interceptions had occurred. This information was not conveyed to the Inspector-General or the Minister for Defence until February 2018.

The Inquiry found that the unlawful interception was the result of an error made by ASIO in preparing the relevant authorisation and by a failure on the part of ASD to check the accuracy of the authorisation before relying on it. When the error was detected ASD promptly requested a new authorisation and ASIO promptly responded to that request. Once the authorisation instrument was corrected ASD undertook a lengthy internal investigation and took appropriate steps to delete all unlawful intercept.

The Inquiry found that ASD's initial reporting of this matter to the Inspector-General and the Minister for Defence was inadequate. ASD did make a comprehensive report of the matter to the Inspector-General and the Minister prior to the Inquiry commencing, and has improved its reporting since this incident occurred. While ASIO did not report the breaches of the warrant to the Attorney-General, ASIO has since amended its procedures and is now reporting breaches to the Attorney-General.

The Inquiry also found that in the past 10 years, in a relatively small percentage of the warrants that ASD was involved in executing, there had been regular legislative breaches and incidents resulting from inadequate management of warrant procedures.

The final Inquiry Report was issued on 2 May 2019. The Inspector-General made five (classified) recommendations to improve the reporting of future breaches of the TIA Act, and reduce the risk of their recurrence. ASD and ASIO accepted all five recommendations and have commenced implementation. ASD and ASIO are expected to report to the IGIS on progress of implementation of the recommendations no later than 30 October 2019.

INQUIRY INTO AN AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION MATTER

On 14 February 2018 in response to ASIO's notification of a potential non-compliance matter, pursuant to section 8(1) of the IGIS Act the Inspector-General, of her own motion, initiated an inquiry into an ASIO matter. The Inquiry examined the conduct and details of a multi-faceted, multi-agency foreign intelligence collection operation led by ASIO, including whether certain intelligence collection activities conducted by ASIO as part of that operation were lawful. While the Inquiry found significant problems with the planning and execution of the operation, stemming from systemic weaknesses within ASIO's compliance management framework, it also concluded it is likely that most, but not all, of the activities reviewed as part of the Inquiry were lawful. Importantly, there was no evidence of any deliberate wrong-doing by the officers involved in the operation.

The issues identified by the Inquiry included poor communication between ASIO's lawyers and operational staff. As a consequence of the poor communication ASIO staff believed, incorrectly, that a warrant was not required to undertake activities that in fact did require such authorisation. Additionally, as ASIO's lawyers were not fully informed about changes to operational plans those activities were conducted without proper advice. Other issues identified by the inquiry included failures to comply with procedural requirements for warrants and associated reports; a key secondment agreement being signed by an officer without the appropriate delegation to do so; and inadequate management and supervision of those officers ostensibly seconded to ASIO.

In addition to reviewing the circumstances surrounding the operation, the Inquiry also examined ASIO's approach to compliance and training more broadly. It found that ASIO provided little if any compliance training for ASIO employees and affiliates in relation to legislative restrictions germane to the operation. The Inquiry also found that whilst operational staff complied with ASIO's operational planning procedures, these procedures were inconsistent with other ASIO policies and were insufficient to ensure that ASIO acted lawfully. At the time of the incident, ASIO did not have a dedicated compliance unit; however, even before the formal recommendations outlined in the following paragraph were made, ASIO had begun to develop a formal compliance framework and to establish a dedicated compliance unit.



The final Inquiry Report was issued on 14 June 2019 and made eight recommendations. Those recommendations focus on ensuring that ASIO's proposed compliance team is established as a matter of priority; that ASIO implements a compliance training program; improves legal advice; and reviews relevant policies and procedures. ASIO has accepted all eight recommendations.

ASIO is expected to report to the Inspector-General on progress of implementation of the recommendations by 30 September 2019. This office will continue to monitor ASIO's implementation of the Inquiry recommendations and further details will be provided in the next annual report.

OBJECTIVE 4 - INSPECTIONS

INSPECTION OF ASIO ACTIVITIES

ASIO's activities have been categorised according to the functions of the Organisation set out in section 17 of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) namely:

- security intelligence collection, correlation and evaluation;
- 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 and communication of foreign intelligence; and
- co-operation with and assistance to other agencies.

During this reporting period the ASIO inspection team met the IGIS target of inspecting at least 75% of ASIO's activity categories. Priority was given to reviewing ASIO's intelligence collection activities, its security assessments, and advice to Ministers on security matters. There were no inspections of ASIO's provision of advice relating to protective security.

During 2018-19 ASIO was involved in three matters which were the subject of inquiries pursuant to section 8 of the IGIS Act. These inquiries are described separately in this report (see page 22).

REGULAR INSPECTIONS OF INVESTIGATIVE CASES

It is not possible to monitor all ASIO activities. Accordingly, IGIS staff regularly inspect a sample of activities selected on the basis of risk and available resources. For this purpose IGIS staff have direct access to the relevant ASIO information technology and records management systems.

Throughout 2018-19 IGIS staff conducted inspections using a variety of methodologies, including thematic reviews, risk-based sampling and random sampling. 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; and
- compliance with internal policies and procedures.

ASIO proactively provided an increased number of briefings to the office compared to the previous reporting period. The briefings covered a wide range of topics including new capabilities, new initiatives and areas of risk.

In the previous reporting period (2017-18), record keeping deficiencies at ASIO were identified as an issue requiring continued monitoring by the office during 2018-19. Inspections in 2018-19 continued to identify minor record-keeping issues; however, the overall standard of record-keeping has improved since June 2018.

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 than those of DIO and ONI, 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. These assessments may also result in ASIO providing specific policy guidance to the Government.

During the reporting period, ASIO instituted several measures to provide greater support to analysts, including the appointment of a senior analyst with specific responsibility for promoting and coordinating analytical tradecraft, training and quality assurance across ASIO.

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 staff reviewed ASIO human source case files and met with ASIO staff to discuss related activities. Overall ASIO handles their human sources sensitively and no significant issues of concern were identified by IGIS staff when reviewing these activities.

ASIO WARRANTS

ASIO can intercept telecommunications under warrants issued by the Attorney-General pursuant to the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). Warrants for the exercise of other intrusive powers, including searches, computer access and surveillance devices, can be issued pursuant to the provisions of the ASIO Act.

Throughout the reporting period IGIS staff inspected an indicative sample of warrants, primarily as part of the regular inspection of investigative cases. As in previous years, several ASIO warrant documents contained typographical errors; however, the majority of typographical errors in 2018-19 were identified by ASIO and proactively advised to this office in a timely fashion, rather than being discovered during an inspection. ASIO has further refined its processes to help ensure that warrant documentation is accurate.

Two systemic issues relating to warrants were raised with ASIO during 2018-19. One issue, first mentioned in the 2017-18 annual report, related to authorisations of classes of persons under section 24 of the ASIO Act. The office raised with ASIO some descriptions that had been used to define a class of persons for the purposes of section 24 that the office considered may be overly broad, uncertain, or not sufficiently connected to the exercise of power under the warrant. In response, ASIO undertook to review its operational arrangements and warrant application procedures.

The second issue related to the inappropriate use of templated text to brief the Attorney-General for the purposes of section 27C(2)(b) of the ASIO Act. In response ASIO amended warrant application templates to prompt officers to provide a tailored brief in relation to this criterion.

As noted above, ASIO proactively informed the office of breaches and other issues relating to warrants issued under the TIA Act and the ASIO Act. There was a substantial increase in the number of notifications made to this office in this reporting period, including early notification of several incidents that were ultimately confirmed to be compliant and notification of incidents that resulted from events outside ASIO's control but which ASIO believed should be notified to this office in the interests of transparency. Some incidents reported were attributable to mistakes made by telecommunications carriers rather than ASIO, nevertheless they required remedial action from ASIO such as deleting information incorrectly sent by the carrier. This office welcomes the increased rate of voluntary disclosures of potential non-compliance and related incidents by ASIO. A detailed summary of compliance incidents reviewed by this office is provided below.

INCIDENTS RELATING TO INTERCEPTION WARRANTS UNDER THE TIA ACT

TYPOGRAPHICAL ERROR IN REQUEST TO INTERCEPT A TELECOMMUNICATIONS SERVICE UNDER S 9A OF THE TIA ACT

ASIO advised of an incident where it requested a telecommunications carrier intercept an additional telecommunications service under a named person warrant, on the grounds that the service was being used, or was likely to be used by the subject of the warrant. In fact, the written request to the carrier contained a typographical error and the specified service was unrelated to the subject of the warrant. The error was identified roughly one month after interception was enabled, at which time efforts to intercept the incorrect service

were discontinued and interception was commenced on the correct service. However, no telecommunications were intercepted on the incorrect service as it was not currently subscribed; consequently, it was not necessary for ASIO to quarantine and delete data.

TYPOGRAPHICAL ERRORS IN WARRANT APPLICATIONS UNDER S 11B OF THE TIA ACT

ASIO advised of three instances where an application for a named person warrant under section 11B of the TIA Act included a typographical error in one of the telecommunications services listed in the application as being used or likely to be used by a foreign person or organisation.

Having regard to the specific circumstances of each incident, the office is satisfied that none of these three incidents resulted in a breach of the TIA Act.

ERRORS BY TELECOMMUNICATIONS CARRIERS LEADING TO UNAUTHORISED COLLECTION

ASIO advised of four instances where errors made by telecommunications carriers resulted in ASIO receiving information which it was not authorised to collect. In all instances ASIO informed the telecommunications carriers of the error; it promptly took steps to prevent collection of further information and to delete all such information stored on ASIO systems.

BREACHES OF S 16 OF THE TIA ACT

ASIO advised of a breach of section 16(2)(c)-(d) of the TIA Act where the interception of a telecommunications service under a named person warrant should cease, but due to a breakdown in internal processes oral and written advice was provided to the carrier over one month after the determination was made. All data collected during this period was deleted within seven days once the error was identified.

In 2018-19 ASIO also separately advised of a second possible breach of section 16(2) of the TIA Act. As at 30 June 2019 ASIO had not concluded its investigation into this incident.

ONGOING NON-COMPLIANCE WITH S 17 OF THE TIA ACT

Section 17(2) of the TIA Act requires ASIO to report to the Attorney-General with details of each telecommunications service intercepted under a named person warrant. In 2017-18 this office identified that ASIO had provided a report to the Attorney-General advising that all services named on a warrant had been intercepted without establishing the accuracy of this advice. IGIS staff continued to note similar instances of non-compliance with section 17(2) of the TIA Act during 2018-19. While ASIO acknowledges its non-compliance is ongoing, practical difficulties render it impossible to remediate this issue completely in the near future. As an interim measure, ASIO has improved the accuracy of section 17 reports by including explanatory notes outlining the limitations on the assurance they can provide to the Attorney-General in relation to section 17(2). In the interests of allocating scarce resources IGIS staff do not propose to monitor this issue further during 2019-20 as the extent of ASIO's non-compliance is now fully known to the Attorney-General and the Minister for Home Affairs.

COLLECTION OF PERSONAL INFORMATION

Under the TIA Act, ASIO is obliged to instruct telecommunications carriers to discontinue interception of telecommunications where there are no longer grounds to maintain the interception or the warrant or authority authorising the interception has lapsed or has been revoked.

As an additional measure and pursuant to the Attorney-General's Guidelines (the Guidelines), ASIO maintains internal controls to terminate the collection and storage of telecommunications data at the moment it is determined the collection is no longer justifiable. These controls mitigate the risk that a delay by the carrier in effecting disconnection will result in the unjustifiable collection of personal information by ASIO.

During the reporting period, ASIO advised this office of two relatively short periods where the ordinary operation of these internal controls failed and required remedial intervention. On both occasions, a greater than usual amount of personal information was collected (covering the time period between providing advice to telecommunications carriers and disconnection being effected); however, this additional information was subsequently deleted from ASIO systems.

Having regard to the circumstances, the IGIS is satisfied that ASIO's actions in relation to this issue are consistent with the Guidelines requirement to take all reasonable steps to minimise the collection of personal information to what is reasonably necessary.

FAILURE TO DELETE DATA AS INTENDED

As an assurance activity, each year IGIS staff conduct an inspection to confirm that the deletion of data from ASIO systems has been effective and that no traces of information unintentionally remain. During 2018-19, the office identified one instance where data that ASIO had advised was deleted from all systems was still available on one system. ASIO deleted this data after it was identified during the inspection activity.

DESCRIPTION OF SERVICES

When ASIO submits a request to the Attorney-General to obtain a named person warrant under section 9A or section 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 staff queried whether ASIO's warrant documentation made clear the nature of the services ASIO intended to target. In this reporting period, ASIO prepared standing guidance for the Attorney-General on how it describes telecommunications services, in consultation with this office. As at 30 June 2019 the advice was yet to be provided to the Attorney-General.

INCIDENTS RELATING TO SPECIAL POWERS UNDER THE ASIO ACT

ISSUE IN RELATION TO A S 25A COMPUTER ACCESS WARRANT

ASIO advised of an issue in relation to a computer access warrant under section 25A of the ASIO Act. At the time the warrant was issued, ASIO assessed on reasonable grounds that a computer specified in the warrant was likely to be used by the subject of an investigation (Person A). Later, during the life of the warrant, it became apparent to ASIO that Person A was not likely to use the computer. Due to a failure in internal processes an ASIO officer mistakenly accessed the computer. Irrespective of questions of legality, in these circumstances, access to the computer would at least raise an issue of propriety. Discussions with ASIO regarding ASIO's response to this incident are continuing.

UNAUTHORISED COLLECTION FROM SURVEILLANCE DEVICES UNDER A S 27F IDENTIFIED PERSON WARRANT

ASIO advised of one instance of unauthorised collection under the ASIO Act. The breach related to the use of surveillance devices under an identified person warrant, pursuant to an authorisation under section 27F of the ASIO Act. A second warrant was issued to permit ASIO to use other special powers in relation to the person but, as ASIO had decided to discontinue the use of surveillance devices, no authorisation was sought to permit the continued use of surveillance devices under the second warrant. The decision not to seek a further authorisation to use surveillance devices under the second warrant was not brought to the attention of the relevant area within ASIO. Consequently, upon expiry of the first identified person warrant ASIO did not disable the surveillance devices. The devices were used without authorisation for seven days before ASIO realised that they were still operational. Upon identifying the issue, all data collected during those seven days were deleted from ASIO systems within 24 hours. ASIO conducted a review of procedures and instituted new checks to be followed at the time a warrant expires, to ensure that any activities not authorised under a successive warrant are terminated.

POTENTIAL UNAUTHORISED ACTIVITY UNDER A S 25 SEARCH WARRANT

ASIO advised this office of a possible breach of section 25 of the ASIO Act in that a person who examined records during a search activity may not have been authorised under section 24 to do so. Discussions are continuing between this office and ASIO to determine whether the person was authorised to examine the records.

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 (the Guidelines).

ASIO reported one instance where it was determined that the subject of a section 176 TIA Act authorisation no longer met the threshold for a security investigation. In closing the investigation, ASIO officers inadvertently failed to revoke the section 176 authorisation; this led to two further weeks of information being collected. Immediately after the non-compliance was identified, ASIO revoked the authorisation and deleted the additional information. The proper operation of section 176(6), supported by similar requirements in the Guidelines, imposes an obligation on ASIO officers to be diligent in revoking authorisations upon identifying that the subject is no longer of security interest. In response to this incident, ASIO revised relevant processes to prevent future occurrences.

ASIO also reported one instance where a typographical error in an authorisation under section 175 of the TIA Act resulted in ASIO collecting information relating to a telecommunications service that was not relevant to ASIO's functions. The error was detected when the collected information was analysed. ASIO deleted the erroneously collected information within 48 hours of identifying the error.

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 section 31A of the ASIO Act, when force is used against a person in the execution of a warrant ASIO must notify the Inspector-General in writing as soon as practicable. The 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 (three days) of the use of force, to be followed by more detailed information within 10 days.

During the reporting period, IGIS received one notification of the use of force against persons during the execution of an ASIO search warrant. The force was used by law enforcement officers assisting ASIO in the execution of the warrant. The incident was subject to the usual police internal reporting and review process and there is no indication in the police report that the force was other than reasonable and proportionate for the purpose for which it was exercised. ASIO provided an initial written notification to IGIS three days after the use of force, and this was followed by a detailed written notification 11 business days after the use of force.

This is only the second use of force notification this office has received since the ASIO Act was amended in 2014 to permit the authorisation of the use of force against persons in the exercise of a search warrant.

SPECIAL INTELLIGENCE OPERATIONS

ASIO's special intelligence operations (SIO) powers introduced in 2014 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 can seek these authorisations to assist in the performance of its special powers functions. The legislation requires ASIO to notify the IGIS as soon as practicable after an authority is given. All SIOs approved during the reporting period were notified to the Inspector-General within 24 hours of approval being granted by the Attorney-General.

The legislation also requires ASIO to provide a written report on each SIO to the Attorney-General and the IGIS. As the details of SIOs are highly sensitive and cannot be included in a public report it is not possible to give more information about the operations here. However, during the reporting period one propriety issue was raised concerning the interim report for a particular SIO; this matter was addressed in the final report to the Attorney-General. No other substantive issues or concerns were identified when reviewing these activities.

Under the provisions of Division 4 of the ASIO Act, SIOs can be varied or cancelled but the Act does not require ASIO to inform SIO participants of a variation or cancellation. During 2018-19 the office identified several instances where special intelligence operations were varied, but participants were not formally advised in a timely manner of a change to their immunity under the SIO authority. As a result, ASIO revised its procedures to ensure that participants are informed in a timely manner of any change to their immunity under an SIO authority.

NEW POWERS UNDER THE TELECOMMUNICATIONS ACT 1997

During 2018-19, ASIO was granted new powers under the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*. ASIO proactively briefed the office on its use of these powers and formally notified the Inspector-General within seven days of a notice being given where required by legislation. The office intends to review each use of these powers as part of the inspection program for the next financial year.

THE ATTORNEY-GENERAL'S GUIDELINES

The Attorney-General's Guidelines (the Guidelines) are issued under section 8A of the ASIO Act and are to be observed by ASIO in the performance of its functions.

The Guidelines require that the initiation of an ASIO investigation be authorised by a senior ASIO officer. IGIS staff identified a small number of instances in which investigative activities were undertaken without first obtaining the proper authorisations required by the Guidelines, however this was not assessed to be a systemic issue.

The Guidelines also require ASIO to review each of ASIO's investigations on an annual basis. In 2018-19 a small number of investigations were conducted without review for periods longer than a year. ASIO proactively reported the majority of these breaches to the Inspector-General.

SUBJECT OF SECURITY INVESTIGATION SUBSEQUENTLY DETERMINED TO BE NOT RELEVANT TO SECURITY

ASIO reported one incident where a person (Person A) was placed under investigation, based on reporting alleging that a person with similar biographical details to Person A was involved with a terrorist organisation. ASIO's investigation subsequently determined that Person A was not the subject of this reporting; rather, the subject was a different person (Person B) whose biographical details were substantially similar to those of Person A. ASIO promptly ceased the investigation into Person A and recorded in its systems that Person A was not relevant to security. ASIO also deleted all other information that had been collected on Person A and proactively notified this office of the incident.

In a similar but separate incident, ASIO conducted an investigation into a person (Person C) but collected telecommunications data on another person (Person D) with similar biographical details to Person C. The checks used biographical information derived from historical intelligence reporting; when the telecommunications data was analysed it was determined the historical reporting was inaccurate and that the data did not relate to the subject of the investigation. Investigative activities that did not rely on this incorrect reporting were always targeted correctly towards Person C. Upon detecting the error, ASIO updated its records, deleted all information that related to Person D, and notified the office of the incident.

The IGIS considers that ASIO's actions in these cases were lawful and proper. It is inevitable that intelligence agencies, frequently working with incomplete information under significant pressure, will occasionally draw incorrect conclusions and will be forced to amend them as new information comes to light. ASIO's response in these matters is a positive demonstration of how agencies, acting transparently and accountably, can preserve the privacy of individuals who are inadvertently affected by such errors.

ASIO'S EXCHANGE OF INFORMATION WITH AUSTRALIAN GOVERNMENT AGENCIES

ASIO's interactions with other Australian Government agencies include the exchange of information. Exchanges of sensitive personal information are of particular interest to the IGIS, and are subject to IGIS staff review as part of periodic inspections.

During the reporting period, ASIO exchanged information with a number of Australian Government agencies including the Australian Criminal Intelligence Commission, Australian Federal Police, State and Territory police services, the Department of Home Affairs, the Department of Defence and the Department of Foreign Affairs and Trade. Regular inspection activity included reviewing these exchanges to assess ASIO's compliance with legislation, the Attorney-General's Guidelines and ASIO policy. No specific concerns were identified during these inspections.

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 information is further governed by a memorandum of understanding 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 staff reviewed ASIO's access to sensitive tax information carried over from the previous financial year. No issues of concern were identified in this inspection. The office will review ASIO's access to taxation information for the 2018-19 period later this year and will report the findings in next year's annual report.

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 the Minister. ASIO has guidelines for the communication of information on Australians and foreign nationals to approved foreign authorities.

ASIO advised of one incident in 2018-19 where a breakdown in process resulted in information relating to Australian citizens being disclosed to a foreign service without sufficient authorisation as required by ASIO internal policy. Appropriate approval was subsequently retrospectively granted and additional procedures for foreign disclosure were implemented to prevent a reoccurrence.

MINISTERIAL SUBMISSIONS

In 2018-19 IGIS staff reviewed a range of submissions to the Attorney-General and Minister for Home Affairs. These reviews continue to be useful in obtaining an overview of legality and propriety issues, and to keep the Inspector-General informed of current operations and emerging issues.

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. Similar to previous years, in 2018-19 IGIS staff reviewed a sample of cases where ASIO issued prejudicial (adverse or qualified) security assessments.

BREACHES OF S 38 OF THE ASIO ACT BY OTHER COMMONWEALTH DEPARTMENTS

In certain circumstances, section 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 written notice to the person, including a copy of the assessment and information concerning the person's right of appeal to the Administrative Appeals Tribunal, within 14 days.



During the reporting period, ASIO advised the office of four cases where a Commonwealth department failed to furnish the relevant information within the time period required by section 38(1). ASIO also advised of one case where another Commonwealth department failed to furnish the relevant information within the time period required by section 38(1).

The office is satisfied that ASIO's actions in relation to these five cases were lawful and proper. During the reporting period the IGIS did not ordinarily have jurisdiction to review the actions of either of the two departments involved and no further inquiries with either department were made in relation to these cases.

INABILITY TO ACCESS INDEPENDENT REVIEWER OF ADVERSE SECURITY ASSESSMENTS

The office of the Independent Reviewer of Adverse Security Assessments fell vacant in September 2018. Mr Robert Cornall AO was subsequently reappointed as Independent Reviewer by the Attorney-General in March 2019.

During the reporting period, ASIO notified IGIS of at least one subject of an adverse security assessment who was eligible to request review by the Independent Reviewer but could not do so while the office was vacant. ASIO continued to update IGIS in relation to the impact of the vacancy until Mr Cornall was reappointed.

DELAYS IN FINALISING SECURITY ASSESSMENTS

In 2017-18 IGIS reported on a security assessment that had been subject to significant delay but was unresolved at the time of the annual report. This case was finalised in 2018-19.

ASIO INSPECTION PROJECTS

In November 2016, the Inspector-General initiated an inspection project focusing on ASIO staff access to surveillance devices and other technical devices used for surveillance. This project was suspended in 2017-18 due to higher priority inspection activities and staffing shortages in this office. It was later reactivated in October 2018 and then finalised in June 2019.

The project considered the risk that devices maintained by ASIO could be misused for unauthorised purposes, and examined whether accountability measures and other risk controls adequately address this risk. The project was not initiated in response to any incident, but instead sought to provide proactive assurance that foreseeable risks of improper or illegal activity are appropriately managed by ASIO.

The office has concluded that the inherent risk of ASIO devices being misused for unauthorised purposes is low due to the complementary effect of risk controls that primarily address operational security and financial accountability risks. However, the project identified opportunities for ASIO to better manage this risk, in particular by ensuring that controls relevant to the risk of unauthorised misuse are clearly established in associated policies and procedures, and that these policies and procedures are easily accessed and applied by staff working with such devices. The office will periodically revisit this issue in the course of our regular inspection program of ASIO activities in 2019-20.

PROTECTING COMPLAINANT INFORMATION

In 2011 ASIO and the Inspector-General agreed on a protocol for the management of information concerning complaints or public interest disclosures made to IGIS. This protocol provides guidance for ASIO's management of lawfully intercepted communications which identify, or potentially identify, a person who has made a complaint or public interest disclosure to this office.

In last year's annual report, the office noted that ASIO was updating the protocol but that its review was not yet finalised. In consultation with IGIS, ASIO finalised the revised protocol and supporting policies and procedures in 2018-19.

INSPECTION OF ASIS ACTIVITIES

The Inspector-General's oversight of ASIS's activities falls into eight categories, which are based on the underlying functions of ASIS as set out in section 6(1) of the *Intelligence Services Act 2001* (ISA). These categories are:

- foreign intelligence collection;
- intelligence communication;
- assistance to the Australian Defence Force;
- counter intelligence;
- foreign liaison;
- cooperation and assistance to certain intelligence agencies and prescribed authorities;
- actions undertaken in relation to ASIO; and
- other activities as the Minister for Foreign Affairs directs.

IGIS staff conducted a range of regular inspections of ASIS activities covering all the agency's functions. These inspections included reviewing: operational files, advice to the Minister for Foreign Affairs, weapons-related matters, and access to sensitive financial information. Inspection activities were conducted using a risk-based approach with priority given to operational file reviews.

This office also conducts other review and oversight related activity apart from inspections and inquiries. These other activities are an important part of the IGIS's oversight of ASIS, and provide additional assurance that ASIS's activities are legal and proper. Examples of such activities include reviewing ASIS reporting provided to this office on legislative non-compliance or other significant matters; being consulted on the legality and propriety of certain proposals and draft internal policies prior to finalisation, which allows the office to identify any concerns before action is taken; and engaging in visits to ASIS officers outside of its Canberra headquarters.

These inspections and other review activities are supplemented by awareness briefings on various matters throughout the year that either this office requests, or are provided proactively by ASIS. These briefings allow the office to stay abreast of emerging issues, or to follow up on observations from inspection activities. There are also regular bi-monthly meetings between the Inspector-General and senior ASIS officers that cover a range of

different matters, and during 2018–19 the Inspector-General also presented to a gathering of all ASIS senior staff.

REVIEW OF OPERATIONAL FILES

IGIS staff visited ASIS premises on a regular basis during 2018-19 to review ASIS's operational case files. Generally these inspections occur monthly, however IGIS staff did not conduct an operational file inspection in each month during the financial year because the ASIS Inquiry in late 2018 was a higher priority for staffing.

Inspections of operational files involve reviewing a sample of files, focusing on higher risk areas as determined by the IGIS office. Considerations applied in the inspections include the appropriate application of the Privacy Rules, and consideration of how ASIS assesses and manages human rights matters. ASIS activities involve the use of human sources and ASIS officers are deployed in many countries to support a wide range of activities including counter terrorism, efforts against people smuggling and support to military operations. These activities are sensitive, and may be high-risk.

During the reporting period this office reviewed files relating to ASIS's operational activities in a number of diverse countries. These inspections provide a deep insight into the operational environment in which field staff operate as well as the extent to which staff in ASIS headquarters evaluate risk and guide sensitive activities, and often indicates the health of inter-agency relations. These inspections typically focus on records created in the previous two years for a given station, source or operation. However, inspections may examine older matters when required. During the reporting period IGIS staff conducted a historical review of ASIS files relating to allegations of improper conduct by ASIS that occurred over ten years ago. That inspection did not identify any legality or propriety concerns.

The sensitive nature of ASIS's operational activities means that specific detail of the topics inspected and matters identified cannot be provided in a public report. Overall, IGIS staff were satisfied with ASIS's operational activities and that ASIS staff are appropriately identifying and considering risks associated with these activities. ASIS staff display high levels of awareness on how to handle possible incidents of torture and other cruel, inhumane or degrading treatment; ASIS's management and record keeping in such cases was appropriate. Where IGIS staff identified areas for further investigation, ASIS was forthcoming in providing additional information or briefing this office, leading to constructive discussions to identify the compliance risks and subsequent mitigation strategies to ensure ASIS activities remain appropriate and consistent with legislation.

MINISTERIAL SUBMISSIONS

IGIS staff review all ministerial submissions provided by ASIS to the Minister for Foreign Affairs as part of a bi-monthly inspection activity. The majority of the submissions reviewed relate to ministerial authorisations (discussed below), however reviewing all submissions allows the office to consider whether the Minister is appropriately informed about ASIS matters. Overall, IGIS staff were satisfied that the information provided to the Minister was appropriate.

MINISTERIAL AUTHORISATIONS TO PRODUCE INTELLIGENCE ON AUSTRALIAN PERSONS

ASIS is a foreign intelligence agency and any intelligence activity it conducts on an Australian person is a key focus area for this office. In 2018-19, IGIS staff reviewed all ministerial authorisations obtained by ASIS from the Minister for Foreign Affairs. There were three cases where ASIS did not report to the Minister for Foreign Affairs within three months of the day on which an authorisation ceased to have effect as required under section 10A(2) of the ISA. This was due to internal administrative delays and human error. While IGIS staff identified two of the cases during inspection activities, in all three cases ASIS had independently identified these incidents and subsequently reported these to this office.

IGIS inspections also identified nine authorisations that were compliant with the ISA but non-compliant with ASIS's own internal procedures. Specifically, these procedures require that the Minister for Foreign Affairs be informed promptly once the Attorney-General has agreed that the subject of an authorisation request is likely a threat to security. ASIS undertook to remind relevant staff of this requirement; the office was satisfied with this response but will continue to review authorisations in relation to all aspects of compliance.

EMERGENCY MINISTERIAL AUTHORISATIONS

There was one instance where ASIS sought an oral authorisation from the Minister for Foreign Affairs in an emergency using the section 9A provisions in the ISA. A written record of the oral authorisation was made within 48 hours and a copy of the record was provided to this office within three days in accordance with section 9A(5) of the ISA. The authorisation raised no concerns for this office.

REPORTING OF COMPLIANCE MATTERS

When the ASIS Compliance Branch identifies a matter of concern, or when an ASIS officer self reports an issue relating to compliance or propriety, ASIS provides written notification of the matter to this office. These reports may relate to non-compliance with legislation, non-compliance with ASIS internal policies and procedures, or could merely record an event that was investigated but determined to be compliant with the law and internal policy. Such reports are an important element of the oversight arrangements between IGIS and ASIS.

While ASIS investigates the matter, IGIS does not normally conduct its own parallel review while awaiting the findings. As part of its investigation, ASIS will initiate remediation where required; this can include issuing corrections to reporting and additional training for the staff and teams involved. This office reviews all of ASIS's investigation reports and undertakes its own independent review of incidents where necessary.

During the reporting period, ASIS provided this office with three reports which involved activities not conducted in accordance with section 10A(2) of the ISA, as mentioned above in the 'Ministerial Authorisations to produce intelligence on Australian persons' section. An additional nine reports provided by ASIS related to the non-application of the Privacy Rules, which are discussed below.

PROTECTING THE PRIVACY OF AUSTRALIAN PERSONS

On 28 March 2019, the Minister for Foreign Affairs signed ASIS's new Privacy Rules, in accordance with section 15 of the ISA, and the Rules took effect on 9 May 2019. As required by section 15(6) of the ISA, on 4 April 2019 the Inspector-General briefed the Parliamentary Joint Committee on Intelligence and Security on the content and effect of ASIS's new Privacy Rules.

The Inspector-General was consulted on the proposed changes and is satisfied that the new Rules protect the privacy of Australian persons. The amendments to the ASIS Privacy Rules largely seek to bring the Rules in line with the ISA and the Australian Privacy Principles (APPs). Adopting similar terminology and phrasing across the APPs, Rules and the ISA aims to assist the interpretation and application of the Rules. The amendments also intend to provide practical changes and clarify certain Rules, while preserving the privacy of Australian persons. IGIS staff pay close attention to the distribution of intelligence about Australian persons by ASIS during regular inspection activities. ASIS continued to provide training to its staff on producing intelligence on Australian persons and introduced initiatives to mitigate against the risk of unintentionally reporting on Australian persons.

Compared to last year, in 2018–19 there was a small increase in the number of instances where ASIS did not apply the Privacy Rules prior to reporting on an Australian person. Nine of these matters were identified and reported to this office by ASIS, and two were identified by this office. Such cases are not in accordance with section 15(5) of the ISA. Some of these breaches occurred earlier than 2018–19, but were identified by ASIS during the reporting period. These incidents represent a very small proportion of the total reporting ASIS produced on Australian persons during 2018–19. All cases were due to combinations of human error and problems associated with an aging IT system. This office found no instances where reporting on an Australian person would not have been reasonable and proper had the Privacy Rules been applied at the time. Separately, there were other occasions where this office identified areas for improvement in ASIS's recordkeeping with respect to the Privacy Rules. IGIS staff will continue to pay close attention to the application of the Privacy Rules by ASIS.

ASIS reported two occasions in 2018–19 where a 'presumption of nationality' was overturned; that is, information became known that an individual previously presumed to be foreign was actually an Australian person. These incidents are required to be reported to the IGIS under the ASIS Privacy Rules. In both cases ASIS's initial presumption was reasonable and in accordance with Privacy Rule 1 as, at the time, there was no evidence that the individuals, located outside of Australia, were Australian.

The office's review of one of these cases identified delays in ASIS overturning the presumption once the information was available; specifically, there was a six week delay between an ASIS officer learning that an individual might be an Australian and checks being conducted to confirm the individual's nationality. Seven weeks then passed between ASIS confirming the individual was an Australian citizen, notifying parts of the Australian Intelligence Community (AIC) of this fact, and following internal processes to remedy the non-application of the Privacy Rules. Where ASIS believes that an individual might be an Australian person, checks to confirm the individual's nationality must occur promptly to ensure legal and policy requirements are met. If, based on these checks, ASIS becomes satisfied that an individual is an Australian person and overturns the presumption of nationality, it would be proper for ASIS to share this information with other AIC agencies as soon as practicable. This was an isolated case and did not reveal any systemic problems.

AUTHORISATIONS RELATING TO THE USE OF WEAPONS

The ISA prevents ASIS officers from undertaking activities that involve violence or the use of weapons. However, the Act allows ASIS to provide its officers with weapons, and to train officers to use weapons and self-defence techniques in certain circumstances, particularly in order to protect themselves or certain other people. In December 2018, provisions of the ISA relating to the use of force and weapons were amended to enable the Minister to specify additional persons outside Australia who may be protected by an ASIS staff member or agent, and allowed ASIS staff members or agents performing specified activities outside Australia to use reasonable and necessary force in the performance of an ASIS function. The Inspector-General was consulted on these changes in a detailed and cooperative manner, and suggestions made during this consultation were accepted by ASIS.

Schedules 2 and 3 of the ISA require that the Minister and Director-General provide certain documentation to this office related to the use of force and weapons, including approvals for weapons and self-defence training; copies of 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 if officers or agents use weapons or self-defence techniques other than in training or approved scenarios.

In the 2018-19 reporting period the Minister and Director-General of ASIS provided relevant reports required under the ISA. The Inspector-General continues to be satisfied that the need for a limited number of ASIS staff to have access to weapons for self-defence in order to perform their duties is genuine. ASIS did not report any cases where a weapon was discharged or self-defence techniques were used other than in training, nor any instances of non-compliance with internal weapons guidelines issued by the Director-General of ASIS. As at 30 June 2019 the Director-General of ASIS had not issued any new or updated guidelines relating to the use of weapons and self-defence techniques, including the use of force or threats of the use of force. In one case the Minister provided an approval for certain ASIS staff members to protect a number of persons under Schedule 2, Clause 1(3) of the ISA.

The IGIS office also examined ASIS weapons and self-defence policies, guidelines and training records during an inspection, and did not identify any issues of concern.



INSPECTION OF ASD ACTIVITIES

ASD's activities subject to the office's oversight are categorised according to the underlying functions of the agency as set out in section 7 of the ISA, namely:

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

In the 2018-19 reporting period IGIS staff met the target of inspecting at least 75% of these categories.

IGIS inspection of ASD activities is assisted by strong working-level 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 ASD's existing and proposed policies to ensure they are appropriate and effective.

During 2018-19, the office inspected a number of ASD activities, including:

- applications for ministerial authorisation to produce intelligence on Australian persons;
- ASD's compliance with the ASD Privacy Rules;
- compliance incident reports; and
- ASD's access to sensitive financial information.

These inspections were supplemented by briefings on various matters across the year, regular meetings with the ASD Oversight and Compliance teams, engagement with ASD Legal staff, and visits to ASD staff posted outside Canberra. The Inspector-General and the Director-General of ASD meet formally on a quarterly basis to discuss oversight matters and developments.

The office also commenced two targeted inspection projects during the reporting period on ASD's use and management of certain warrants under the TIA Act, and ASD's compliance with particular administrative arrangements it has in place with the Australian Defence Force. These have been finalised and no systemic issues or concerns have been identified to date.

MINISTERIAL AUTHORISATIONS

The ISA requires ASD to obtain authorisation from the Minister for Defence before conducting certain activities, including the production of intelligence on Australian persons. During 2018-19 the office inspected over 96% of the applications made by ASD for ministerial authorisation, an increase on the approximately 80% reviewed in the last reporting period. The submissions were generally of a high standard, and no significant issues were identified.

However, IGIS staff did identify several instances during the reporting period where ASD did not display appropriate administrative restrictions on certain database records. These lapses heightened the risk of an inadvertent breach of the ISA by omitting a layer of additional administrative assurance. ASD's response to feedback on this issue was positive and IGIS staff continue to monitor this aspect of ministerial authorisations and associated records.

Once a ministerial authorisation has expired, ASD is required, within specified timeframes, to provide the Minister with a report on the activities it conducted under the authorisation. IGIS staff reviewed a number of these reports. In one case, ASD failed to provide the Minister with a section 10A report within one month of an emergency ministerial authorisation expiring. ASD investigated this case and reported its findings to the IGIS in a Compliance Incident Report, which is discussed in more detail below.

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, or other select ministers where the Minister for Defence is unavailable. Alternatively the Director-General of ASD can authorise such activities if the ministers are not readily available. Emergency authorisations are only valid for 48 hours after which any further activity will require a new authorisation if ASD is to continue that activity.

Three emergency ministerial authorisations were issued to ASD during the reporting period. IGIS staff reviewed all these applications for authorisation and found no issues of concern with their initial administrative management; however, as noted above, on one occasion ASD did not provide the Minister with a section 10A report within one month of the authorisation ceasing.

MINISTERIAL SUBMISSIONS

During the reporting period IGIS staff conducted a quarterly review of ASD's submissions to the Minister for Defence. The office seeks to ensure the Minister is given timely and accurate information about critical ASD issues. Over this reporting period, IGIS staff found that the submissions were generally of a high standard, and were provided to the Minister within an appropriate time frame. IGIS staff appreciated ASD's consultation with the IGIS office in relation to several submissions.

PROTECTING THE PRIVACY OF AUSTRALIANS

The Minister for Defence issues written rules (the ASD Privacy Rules) to regulate how ASD communicates and retains intelligence information about Australian persons. The ISA prohibits ASD from communicating intelligence information concerning an Australian person otherwise than in accordance with those rules.

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

In accordance with its obligations under the Privacy Rules, ASD reported on cases during the reporting period where ASD had initially presumed in accordance with the guidance set out in the rules that a particular individual was not an Australian person, but where the presumption was subsequently rebutted and the person was shown to be Australian. These reports included details of the measures taken to protect the privacy of that person. IGIS staff reviewed these cases and found that the initial presumptions of nationality were reasonable given the information available to ASD at the time. ASD's actions, including informing other intelligence agencies that the person is Australian, were appropriate and in accordance with the Privacy Rules. The office notes that ASD, as a propriety measure, began to inform second parties of overturned presumptions of nationality in mid-2018. The office acknowledges this extra step that ASD is taking to ensure the privacy of Australian persons is protected.

In July 2018, ASD informed the office that it had communicated intelligence information concerning an Australian person, otherwise than in accordance with the ASD Privacy Rules, thereby contravening the ISA. The incident occurred when ASD conducted intelligence activities without the appropriate authorisation, and conducted a subsequent activity without consideration of the ASD Privacy Rules. This incident is discussed in the section below.

LEGISLATIVE NON-COMPLIANCE

ASD has a strong record of proactive self-reporting to the IGIS where it identifies breaches of legislation and significant or systemic matters of non-compliance with ASD policy. When this occurs, ASD provides written notification to the office, undertakes an investigation of the incident and provides its findings. The office reviews these reports and where necessary undertakes further independent investigation of the incident. ASD takes mitigation and remediation actions where required in consultation with the office.

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. In July 2018, ASD advised this office that it had intercepted communications without a warrant, thereby breaching the TIA Act, and had then communicated the intercepted material, also in breach of the TIA Act. The breach was the result of a system processing error. The office was satisfied with ASD's investigation and the remedial action taken to prevent recurrence.

In May 2019, ASD notified the IGIS office that, on two occasions, ASD may have contravened section 7 of the TIA Act, by enabling interception without the correct warrant. ASD investigated this incident, and in June 2019 confirmed that the activity contravened section 7. As of 30 June 2019, ASD had not yet completed the associated compliance incident report. This office will report independent findings relating to this case in the next annual report.

In June 2019, ASD informed the IGIS office that ASD may have contravened section 7 of the TIA Act by unauthorised interception of a specific type of communication. ASD investigated this incident, and in late June 2019 confirmed that the activity likely contravened the TIA Act. As of 30 June 2019, ASD was still compiling the associated compliance incident report. This office will report independent findings relating to this case in the next annual report.

In addition to these confirmed instances of non-compliance, ASD also advises this office of 'potential breaches' where a breach is technically possible but 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. The IGIS office reviews these matters in the same manner as it reviews compliance incidents. As outlined below, ASD advised IGIS of two potential breaches in the reporting period.

In October 2018, ASD advised this office of a potential breach of section 7 of the TIA Act as a result of the misconfiguration of an ASD system. ASD advised that it was not possible to confirm whether unauthorised communications had actually been intercepted. This office reviewed the incident and considers that ASD potentially breached section 7 and section 63; however, the office notes that ASD acted promptly to inform the IGIS and to rectify the incident. The office is satisfied with the proposed measures for mitigating future risk associated with this matter.

In October 2018, ASD also informed the IGIS office of its investigation into an incident whereby communications were potentially intercepted due to a system error. In December 2018, ASD confirmed its assessment that the incident was not a breach of legislation. This office conducted an independent review of the incident and considers that a component of the collection constituted a potential breach of section 7 of the TIA Act as it cannot be conclusively demonstrated that the suspect interception did not occur. ASD undertook appropriate mitigation measures following this incident.

INTELLIGENCE SERVICES ACT 2001 INCIDENT REPORTS

The ISA requires the Minister for Defence to issue a written direction to ASD requiring ASD to obtain ministerial authorisation before conducting certain activities for the purposes of producing intelligence on an Australian person. The Act requires the Director-General of ASD to ensure that ASD complies with those directions. The ISA also prohibits ASD from communicating intelligence information concerning Australian persons, except in accordance with the ASD Privacy Rules. In July 2018, ASD advised this office of its investigation into a breach of these obligations. The incident occurred when ASD conducted intelligence activities in relation to two Australian persons without obtaining authorisation from the Minister. ASD then further contravened the requirements of the ISA by conducting a subsequent activity without consideration of the ASD Privacy Rules. The combination of human error and a failure to comply with ASD policy contributed to the breaches. This office was satisfied with ASD's investigation and remedial action to prevent recurrence.

In August 2018, ASD advised this office of its investigation into another breach of its ISA obligation to obtain a ministerial authorisation. The breach involved undertaking activity to produce intelligence on an Australian person without obtaining ministerial authorisation to do so. The breach resulted from a failure to consider if there is a purpose to produce intelligence on an Australian person where there is more than one purpose. This office was satisfied with ASD's investigation and remedial action to prevent recurrence.

In January 2019, following queries from this office regarding the status of a report under section 10A of the ISA, ASD confirmed an incident where it had failed to provide a report to the Minister for Defence in relation to activities conducted under an emergency ministerial authorisation. ASD assessed this to be a breach of the reporting requirements set out in section 10A, and sent its final report to the IGIS in March 2019. This office reviewed ASD's investigation and considered the findings to be reasonable, and is satisfied that the remedial actions proposed and implemented by ASD will help to prevent similar errors in the future.

OTHER INCIDENT REPORTS

In late 2018, ASD advised the IGIS of an instance where it had contravened certain legislation. The sensitive nature of ASD's operational activities mean that specific details cannot be included in this report.

INSPECTION OF AGO ACTIVITIES

The activity categories assigned to AGO are derived from AGO's statutory functions under the ISA:

- intelligence collection and other activities in support of the Australian Government;
- intelligence collection in support of the Australian Defence Force;
- 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 certain intelligence agencies and prescribed authorities; and
- the functions of the Australian Hydrographic Office.

During 2018-19, this office achieved the target of inspecting at least 75% of AGO's activity categories. The inspections included:

- applications for ministerial authorisation to produce intelligence on Australian persons;
- Director's approvals and post-activity reporting;
- AGO's compliance with the AGO Privacy Rules; and
- AGO's access to sensitive financial information (discussed later in the report).

The office received briefings from AGO teams in Canberra and Bendigo which enabled IGIS officers to gain a better understanding of the agency's functions and to identify emerging issues. They also assisted this office to enhance working-level relationships within AGO and to follow up on matters observed during inspections. Visits to regional offices enable the office to conduct outreach and inform staff of our role in handling complaints and disclosures.

The Inspector-General held four meetings with the Director of AGO during the reporting period to discuss key issues and arrangements for oversight. The office also engaged with AGO on matters such as the Comprehensive Review of the Legal Framework Governing the National Intelligence Community and amendments to the AGO Ministerial Directions.

Based on inspection and review activities, the office is satisfied that AGO met its statutory obligations under the ISA during the 2018-19 reporting period, and that AGO has established systems and processes to encourage compliance.

MINISTERIAL AUTHORISATIONS TO PRODUCE INTELLIGENCE ON AUSTRALIAN PERSONS

The ISA 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 usually requested in conjunction with ASD. During 2018-19, IGIS reviewed all applications made by AGO for ministerial authorisation. IGIS inspections did not identify any concerns relating to AGO's applications for ministerial authorisation, renewals, or circumstances in which AGO sought to cancel an authorisation. One emergency ministerial authorisation was issued to AGO during the reporting period; IGIS staff reviewed this emergency authorisation and did not identify any issues of concern.

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 during the reporting period by IGIS staff, and no issues were identified.

At the conclusion of approved activities, AGO staff prepare a post-activity compliance report for the Director, which this office examines. During 2018-19, IGIS staff identified no significant issues with these reports. However, one instance was noted of non-compliance with the Ministerial Directions where a Director's Approval was not approved at the appropriate level of delegation. This office subsequently recommended to AGO that it would be prudent to put in place a formal delegation procedure that makes clear the circumstances in which another officer may sign as acting Director. The office is satisfied that AGO has taken appropriate remedial action in response to this matter.

AGO COMPLIANCE WITH PRIVACY RULES

The Minister for Defence issues written rules (the AGO Privacy Rules) to regulate how AGO communicates and retains intelligence information concerning Australian persons. During the 2018-19 reporting period IGIS staff did not identify any concerns in relation to AGO's compliance with the Privacy Rules. This is the third consecutive year in which AGO has been fully compliant with the AGO Privacy Rules.

BENDIGO OFFICE

In May 2019, IGIS staff visited AGO offices in Bendigo, Victoria. This visit enabled the office to learn about the work conducted in Bendigo, including the AGO traineeship program, and to provide briefings to the staff regarding the role and responsibilities of the IGIS office.

AUSTRALIAN HYDROGRAPHIC OFFICE

In October 2017 the Australian Hydrographic Office (AHO) functions were transferred from the Royal Australian Navy to AGO. This transfer meant that the IGIS office 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 ISA requirements into its daily workflows and has received relevant compliance training. However, due to current differences in task tracking and recording in separate systems, this office has not yet reviewed any AHO office products. IGIS staff will conduct outreach and inspections at the Wollongong site once infrastructure upgrades are completed.

INSPECTION OF DIO ACTIVITIES

Inspections of DIO are less frequent than for ASIO, ASIS, ASD and AGO, as the office focuses its limited resources on inspecting and reviewing the activities of the intelligence collection agencies in preference to those of the assessment agencies DIO and ONI.

In this reporting period the office inspection of DIO's activities included following up on matters identified during the inquiry into the analytic independence and integrity of DIO conducted in 2017, as well as routine inspections of DIO's compliance with the *Guidelines to Protect the Privacy of Australian Persons*. IGIS staff also reviewed DIO's access to sensitive financial information from AUSTRAC, which is discussed later in this report.

In addition to these inspection activities, the office attended relevant compliance training run by DIO, and monitored the percentage of DIO staff that have completed mandatory compliance training requirements.

COMPLIANCE WITH DIO'S PRIVACY GUIDELINES

DIO's compliance with its Privacy Guidelines was reviewed twice during the reporting period by IGIS staff. These guidelines, which are available on the DIO website, are similar to the Privacy Rules established under section 15 of the ISA for ASIS, ASD and AGO. They allow DIO to perform its role while protecting the privacy of Australians. This office did not identify any significant issues or concerns in this reporting period, and there was no evidence that DIO breached the Privacy Guidelines.

INSPECTION AND REVIEW OF ONA AND ONI ACTIVITIES

During 2018-19 this office had oversight of the Office of National Assessments (ONA) which subsequently became the Office of National Intelligence (ONI). ONI was established on 20 December 2018 following the passage of the *Office of National Intelligence Act 2018* (ONI Act), and was established to provide Government with a better coordinated and more integrated intelligence community. It subsumed the role, functions and staff of ONA. ONI is responsible for enterprise level management of the National Intelligence Community. It also produces all-source intelligence assessments for government and maintains the Open Source Centre; it is these functions that are of particular interest for the inspection and review activities of this office.

The *Office of National Intelligence Rules to Protect the Privacy of Australians* (the ONI Privacy Rules) were made by the Prime Minister in accordance with section 53 of the ONI Act; the Rules replaced the Privacy Guidelines in place for ONA. Given the focus on the development of the Rules, IGIS staff undertook one less on-site inspection than usual of ONA's application of the Privacy Guidelines.

The functions of ONI, and formerly ONA, mean that it is less likely than intelligence collection agencies to intrude on the privacy of Australian persons or operate in breach of legislation. As such the office made fewer inspections of ONA and ONI compared to the intelligence collection agencies. ONA had three broad statutory functions, whereas ONI has 11 different functions under the ONI Act. This office did not meet the target of inspecting at least 75% of ONA's or ONI's activity categories; however not all of ONI's functions were a focus for this office during the reporting period. For this financial year, IGIS staff focused on the areas considered to be of highest risk, namely ONI's implementation of the new ONI Privacy Rules and the associated policies and guidelines. This office will continue to review its approach to ONI inspection and review activity to ensure it focuses on key areas of legality and propriety risks.

COMPLIANCE WITH THE PRIVACY RULES

On 18 December 2018, the Prime Minister signed the ONI Privacy Rules. ONI published the Rules on its website as required by section 53(4A) of the ONI Act. In accordance with section 53(6) of the ONI Act, the Inspector-General provided a brief to the PJCS on the content and effect of the Rules. This office was consulted extensively in the preparation of the ONI Privacy Rules and the Inspector-General is satisfied that the Rules protect the privacy of Australian persons. The Inspector-General also had relevant discussions with the Privacy Commissioner during the consultation period.



IGIS staff focused on the distribution of information about Australian persons during the inspection of ONI. The ONI Privacy Rules require that it only retain or communicate information about an Australian person where it is necessary to do so for the proper performance of ONI's functions, or where retention or communication is authorised or required under another Act. ONI must advise this office if it identifies a breach of the Rules, and include information about the measures taken to protect the privacy of the affected Australian person, or of Australian persons more generally. Adherence to this reporting requirement provides the office with sufficient information upon which to decide whether appropriate remedial action has been taken, or further investigation and reporting back to the IGIS is required. No breaches were reported to our office by ONI.

The office's one on-site inspection during 2018-19 did not identify any breaches of the Privacy Rules, and the majority of ONI's records reviewed were of a high standard. The inspection did identify some minor areas where ONI could improve its compliance with relevant ONI policy. During the inspection IGIS staff were also briefed on activities of ONI's Open Source Centre, ONI's progress in establishing a framework to use assumed identities, and other matters.

CROSS-AGENCY INSPECTION MATTERS

During the reporting period this office 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 and ASIS 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. In December 2018, the *Crimes Act 1914* was amended to extend authority to acquire and use assumed identities to ONI.

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 section 15LE requires that each agency provide the Inspector-General with an annual report containing information on the assumed identities created and used during the year. During 2018-19 the Director-General of Security and the Director-General of ASIS each provided this office with a report covering the activities of their respective agencies for the 2017-18 reporting period. There was nothing in the reports to suggest that ASIO or ASIS were not complying with their legislative responsibilities or which otherwise caused concern. ONI was not required to submit a report for 2017-18. Agency reports covering the period 2018-19 will be submitted during 2019-20.

ACCESS TO SENSITIVE FINANCIAL INFORMATION BY INTELLIGENCE AGENCIES

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the AML/CTF Act) provides a legal framework in which designated agencies are able to access and share financial intelligence information created or held by the Australian Transaction Reports and Analysis Centre (AUSTRAC). All intelligence agencies and IGIS are designated agencies for the purposes of the AML/CTF Act.

The IGIS is party to a memorandum of understanding (MOU) with AUSTRAC. This MOU establishes 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, the office checks that there is a demonstrated intelligence purpose pertinent to the agencies' functions, that access is appropriately limited, searches are focused, and the passage of information to both Australian agencies and foreign intelligence counterparts is correctly authorised. In 2018-19, as in previous years, the Inspector-General 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.

During 2018-19, the office inspected ASIO's use of AUSTRAC material during 2017-18 and identified multiple breaches of section 133 of the AML/CTF Act. These breaches were consistent with the findings of an earlier ASIO internal review (conducted during 2017-18) that identified systemic deficiencies in ASIO's compliance with the requirements of the AML/CTF Act and ASIO's MOU with AUSTRAC. Additional detail about this review and the identified deficiencies can be found in the IGIS annual report for 2017-18. As reported last year, the ASIO internal review prompted measures to address these deficiencies and the office saw some evidence in 2018-19 that these measures are improving ASIO's handling of AUSTRAC material. In particular, the office noted an improvement in ASIO officers' understanding of the procedural requirements for the communication of AUSTRAC information, however, the quality of record-keeping related to the dissemination of AUSTRAC information remains inconsistent.

In 2018-19 the office conducted a specific inspection of ASIS records concerning AUSTRAC information, as well as incidentally reviewing ASIS's use of AUSTRAC material during inspections of operational files throughout the year. The inspections found that ASIS's governance and record-keeping in relation to AUSTRAC information continued to be effective.

Inspections of ASD, AGO and DIO relating to AUSTRAC information did not reveal any issues of concern. There were no instances of non-compliance by ASD, AGO and DIO regarding 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 with regard to handling of this information.



The office reviewed ONI's use of AUSTRAC material and found that, overall, ONI's governance and record-keeping continued to be effective. ONI self-reported an issue where AUSTRAC was disseminating reports to an ONI email distribution list containing individuals not authorised to receive the reports. This activity did not constitute a breach of the AML/CTF Act as, in accordance with section 121(3)(b) of the Act, staff of AUSTRAC are able to disclose product to ONI staff to assist in the performance of their duties.

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 for Australia's intelligence bodies. One recommendation of that Review is that the jurisdiction of the IGIS be expanded to include the intelligence functions of the Australian Criminal Intelligence Commission (ACIC), Australian Federal Police (AFP), AUSTRAC and the Department of Home Affairs. The Government has allocated additional funding to this office since 2017-18 to implement this recommendation, however expansion of IGIS jurisdiction will require amendments to the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act). The timing and final form of any amendments is a matter for the Government and the Parliament, however, in anticipation of some expansion of jurisdiction the office has commenced planning and preparation for these new responsibilities.

OUTREACH ACTIVITIES

During 2018-2019 the office continued engagement with key contacts and senior managers within ACIC, AFP, AUSTRAC and the Department of Home Affairs to assist this office in developing 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 briefings at the agency, branch and team level as well as specific operational briefings, capability briefings and regional visits. IGIS staff have attended agency induction programs as well as training specific to intelligence areas within the agencies. Additionally, IGIS is placing staff with the agencies to build a more detailed and practical understanding of the agencies' intelligence functions and the internal policies and procedures that support those functions.

Outreach activities conducted by the office during this period have also focused on explaining the role of the Inspector-General and the office's approach to the role, including through all-staff briefings by the Inspector-General and IGIS staff briefings to line areas.

INTERIM INSPECTION PLANS

While the final form and timing of any expanded jurisdiction of the office remains a matter for the Government and Parliament, this office has continued to build the relationships and understanding of agency activities and is developing interim inspection plans accordingly. The IGIS is well placed to have interim inspection plans for the intelligence functions of ACIC, AFP, AUSTRAC, and the Department of Home Affairs by the time the relevant amendments commence.



OBJECTIVE 4 – COMPLAINTS

ABOUT COMPLAINTS

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

The office 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 of an intelligence agency within the jurisdiction of the office. 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 public interest disclosure (PID) 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 staff 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 the office is given advice about actions taken in response to their concerns and the outcomes, to the extent possible within the security obligations of this office.

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%)	VISA/CITIZENSHIP-RELATED COMPLAINTS RESOLVED WITHIN TWO WEEKS (TARGET: 85%)
Visa/citizenship-related	750	97%	93%
Other IGIS Act complaints	29	93%	n/a
Public Interest Disclosures	5	100%	n/a
TOTAL	784	97%	93%

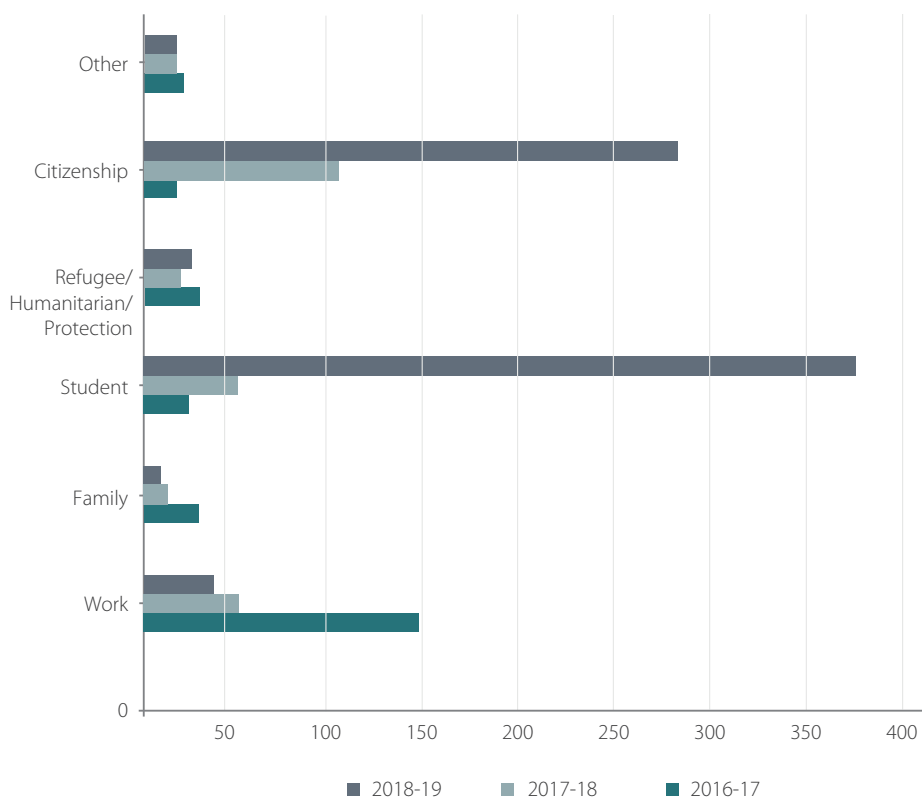


COMPLAINTS ABOUT VISA AND CITIZENSHIP APPLICATIONS

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 has the role of reviewing these actions to ensure they are legal and meet the required propriety standard.

In 2018-19, the office received 750 complaints about visa or citizenship applications, nearly triple the number of similar complaints (279 visa or citizenship complaints) in 2017-18. In 2018-19, the average number of visa or citizenship complaints received per month was 63, compared to an average of 23 complaints per month in 2017-18, 21 complaints per month in 2016-17 and 10 complaints per month in 2015-16.

Figure 2.3: visa/citizenship complaint trends 2016-17 to 2018-19





In 2017-18, the largest number of complaints made to this office related to delays in citizenship applications, accounting for approximately 37% of all visa and citizenship-related complaints. As signalled in last year's report, staff from the office explored the reason for this trend in 2018-19, including meeting regularly with the Office of the Commonwealth Ombudsman to develop an understanding of the issue beyond the confines of IGIS jurisdiction. For almost every citizenship case reviewed by the office in 2018-19, the office was able to determine that no Australian intelligence agency was the cause of delay in processing the application. In 2018-19 the largest number of complaints related to student visas, accounting for half of all visa and citizenship-related complaints, compared to 22% the previous year.

The number of complaints received from individuals seeking skilled business or work visas continued to decline. There was a 53% increase (from 15 to 23) in complaints received about protection and refugee visa applications.

The most frequent complaint about visa and citizenship applications continues to be the length of time taken to finalise an application beyond the indicative timeframes listed on the Department of Home Affairs' website.

In 2018-19 the Inspector-General extended the minimum time that must pass before the office will inquire into a visa or citizenship application in response to a complaint. In 2017-18, the office would only take action in relation to applications for citizenship and permanent visas that were lodged more than 12 months prior, and temporary visas lodged more than three months prior. The experience of the office in 2018-19 has been that these timeframes are resulting in reviews that are premature. In the ordinary course of events complaints to the office about visa or citizenship applications are not generally affected by issues of legality or propriety within an Australian intelligence agency within these time periods, and most cases reviewed by the office within these timeframes will not be resolved for a further several months. For these reasons, and in light of the significant increase in complaint volumes, the office will now only take action on a citizenship complaint when two years have passed since the citizenship application was lodged with the Department of Home Affairs. In the case of visa applications, the office will review complaints for permanent visas, student visas and temporary activity visas when six months have passed since the application was lodged, or three months since the application was lodged for any other temporary visa class.

During the reporting period, 97% of visa and citizenship-related complaints received by the office were acknowledged within five working days, well above the office's performance indicator of 90%. Of the visa and citizenship complaints received in 2018-19, 93% were resolved within 14 days of receipt, also well above our target of 85%. The office considers a complaint about a delay in visa or citizenship security assessments to be resolved once IGIS staff have completed consideration of the complaint and responded to the complainant.





CASE STUDY 1: UNDUE DELAY IN FINALISING A VISA APPLICATION

The Department of Home Affairs may request ASIO to make a security assessment or provide advice in support of the visa process. It is not possible to predict how long it will take to complete a security assessment. In a number of cases, this office found that some processes for following up requests for information contributed to delays in finalising assessments. This office has not identified any illegality or impropriety in the processes. Nevertheless, IGIS has noted the impact of the delay on applicants and has requested that delays be addressed.

OTHER COMPLAINTS MADE UNDER THE IGIS ACT

The office received 29 non-visa/citizenship-related complaints in the reporting period (excluding PID matters), continuing a downward trend since the 2016-17 reporting period. Ten complaints received in 2017-18 were carried into the 2018-19 reporting period, while at the end of 2018-19 one complaint remained open. The average time taken to acknowledge these complaints was three business days. IGIS staff responded to 93% of such complaints within five business days, exceeding the performance measure of 90%.

Figure 2.4: Other complaint statistics 2016-17 to 2018-19

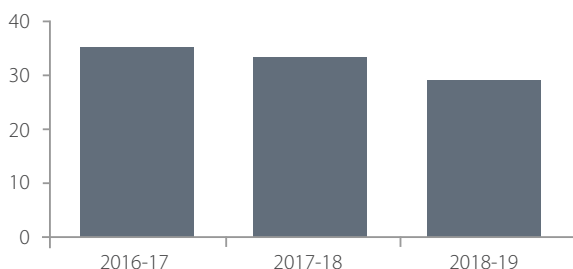


Figure 2.5: Other complaint trends 2018-19

ALLEGATIONS	ASIO	ASIS	ASD
Communication issues	2	0	0
Delay – security assessment	11	0	0
Detriment to member of public arising from agency action	2	0	1
Employment – internal security	1	1	2
Employment – management action	1	0	1
Legality	2	1	1
Harassment	3	0	0

During the reporting period, we sought agency information about 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 the complaint. IGIS staff have established effective relationships with agency staff which ensures most matters are able to be resolved efficiently. Where complex issues are identified, discussions are constructive.

On finalisation, all complainants were given advice about the action the office had taken in response to their complaints, our consideration of agency briefings and records, and how any concerns were resolved. Where appropriate, complainants were also invited to contact the office again if their concerns persisted.

The majority of complaints (22) were about ASIO, while five were about ASD and two concerned ASIS. No complaints were received concerning AGO, DIO or ONI.

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

- security assessments for employment;
- recruitment irregularities;
- obstruction in obtaining software certification; and
- harassment.

Half of the 22 complaints about ASIO concerned delay in security assessments for security clearances required for employment in Australian Government agencies or for an Aviation Security Identification Card. ASIO information revealed that, of the 11 complaints about delay, five concerned cases that did not meet the criteria for priority assessment and had not progressed faster due to competing priorities. No concerns were identified as to the legality or propriety of any ASIO action, and this office does not interfere with the assessment itself or comment on agency resourcing decisions. Where complainants advised their work was affected by the delay, IGIS staff suggested alternative action for complainants to take, such as seeking prioritisation through their employer and the Australian Government Security Vetting Agency (AGSVA).

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 this office. Understandably this may leave complainants dissatisfied with the complaint process even where everything possible has been done. It should be noted that few complainants contact the office to report either satisfaction or disappointment with the outcome of their complaints. Where IGIS staff are aware that an issue remains unresolved when a complaint is closed, IGIS staff may monitor agencies' actions through the office's inspection program. In all cases, the office provides advice about its role, and the role and functions of relevant Australian intelligence agencies. Where the concerns raised are outside the office's jurisdiction, IGIS staff provide details of alternative avenues that might be pursued, if this is appropriate.

CASE STUDIES 2 AND 3: COMMUNICATION ISSUES

CIRCUIT BREAKER

A lawyer complained on behalf of an asylum seeker in detention. Correspondence from the Department of Home Affairs and ASIO had given the asylum seeker conflicting advice about which agency was responsible for telling him the outcome of his ASIO security assessment. IGIS staff sought ASIO advice about the matter and it appeared ASIO understood, wrongly as it happened, that the Department of Home Affairs would notify the individual of the outcome. The result was that neither agency had informed him of the non-prejudicial outcome of the assessment which had been issued more than a year before the complaint was made. IGIS staff subsequently advised the lawyer for the asylum seeker the outcome of ASIO's security assessment.

DATABASE ERRORS AND AN APOLOGY

A member of the public complained of irregularities in an ASIO recruitment process. Following inquiries from the office, ASIO identified a database error which had resulted in no written advice being sent to the complainant concerning the outcome of a 2018 recruitment process. The same database error also led to ASIO giving incorrect verbal advice to the complainant. ASIO corrected the database error and sent a letter of apology to the complainant.

CASE STUDY 4: DEALING WITH DISABILITIES

An individual complained that ASIO had interviewed a member of the public several times without an Auslan interpreter, despite multiple requests for an interpreter to be used.

IGIS staff sought advice from the Australian Human Rights Commission before raising the complaint with ASIO. The IGIS found there were some deficiencies in ASIO's arrangements for ensuring an appropriately independent Auslan interpreter was made available for interviews. However ASIO considered sensitive interviews should be undertaken by a security-cleared interpreter and had difficulty in obtaining one, and the IGIS formed the view that it was for ASIO to decide if the interpreter needed to be security-cleared.

In response to an IGIS recommendation, ASIO agreed not to interview the person again without an interpreter, developed a policy on interviewing people with disabilities to ensure reasonable adjustments are made in future cases, and amended its practice manual to include arrangements for interviewing persons with a disability in compliance with the *Disability Discrimination Act 1992*.



CASE STUDY 5: IMPROVING AGENCY PROCEDURES

A member of the public applied to the Australian Cyber Security Centre (ACSC, a division of ASD) for certification of encryption software and complained to the IGIS about the ACSC's lack of response. The ACSC informed IGIS staff of their prior contact with the individual; the person's emails had been blocked permanently due to their offensive language and threatening conduct towards ACSC staff.

ASD's functions require little interaction with members of the public and the ACSC, which provides a range of services requiring public engagement, was unfamiliar with strategies for managing such problems. IGIS staff provided advice (and resources available from the Office of the Commonwealth Ombudsman) about appropriate management of unreasonable conduct to ASD. As a result, the ACSC wrote to the individual formally advising the communication restrictions, the timeframe during which the restrictions would be imposed, and conditions to be met in regard to any future contact. The ACSC expressed appreciation for the guidance IGIS staff provided and indicated an intention to incorporate it in staff training.



PUBLIC INTEREST DISCLOSURES

ABOUT PUBLIC INTEREST DISCLOSURES

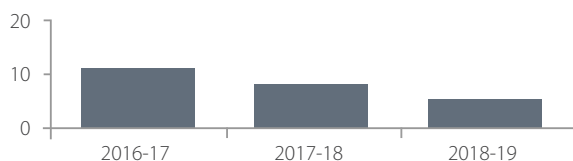
The *Public Interest Disclosure Act 2013* (PID Act) is intended to promote integrity and accountability within the Commonwealth public sector, including by encouraging public interest disclosures by public officials, providing appropriate support to disclosers to ensure that they are not subject to adverse 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

The office 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; and
- Overseeing the operation of the PID scheme in the intelligence agencies.

The office has nine 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.

Figure 2.6: Number of public interest disclosure (PID) received 2016-17 to 2018-19**Figure 2.7: Timeliness of responses to public interest disclosures in 2018-19**

NUMBER OF PID	ACKNOWLEDGED WITHIN 5 BUSINESS DAYS	AVERAGE BUSINESS DAYS TO ACKNOWLEDGE	PID ACT INVESTIGATION	IGIS ACT INVESTIGATION	NUMBER FINALISED	AVERAGE DAYS TO FINALISE
5	5	2	0	5	3	129

Figure 2.8: Public interest disclosures by agency and source in 2018-19

AGENCY	NUMBER OF PID	FROM PUBLIC	FROM INTELLIGENCE AGENCY EMPLOYEE OR EX-EMPLOYEE
ASIO	1	0	1
ASIS	3	0	3
ASD	1	0	1

There were five public interest disclosures concerning intelligence agencies during the reporting period, reflecting a downward trend since the commencement of the scheme in the 2016-17 reporting period. No disclosable conduct was reported in relation to the IGIS.

All five of the public interest disclosures raised allegations of maladministration in security assessment processes, including procedural fairness, bias and other unprofessional conduct. One related to the conduct of a pre-employment security assessment, one to conditions for contractors seeking to work across multiple agencies, and three concerned the withdrawal of clearances. One of these also alleged maladministration in relation to reported concerns about staff well-being.

Investigation of one case did not proceed as the discloser withdrew the claim in order to pursue other internal avenues. Section 48 of the PID Act provides the principal officer of the agency with discretion not to investigate. As the disclosure related to a decision by the employer to withdraw the complainant's Positive Vetting security clearance and thus terminate their employment, the Inspector-General was satisfied there was no merit in investigating the case at this time.

Investigation of the remaining disclosures was conducted in accordance with the IGIS Act, rather than the PID Act, to enable the use of the IGIS inquiry powers if required. Recommendations were made in one case. Two of the five PIDs remained open at the end of the reporting period.

Despite what appears to be a cluster in reporting about maladministration in security clearance processes, no trends have been identified through the cases examined by this office.

CASE STUDY 6: DISCLOSURE ALLEGING MALADMINISTRATION

A PID relating to ASD concerned maladministration resulting in the denial of a contracting position. The discloser alleged ASD did not provide procedural fairness and was concerned the denial could be reprisal action for having made a previous complaint.

Investigation under the IGIS Act found no evidence to prove the allegations. While the investigation found some areas for improvement in ASD's communication and processes, these would not have changed ASD's decision in the case. The Inspector-General made two recommendations relating to ASD's internal processes and two relating to the specific case, all of which were accepted by ASD.

OVERSEEING THE OPERATION OF THE PID SCHEME IN THE INTELLIGENCE AGENCIES

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

IGIS was informed of one PID received by ASD in the 2018-19 reporting period. The remaining intelligence agencies reported having received no PIDs in the same period.

IGIS also has a role in meeting annual reporting obligations by collecting and collating the intelligence agencies' responses to the Commonwealth Ombudsman's annual PID survey. IGIS performs this role to ensure the protection of classified details relating to the intelligence agencies.

OTHER CONTACTS

In 2018-19 the office also received contacts from approximately 200 individuals seeking advice or expressing concern about matters affecting them that were assessed to be outside the jurisdiction of the office or did not require action. This represents an increase of around 23% over the previous reporting period. Over one-third of these individuals made repeated contact raising the same or similar issues. IGIS staff apply a consistent, fair approach to managing such matters.

When the office is contacted about matters that it cannot pursue, IGIS staff provide written or oral advice about the office's jurisdiction and alternative action that can be taken to resolve concerns, including reference to other complaint-handling bodies, police and the National Security Hotline. In cases where there has been previous contact about matters that have already been assessed, the office takes no further action unless substantially new and credible information is provided.

OBJECTIVE 5 – INFRASTRUCTURE AND RELATIONSHIPS

RELOCATION OF IGIS PREMISES

In March 2019 IGIS relocated from its premises at One National Circuit, Barton to new larger premises co-located with the Attorney-General's Department at 3-5 National Circuit, Barton. The increased size of the new premises was necessary to accommodate the projected growth in staff numbers in line with the office's corporate plan. The office move was completed on time, within budget and with no security concerns.

ABOUT LIAISING WITH OTHER ACCOUNTABILITY OR INTEGRITY AGENCIES

The office frequently liaises with other accountability and integrity agencies, both in Australia and overseas, to discuss matters of mutual interest, learn from each other's practices, and to keep abreast of significant developments in other jurisdictions.

DOMESTIC LIAISON WITH OTHER ACCOUNTABILITY AND INTEGRITY AGENCIES

The focus of our engagement with other domestic accountability and integrity agencies has been the practicalities of implementing the recommendations from the *2017 Independent Intelligence Review* 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. During the reporting period the office worked with the Australian Commission for Law Enforcement Integrity (ACLEI), the Australian Human Rights Commission (AHRC), the Inspector-General of the Australian Defence Force (IGADF), the Office of the Commonwealth Ombudsman (OCO) and the Office of the Australian Information Commissioner (OAIC) on measures to ensure that our future oversight activities are complementary and to avoid overlap to the greatest possible extent. An agreement-in-principle has been reached and set out in a Statement of Cooperation. The Statement of Cooperation will be finalised once legislation expanding the jurisdiction of IGIS has commenced.

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

During the reporting period the office continued to strengthen our relationship with ACLEI ahead of proposed changes to our jurisdiction. An IGIS officer completed a six-month Immersive Development Placement with ACLEI to enhance our understanding of their activities, practices and procedures. Additionally, IGIS officers attended ACLEI's Community of Practice for Corruption Prevention meeting as observers.

AUSTRALIAN HUMAN RIGHTS COMMISSION

The AHRC is required by section 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 and security agencies to the Inspector-General. During 2018-19 no such matters were referred by the AHRC.

INSPECTOR-GENERAL OF THE AUSTRALIAN DEFENCE FORCE

During the reporting period IGIS officers attended training conducted by the IGADF on the conduct of administrative inquiries in the Australian Defence Force.

OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER

In December 2018 the Deputy Inspector-General met with the Australian Information Commissioner and Privacy Commissioner to discuss the development of privacy rules for ONI.

OFFICE OF THE COMMONWEALTH OMBUDSMAN

The work of the OCO and this office is complementary and there is a memorandum of understanding that provides guidance on handling complaints that overlap the jurisdiction of each office. A review of the memorandum was conducted during the reporting period with a view to updating the guidance and broadening its scope, in particular to address the proposed expansion of the jurisdiction of this office. During the reporting period, IGIS continued to hold regular face-to-face meetings at the Deputy Inspector-General/Deputy Ombudsman level as well as working level engagement. At the working level our engagement with OCO has focused on the measures to avoid duplication of future oversight and has included IGIS officers observing elements of Ombudsman inspections of agencies within the scope of the proposed expansion of IGIS jurisdiction. During 2018-19 one IGIS staff member completed an Immersive Development Placement with OCO.

INTERNATIONAL ENGAGEMENT WITH ACCOUNTABILITY AND INTEGRITY AGENCIES

FIVE EYES INTELLIGENCE OVERSIGHT AND REVIEW COUNCIL

In October 2018 the Inspector-General hosted the annual meeting of the Five Eyes Intelligence Oversight and Review Council (the Council) in Canberra. The Council 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 Communications Security Establishment Commissioner and the Security and Intelligence Review Committee 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. Council members

exchange views on subjects of mutual interest and concern; compare best practices in review and oversight methodology; where appropriate explore areas where cooperation on reviews and the sharing of results is permitted; encourage transparency to the largest extent possible to enhance public trust; and maintain contact with political offices, oversight and review committees, and non-Five Eyes countries as appropriate. The Council meets in person at least once per year.

The 2018 Council meeting agenda focused on the themes of independence and keeping up with technology. During the first day discussion focused on the importance of, and challenges associated with, intelligence review and oversight entities maintaining their institutional independence. Issues covered included the importance of independence, the security of their independence and its limitations, the relative importance of actual and perceived independence, the potential for compromise of independence, and how review and oversight bodies demonstrate their independence. On the second day of the conference, discussion focused on the importance of, and challenges associated with, the intelligence review and oversight entities' abilities to keep up with technology. Issues discussed included challenges associated with hiring, training, and retaining their workforces, the potential for accountability capture by the intelligence services, and developing cultures of compliance with intelligence services subject to intelligence review and oversight. Sessions on unauthorised disclosures and exchange programs were also held on the second day.

During the conference Alexander W. Joel, the Chief of the Office of Civil Liberties, Privacy, and Transparency with the United States Office of the Director of National Intelligence, delivered a keynote address on the importance of transparency. This address was attended by the Council members as well as senior representatives from Australian and New Zealand intelligence communities and a member of the Australian parliament.

During the reporting period, the Council has also liaised via teleconference in preparation for its October 2019 meeting, which will take place in the United Kingdom. This activity will be reported in the 2019-20 annual report.

BILATERAL ENGAGEMENT

In early May 2019 the Inspector-General and a senior officer travelled to the United Kingdom to meet with the Investigatory Powers Commissioner and members of his office. Discussions covered the formation and functioning of the Investigatory Powers Commissioner's Office and the 'double-lock' mechanism, the Technology Advisory Panel, oversight of covert effects and bulk data, oversight of policing bodies, and dealings with civil society groups. This engagement also saw the Inspector-General meet with agencies within the oversight jurisdiction of the Investigatory Powers Commissioner's Office.

In late May 2019 the Inspector-General and Deputy Inspector-General travelled to Wellington to meet with the New Zealand Inspector-General of Intelligence and Security and her office. This engagement enabled discussion on key national developments and matters of mutual interest, including changes to the National Intelligence Community, outreach with civil society groups, collaborative projects, and the conduct of overseas inspections.

OBJECTIVE 6 – HIGH-PERFORMING WORKFORCE

OVERVIEW

IGIS maintains a strategic human resources (HR) plan to ensure that the office recruits, develops and retains a workforce that effectively supports the Inspector-General in current activities as well as preparing the office for its anticipated expansion of jurisdiction. In 2018-19 the average staff turnover for the office was 8.4%. The office is partially meeting its recruitment targets in the strategic HR plan and several candidates are undergoing relevant pre-employment suitability and security checks.

In 2018-19 the office continued its program of internal training in job-specific skills and knowledge including recent changes to legislation, complaints handling and security awareness. In order to manage increased recruitment activity and larger staff numbers overall, in 2018-19 the office implemented a formal five day induction program for new staff. The office also provided opportunities for staff to attend training courses and seminars relevant to their role. The IGIS Enterprise Agreement 2016-2019 provides a studies assistance scheme for employees who pursue studies relevant to the work of the office.

The office conducts regular staff surveys to seek feedback on the office's performance management and training arrangements. In a staff survey conducted in June 2019, roughly 70% of staff agreed or strongly agreed that performance management, training and development and leadership provided by the IGIS executive adequately support employees to perform the duties of the office.

STAFF PLACEMENTS

During 2018-19 this office has undertaken Immersive Development Placements with other Commonwealth government agencies, including the Australian Commission for Law Enforcement Integrity (ACLEI), the Australian Criminal Intelligence Commission (ACIC), the Australian Federal Police (AFP), the Australian Transaction Reports and Analysis Centre (AUSTRAC), and the Office of the Commonwealth Ombudsman (OCO). These placements have been undertaken in accordance with arrangements developed in a memorandum of understanding with each host agency, and further tailored to each individual placement. A Memorandum of Understanding for Immersive Development Placements has also been negotiated with the Department of Home Affairs.

These placements were designed to improve the expertise of this office ahead of the commencement of its expanded jurisdiction. They also enabled 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. Where individuals have been hosted in the ACIC, AFP and AUSTRAC, it has also improved the office's understanding of the intelligence functions of these agencies, and developed the skills and capability of our employees in relation to those functions. The placement of IGIS employees with other oversight bodies (ACLEI and OCO) has assisted this office in its work to prepare for the de-confliction of oversight when the expanded jurisdiction commences. Placements have primarily been undertaken by newly recruited staff who are in the process of obtaining the security clearance for IGIS roles.

SECTION THREE

MANAGEMENT AND ACCOUNTABILITY





MANAGEMENT AND ACCOUNTABILITY

CORPORATE GOVERNANCE

ORGANISATIONAL STRUCTURE

Senior positions occupied during 2018–19 were as follows:

Inspector-General of Intelligence and Security (Statutory officer)

The Honourable Margaret Stone AO FAAL, appointed 24 August 2015.

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

Mr Jake Blight, appointed 23 October 2018; 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.

These four positions were designated by the Inspector-General as Key Management Personnel for 2018–19.

SENIOR MANAGEMENT COMMITTEES

The office's corporate governance framework incorporates 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 Audit Committee is discussed later in this report under Internal Audit and Risk Management.

CORPORATE AND OPERATIONAL PLANNING

The office's corporate and operational planning processes are straightforward in nature, 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;
- weekly meetings between the Inspector-General and senior staff members, to review and document operational priorities;
- monthly meetings between the Inspector-General and all office staff, during which current operational matters, internal guidelines as well as procedures and governance issues are discussed; and

- a forward plan for inspection activities in each intelligence agency, which is determined in consultation with the relevant agency head (in accordance with section 9A of the IGIS Act).

PROTECTIVE SECURITY

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

The governance arrangements and core policies in the framework describe the higher level protective security outcomes and identify mandatory compliance requirements which IGIS must meet.

As at 30 June 2019, the office was fully compliant with all 36 mandatory requirements.

INTERNAL AUDIT AND RISK MANAGEMENT

The membership and functions of the Audit Committee are structured according to the PGPA Act. During 2018-19 the membership comprised Mr Trevor Kennedy (Attorney-General's Department) as Chair, Ms Sarah Vandebroek (Department of Communications and the Arts) and Mr Jake Blight (IGIS). The Inspector-General attends 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; and
- 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 including the following:

- 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;
- corporate liability;
- fraud prevention, detection and management; and
- corporate compliance requirements.



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

ETHICAL STANDARDS AND FRAUD CONTROL

During 2018-19 IGIS continued its commitment to high ethical standards and having high performing and professional staff. Our high ethical standards are maintained through:

- modelling of appropriate behaviours by the agency's Senior Executive;
- implementation of organisational suitability assessments;
- a requirement that all staff maintain a high level security clearance;
- annual declaration of known interests by the Senior Executive and all employees; and
- incorporation of APS Values and Code of Conduct expectations in the agency's performance agreement process.

The office is a member of the Australian Public Service 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 cases of fraud or breaches of the APS Code of Conduct.

The office has established and maintains appropriate systems of risk oversight, management and internal controls in accordance with section 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, considered and discussed 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.

The terms and conditions of all SES officer employment, including salary, are set out in individual section 24(1) determinations and are based broadly on SES remuneration within the Attorney-General's Department. Each section 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 set 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 section 32(3) of any person to perform functions and exercise powers for the purposes of a particular inquiry, and any delegation under section 32AA to such a person. Mr Bruce Miller AO was appointed on 1 August 2018 to conduct an inquiry during 2018-19. Mr Miller's appointment concluded on 20 December 2018. Further details of this inquiry are provided in the Annual Performance Statement.

ISSUES RELATING TO SIGNIFICANT NON-COMPLIANCE WITH THE FINANCE LAW

There were no significant issues relating to non-compliance with the finance law during 2018-19 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

There were no reports on the operation of the office (other than the report on financial statements) by any of the above bodies. It should be noted that the office is not within the jurisdiction of the Commonwealth Ombudsman.

The office has received an unqualified audit report from the Australian National Audit Office (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.

CAPABILITY REVIEWS

No capability reviews of IGIS were released during 2018-19.

MANAGEMENT OF HUMAN RESOURCES

ORGANISATIONAL PROFILE

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 APS employee was employed on a non-ongoing basis.

No employees identified as Indigenous.

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

Figure 3.1: Organisational Profile as at 30 June 2019 (employment level and status)

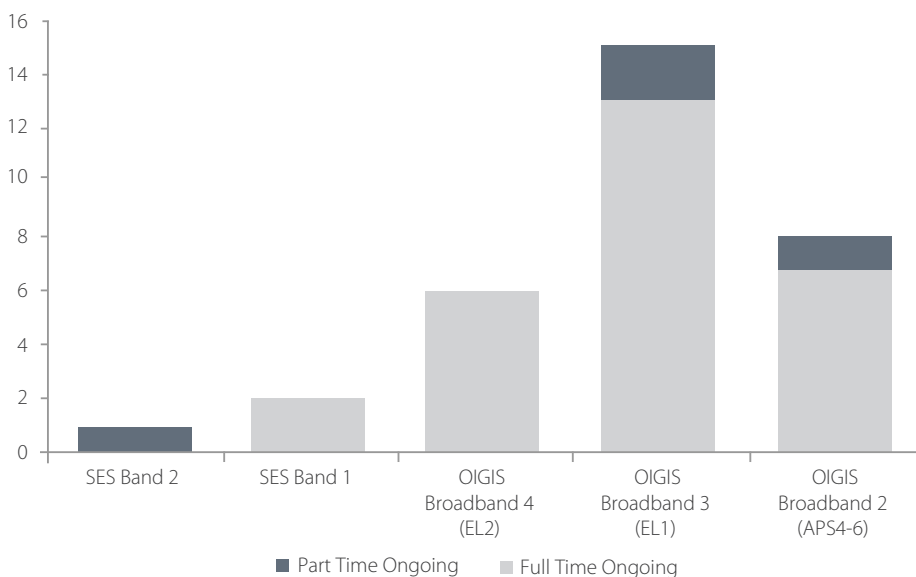
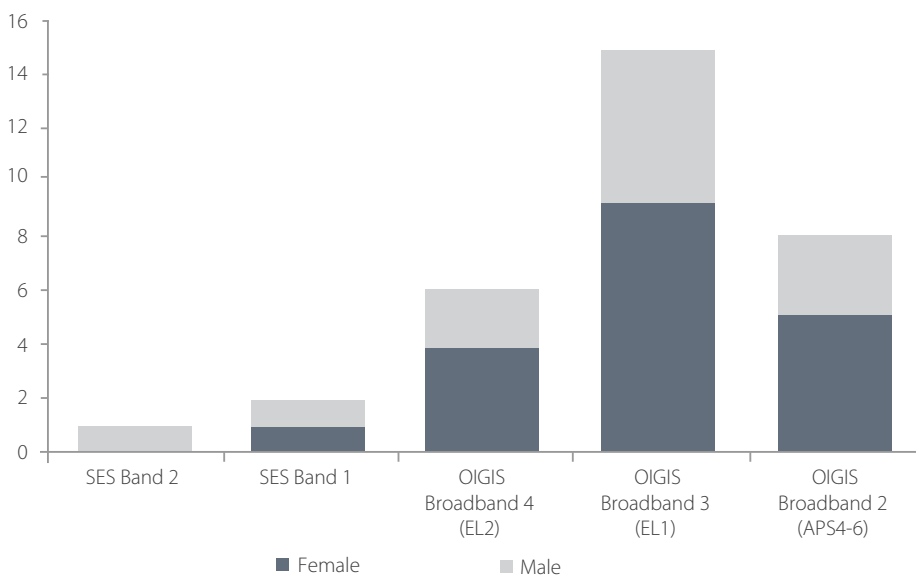


Figure 3.2: Gender Balance as at 30 June 2019 (by employment level and status)



EMPLOYMENT FRAMEWORKS

Since 6 February 2017, all non-SES staff have been employed under the IGIS Enterprise Agreement 2016-2019. Three SES staff members are presently employed in accordance with individual determinations under section 24(1) of the *Public Service Act 1999*. During 2018-19 one non-APS staff member was employed on a non-ongoing basis in accordance with a written agreement under section 32(3) of the IGIS Act.

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 staff 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 was \$1,148 until 7 February 2019 when the allowance increased to \$1,159 in line with IGIS Enterprise Agreement 2016-2019 annual remuneration increases.

MANAGING AND DEVELOPING EMPLOYEES

Objective 6 of the IGIS Corporate Plan 2018-19 relates to managing and developing staff in the office to achieve IGIS outcomes. An assessment of effectiveness is contained in the Annual Performance Statement.

PERFORMANCE PAY

The office does not have a performance pay scheme.

ASSETS MANAGEMENT

Management of the office's assets is governed by the office's 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 IGIS 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/statistics-on-commonwealth-purchasing-contracts/.

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 2018-19, twelve new consultancy contracts were entered into, involving total actual expenditure of \$486,952.35 (GST inclusive). In addition, two ongoing consultancy contracts were active during the period, involving total actual expenditure of \$9,526.00 (GST inclusive).

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 2018-19 was to obtain specialist expertise not available within the office due to its small size.

Annual reports contain information about actual expenditure on contracts and consultancies. Information on the value of contracts and consultancies is available on the AusTender website, 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

Eight contracts totalling \$5,601,023.99 were entered into during the reporting period that have been exempt from publishing on AusTender.

DISABILITY REPORTING MECHANISM

Since 1994, Commonwealth departments and agencies have reported on their performance as a policy adviser, purchaser, employer, regulator and provider under the Commonwealth Disability Strategy. In 2007–08, reporting on the employer role was transferred to the Australian Public Service Commission's State of the Service Report and the APS Statistical Bulletin. These reports are available at www.apsc.gov.au. From 2010-11, departments and agencies have no longer been required to report on these functions.

The Commonwealth Disability Strategy has been overtaken by the National Disability Strategy 2010-2020, which sets out a 10 year national policy framework to improve the lives of people with disability, promote participation and create a more inclusive society. A high level biennial report will track progress against each of the six outcome areas of the strategy and present a picture of how people with disability are faring. The first of these reports was published in 2015, and can be found at www.dss.gov.au.

INFORMATION PUBLICATION SCHEME

Entities subject to the *Freedom of Information Act 1982* (FOI Act) are required to publish information to the public as part of the Information Publication Scheme (IPS). This requirement is in Part II of the FOI Act and has replaced the former requirement to publish a section 8 statement in an annual report. Each agency must display on its website a plan showing what information it publishes in accordance with the IPS requirements.

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

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 2018-19 financial statements. A summary of our financial performance follows.

The office operated within available resources in 2018-19 and ended the year with a surplus of \$3,152,838. The summary of financial performance is based on the original budget figures as published in the Portfolio Budget Statements 2018-19.

Appropriation funding levels in 2018-19 increased significantly with the office being funded to increase from 16 to 42 staff during the year. Other Income decreased by \$136,384 largely due to a decrease in resources received free of charge by the office with the office commencing payment for property expenses. The decrease in Other Income was matched by a corresponding decrease in Supplier Expenses so there was no impact on the overall financial outcome.

In relation to expenditure, the most significant variance against original budget figures related to employee expenses which were \$2,807,867 underspent due largely to recruitment onboarding 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 due to delays in the relocation of the office and the completion of associated leasehold improvements.

Total equity increased from \$18,406,446 in 2017-18 to \$21,821,168 in 2018-19. Movements in equity included a \$3,152,838 increase in retained surplus. Contributed Equity also increased from \$12,109,283 in 2017-18 to \$12,371,167 in 2018-19 with capital funding totalling \$275,000 in the current year.

The following tables show:

Figure 4.1 – Entity Resource Statement and Resource for Outcomes 2018-19.

Figure 4.2 – Expenses and Resources for Outcome 1.

ENTITY RESOURCE STATEMENT AND RESOURCES FOR OUTCOMES 2018-19

Figure 4.1: Entity resource statement for 2018-19

	ACTUAL AVAILABLE APPROPRIATION FOR 2018-19 \$'000 (A)	PAYMENTS MADE 2018-19 \$'000 (B)	BALANCE REMAINING 2018-19 \$'000 (A) – (B)
Ordinary Annual Services			
Departmental Appropriation			
Prior year departmental appropriation	19,310	11,109	8,201
Departmental appropriation	9,917	1,032	8,885
S74 Relevant Agency Receipts	1,160	-	1,160
Total	30,387	12,141	18,246
Administered expenses			
Total	-	-	-
Total ordinary annual services A	30,387	12,141	18,246
Other services			
Departmental non-operating	-	-	-
Total	-	-	-
Total other services B	-	-	-
Total available annual appropriations			
	30,387	12,141	18,246
Special appropriations			
Total special appropriations C	-	-	-
Special accounts			
Total special accounts D	-	-	-
Total resourcing A + B + C + D	30,387	12,141	18,246
Less appropriations drawn from annual or special appropriations above and credited to special accounts and/or payments to corporate entities through annual appropriations	-	-	-
Total net resourcing and payments for agency	30,387	12,141	18,246

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 2018-19 \$'000	ACTUAL EXPENSES 2018-19 \$'000	VARIATION 2018-19 \$'000
	(A)	(B)	(A)-(B)

**Program 1.1: Office of the
Inspector-General of Intelligence
and Security**

Departmental expenses

Departmental appropriation ¹	9,642	9,642	-
Special appropriations	-	-	-
Special Accounts	-	-	-
Expenses not requiring appropriation in the Budget year	1,851	(3,080)	4,931
Total for Program 1.1	11,493	6,562	4,931

**Outcome 1 Totals by
appropriation type**

Departmental expenses

Departmental appropriation ¹	9,642	9,642	-
Special appropriations	-	-	-
Special Accounts	-	-	-
Expenses not requiring appropriation in the Budget year	1,851	(3,080)	4,931
Total expenses for Outcome 1	11,493	6,562	4,931

	Budget 2018-19	Actual 2018-19	
Average Staffing Level (number)	42	26	16

¹ 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 2018-19 included:

- A \$2,823,000 increase in Revenue from Government.
- A \$1,599,579 increase in employee expenses arising largely due to recruitment activity associated with the expansion of the office.
- A \$1,345,156 increase in supplier expenses. Increases in expenditure included \$587,801 in occupancy expenses, \$414,942 in consultancy expenses, \$88,045 in HR support fees, \$97,002 in ICT expenses, \$58,323 in minor equipment purchases, \$62,680 in travel and \$33,441 in security vetting expenses.
- A \$5,589,642 increase in Property, Plant and Equipment following the relocation of the office with associated leasehold improvements, new software licensing arrangements and office furniture expenditure. The increased capital expenditure was offset by a \$253,174 increase in depreciation expenses.
- A \$479,009 increase in Employee Provisions due to the increasing staff numbers associated with the expansion of the office.

Figure 4.3: Trends in finance

		2018-19 OUTCOME 1 \$	2017-18 OUTCOME 1 \$	CHANGE FROM PREVIOUS YEAR
Revenue from Government		9,642,000	6,819,000	+41.4%
Other Income		72,470	208,854	-65.3%
TOTAL INCOME		9,714,470	7,027,854	
Employee expenses		4,444,133	2,844,554	+56%
Supplier expenses		1,819,509	474,353	+383.5%
Other expenses		297,990	44,816	+664.9%
TOTAL EXPENSES		6,561,632	3,363,723	
OPERATING RESULT		3,152,838	3,664,131	
Financial assets	A	18,437,104	19,476,805	-5.4%
Non-financial assets	B	5,738,199	56,468	+10,162%
Liabilities	C	2,354,135	1,126,827	+208.9%
NET ASSETS = A + B - C		21,821,168	18,406,446	



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 2019:

- (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 2019 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 2019 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

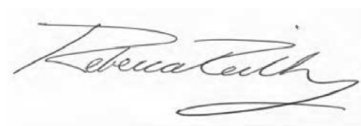
My objective is to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes my opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that 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
24 September 2019

STATEMENT BY THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2019 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.



Margaret Stone
Inspector-General of
Intelligence and Security

24 September 2019



OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY
STATEMENT OF COMPREHENSIVE INCOME
for the year ended 30 June 2019

	Notes	2019 \$	2018 \$	Original Budget \$
NET COST OF SERVICES				
Expenses				
Employee benefits	2A	4 444 133	2 844 554	7 252 000
Suppliers	2B	1 819 509	474 353	2 517 000
Depreciation	5	297 990	44 816	1 724 000
Total expenses		<u>6 561 632</u>	<u>3 363 723</u>	<u>11 493 000</u>
Own-Source Income				
Own-source revenue				
Other revenue	3A	72 470	208 854	127 000
Total own-source income		<u>72 470</u>	<u>208 854</u>	<u>127 000</u>
Net cost of services		<u>6 489 162</u>	<u>3 154 869</u>	<u>11 366 000</u>
Revenue from Government		<u>9 642 000</u>	<u>6 819 000</u>	<u>9 642 000</u>
Surplus /(deficit) on continuing operations		<u>3 152 838</u>	<u>3 664 131</u>	<u>(1 724 000)</u>
OTHER COMPREHENSIVE INCOME				
Items not subject to subsequent reclassification to net cost of services				
Changes in asset revaluation surplus		<u>-</u>	<u>-</u>	<u>-</u>
Total comprehensive income/(loss)		<u>3 152 838</u>	<u>3 664 131</u>	<u>(1 724 000)</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 2019

	Notes	2019 \$	2018 \$	Original Budget \$
ASSETS				
Financial Assets				
Cash and cash equivalents		306 265	199 788	450 000
Trade and other receivables	4	18 130 839	19 277 017	5 747 000
Total financial assets		<u>18 437 104</u>	<u>19 476 805</u>	<u>6 197 000</u>
Non-Financial Assets				
Property, plant and equipment	5	5 646 110	56 468	10 211 000
Other non-financial assets	6	92 089	-	-
Total non-financial assets		<u>5 738 199</u>	<u>56 468</u>	<u>10 211 000</u>
Total Assets		<u>24 175 303</u>	<u>19 533 273</u>	<u>16 408 000</u>
LIABILITIES				
Payables				
Suppliers	7A	783 065	22 463	1 000 000
Other payables	7B	41 158	53 461	100 000
Total payables		<u>824 223</u>	<u>75 924</u>	<u>1 100 000</u>
Provisions				
Employee provisions	8	1 529 912	1 050 903	2 000 000
Other provisions		-	-	50 000
Total provisions		<u>1 529 912</u>	<u>1 050 903</u>	<u>2 050 000</u>
Total Liabilities		<u>2 354 135</u>	<u>1 126 827</u>	<u>3 150 000</u>
Net Assets		<u>21 821 168</u>	<u>18 406 446</u>	<u>13 258 000</u>
EQUITY				
Contributed equity		12 371 167	12 109 283	12 388 000
Reserves		21 623	21 623	22 000
Retained surplus		9 428 378	6 275 540	848 000
Total Equity		<u>21 821 168</u>	<u>18 406 446</u>	<u>13 258 000</u>

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



OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY
STATEMENT OF CHANGES IN EQUITY
for the period 30 June 2019

	2019 \$	2018 \$	Original Budget \$
CONTRIBUTED EQUITY			
Opening balance as at 1 July	12 109 283	528 126	12 113 000
Transactions with Owners			
Contributions by Owners			
Return of Equity	(13 116)	(1 000)	
Departmental Capital Budget	275 000	11 582 157	275 000
Total Transactions with Owners	261 884	11 581 157	275 000
Closing balance as at 30 June	12 371 167	12 109 283	12 388 000
RETAINED EARNINGS			
Opening balance as at 1 July			
Balance carried forward from previous period	6 275 540	2 611 409	2 572 000
Comprehensive Income			
Surplus/deficit for the period	3 152 838	3 664 131	(1 724 000)
Total comprehensive income	3 152 838	3 664 131	(1 724 000)
Closing balance as at 30 June	9 428 378	6 275 540	848 000
ASSET REVALUATION RESERVE			
Opening balance as at 1 July			
Balance carried forward from previous period	21 623	21 623	22 000
Comprehensive Income			
Other Comprehensive Income	-	-	-
Total comprehensive income	-	-	-
Closing balance as at 30 June	21 623	21 623	22 000
TOTAL EQUITY			
Opening balance			
Balance carried forward from previous period	18 406 446	3 161 158	14 707 000
Comprehensive Income			
Surplus/deficit for the period	3 152 838	3 664 131	(1 724 000)
Other comprehensive income	-	-	-
Total comprehensive income	3 152 838	3 664 131	(1 724 000)
Transactions with Owners			
Contributions by Owners			
Return of Equity	(13 116)	(1 000)	
Departmental Capital Budget	275 000	11 582 157	275 000
Total Transactions with Owners	261 884	11 581 157	275 000
Closing balance as at 30 June	21 821 168	18 406 446	13 258 000

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 2019

	Notes	2019 \$	2018 \$	Original Budget \$
OPERATING ACTIVITIES				
Cash received				
Appropriations		5 759 654	3 353 815	9 049 000
Net GST received		585 149	14 139	-
Other cash received		575 026	261 646	127 000
Total cash received		<u>6 919 829</u>	<u>3 629 600</u>	<u>9 176 000</u>
Cash used				
Employees		(4 130 812)	(3 042 837)	(6 327 000)
Suppliers		(2 172 315)	(326 042)	(2 849 000)
Section 74 receipts transferred to OPA		(510 224)	(261 431)	-
Total cash used		<u>(6 813 351)</u>	<u>(3 630 310)</u>	<u>(9 176 000)</u>
Net cash from/(used by) operating activities		<u>106 477</u>	<u>(710)</u>	<u>-</u>
INVESTING ACTIVITIES				
Cash used				
Purchase of property, plant and equipment		(5 838 030)	(11 884)	(275 000)
Total cash used		<u>(5 838 030)</u>	<u>(11 884)</u>	<u>(275 000)</u>
Net cash from/(used by) investing activities		<u>(5 838 030)</u>	<u>(11 884)</u>	<u>(275 000)</u>
FINANCING ACTIVITIES				
Cash received				
Contributed equity		5 838 030	11 884	275 000
Total cash received		<u>5 838 030</u>	<u>11 884</u>	<u>275 000</u>
Net cash from financing activities		<u>5 838 030</u>	<u>11 884</u>	<u>275 000</u>
Net increase/(decrease) in cash held		<u>106 477</u>	<u>(710)</u>	<u>-</u>
Cash and cash equivalents at the beginning of the reporting period		199 788	200 498	450 000
Cash and cash equivalents at the end of the reporting period		<u>306 265</u>	<u>199 788</u>	<u>450 000</u>

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



Major Budget Variances for 2019

The following table provides high level commentary of major variances between budgeted information for the OIGIS published in the 2018-19 Portfolio Budget Statements (PBS) and the 2018-19 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 – \$2,807,867 below budget. The variance reflects delays in on boarding activities, partly associated with the lengthy security clearance process.</p> <p>Employee Provisions - \$470,088 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 – \$697,491 below budget. The most significant variances related to security clearance fees, which were lower due to recruitment delays, and ICT support fees. Other variances include underspends in expenses driven by the number and scope of inquiry work, including legal and travel expenses.</p> <p>Suppliers payable - \$216,938 below budget. The variance is linked to underspend in supplier expenses.</p>	<p>Impacted:</p> <p>Statement of Comprehensive Income: Supplier expenses</p> <p>Statement of Financial Position: Appropriation receivable Suppliers payables Retained surplus</p> <p>Cashflow Statement: Cash used - operating activities</p>
<p>Property, Plant and Equipment – capital expenditure was approximately \$4,564,890 below budget due to the timing of asset purchases. The variance reflects plans to undertake further capital works for OIGIS's office space.</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>

Note 1 – Overview

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.

1.3 New Australian Accounting Standards

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

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.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2019

Note 2 – Expenses

	2019	2018
	\$	\$
<u>Note 2A – Employee Benefits</u>		
Wages and salaries	3 354 324	2 123 953
Superannuation:		
Defined benefit plans	239 787	162 303
Defined contribution plans	329 297	202 013
Leave and other entitlements	520 725	356 285
Total employee benefits	<u>4 444 133</u>	<u>2 844 554</u>

Accounting Policy

Accounting policies for employee related expenses are contained in Note 8.

	2019	2018
	\$	\$
<u>Note 2B – Suppliers</u>		
Goods and services supplied or rendered		
Consultants	467 878	52 936
ICT support	143 002	46 000
Legal expenses	4 165	-
Printing publications	13 352	13 614
Resources received free of charge	39 545	201 417
Stationery	32 183	16 637
Training	20 041	16 150
Travel	102 620	39 940
Security Vetting Expenses	76 587	43 146
HR Support Services	88 045	-
Minor Assets	58 323	-
Scribe Services	24 522	-
Occupancy Expenses	587 801	-
Accommodation - Placements	50 377	-
Other	90 452	24 115
Total goods and services supplied or rendered	<u>1 798 893</u>	<u>453 955</u>
Other suppliers		
Motor Vehicle Lease – minimum lease payments	8 555	15 994
Workers compensation premiums	12 061	4 404
Total other supplier	<u>20 616</u>	<u>20 398</u>
Total supplier	<u>1 819 509</u>	<u>474 353</u>

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2019

Leasing Commitments

Commitments for minimum lease payments in relation to non-cancellable operating leases are payable as follows:

	2019 \$	2018 \$
Within 1 year	6 058	6 903
Between 1 to 5 years	12 619	19 181
Total operating lease commitments	18 677	26 084

Note 3 – Own-Source Revenue

	2019 \$	2018 \$
<u>Note 3A – Other Revenue</u>		
Employee FBT Contributions	19 155	5 262
Other	13 770	2 175
Resources Received Free of Charge:		
Department of the Prime Minister & Cabinet	-	175 872
Australian National Audit Office	35 000	21 000
Australian Signals Directorate	4 545	4 545
Total other own-source revenue	72 470	208 854

Accounting Policy

Resources Received Free of Charge

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

The main resources received free of charge in 2018-19 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

	2019 \$	2018 \$
<u>Trade and other receivables</u>		
Appropriations receivable	17 939 771	19 123 295
GST receivable from the Australian Taxation Office	67 739	1 803
Other receivables	123 329	151 919
Total trade and other receivables (net)	18 130 839	19 277 017

All receivables are expected to be recovered in less than 12 months.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2019

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 \$
As at 1 July 2018				
Gross book value	101 284	-	-	101 284
Accumulated depreciation and impairment	(44 816)	-	-	(44 816)
Total as at 1 July 2018	56 468	-	-	56 468
Additions				
by purchase	1 741 332	3 392 088	754 739	5 888 159
Disposals	(527)	-	-	(527)
Depreciation expense	(91 219)	(206 771)	-	(297 990)
Total as at 30 June 2019	1 706 054	3 185 317	754 739	5 646 110
Total as at 30 June 2019 represented by:				
Work in progress	530 000	-	754 739	1 284 739
Gross book value	1 280 416	3 392 088	-	4 672 505
Accumulated depreciation and impairment	(104 362)	(206 771)	-	(311 134)
Total as at 30 June 2019	1 706 054	3 185 317	754 739	5 646 110

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.

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 2019 included \$4,889,735 Level 2 assets (including office equipment and furniture, software and leasehold improvements) and \$1,636 Level 3 assets (including office furniture).

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2019

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 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. The most recent revaluation was conducted by the B&A Valuers as at 30 June 2017.

All assets were examined for indicators of impairment during the stocktake completed on 30 June 2019. 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 (2018: 1 – 11 years)
Leasehold Improvements 5 years (2018: Not applicable)

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.

Note 6 – Other Non-Financial Assets

	2019 \$	2018 \$
Prepayments	92 089	-
Total Other non-financial assets	92 089	-



NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2019

Note 7 – Payables

	2019	2018
	\$	\$
<u>7A - Suppliers</u>		
Trade creditors and accruals	783 065	22 463
Total suppliers	<u>783 065</u>	<u>22 463</u>

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).

	2019	2018
	\$	\$
<u>7B - Other Payables</u>		
Salaries and wages	31 210	23 567
Superannuation	4 874	3 492
Salary reimbursements for seconded officers	-	26 030
Other	5 074	372
Total other payables	<u>41 158</u>	<u>53 461</u>

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 – Employee Provisions

	2019	2018
	\$	\$
<u>Employee Provisions</u>		
Leave	1 529 912	1 050 903
Total employee provisions	<u>1 529 912</u>	<u>1 050 903</u>

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 sick leave as all sick leave is non-vesting and the average sick leave taken in future years by employees of OIGIS is estimated to be less than the annual entitlement for sick leave.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2019

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 9 – 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:

	2019 \$	2018 \$
Short-term employee benefits:		
Salary	901 374	705 181
Other Benefits & Allowances	110 734	69 572
Total short-term employee benefits	1 012 108	774 753
Post-employment benefits:		
Superannuation	125 197	90 563
Total post-employment benefits	125 197	90 563
Other long-term employee benefits:		
Long Service Leave	15 805	13 343
Total other long-term employee benefits	15 805	13 343
Total senior executive remuneration expenses	1 153 110	878 659

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 (2018: 3 individuals). The 2019 figure includes one of the officers for part of the year. The 2018 figure also included one of the officers for part of the year.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2019

Note 10 – 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 11 - 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 2019 (2018: Nil).

Note 12 – Financial Instruments

	2019 \$	2018 \$
<u>Categories of Financial Instruments</u>		
Financial Assets Under AASB 139		
Loans and receivables		
Cash and cash equivalents	-	199 788
Trade and other receivables	-	151 919
Total loans and receivables	-	351 707
Total financial assets at fair value through profit or loss	-	351 707
Financial Assets under AASB 9		
At amortised cost		
Cash and cash equivalents	306 265	-
Trade and other receivables	123 329	-
Total financial assets at amortised cost	429 594	-
Total financial assets at fair value through profit or loss	429 594	-
Total financial assets	429 594	351 707

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2019

Financial Liabilities

At amortised cost

Suppliers	783 065	22 463
Total financial liabilities	783 065	22 463

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 (2018: 30 days).

Classification of financial assets on the date of initial application of AASB 9

Financial assets class	AASB 139 original classification	AASB 9 new classification	AASB 139 carrying amount at 1 July 2018 \$	AASB 9 carrying amount at 1 July 2018 \$
Cash and cash equivalents	Loan and receivables	Amortised Cost	199 788	199 788
Trade and other receivables	Loan and receivables	Amortised Cost	151 919	151 919
Total Financial Assets			351 707	351 707

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.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2019

Note 13 – Appropriations

Note 13A – Annual Appropriations ('Recoverable GST exclusive')

	2019 \$	2018 \$
Ordinary Annual Services		
Annual Appropriation	9 642 000	6 819 000
PGPA Act – Section 74 Receipts	510 223	261 431
Annual Departmental Capital Budget ¹	275 000	11 585 000
Total appropriation	10 427 223	18 665 431
Appropriation applied (current and prior years)	11 491 154	3 353 815
Variance²	(1 063 931)	15 311 616

- 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 and underspends related largely to recruitment delays associated with security clearance requirements. The underspend in the current year is offset by the expenditure of previous years appropriations related to the purchase of assets and construction of the SCIF leasehold improvement.

Note 13B: Unspent Annual Appropriations ('Recoverable GST exclusive')

	2019 \$	2018 \$
Departmental		
Appropriation Act (No 1) 2015-16 – DCB	-	13 116
Supply Act 1 2016-17	-	419 747
Appropriation Act (No 1) 2016-17 – DCB	-	14 000
Supply Act 1 2016-17 – DCB	-	11 000
Appropriation Act (No 1) 2017-18	-	3 418 431
Appropriation Act (No 1) 2017-18 – DCB	-	25 000
Appropriation Act (No 3) 2017-18	2 772 309	3 662 000
Appropriation Act (No 3) 2017-18 – DCB	5 771 969	11 560 000
Appropriation Act (No 1) 2018-19	9 120 492	-
Appropriation Act (No 1) 2018-19 – DCB	275 000	-
Cash	306 265	199 788
Total Departmental	18 246 035	19 323 082

Note 14 – Aggregate Assets and Liabilities

	2019 \$	2018 \$
Assets expected to be recovered in:		
No more than 12 months	18 523 695	19 533 274
More than 12 months	5 651 608	0
Total assets	24 175 303	19 533 274
Liabilities expected to be recovered in:		
No more than 12 months	1 370 142	474 444
More than 12 months	983 993	652 381
Total liabilities	2 354 135	1 126 825

SECTION FIVE

ANNEXURES





ANNEXURE 5.1

IGIS SALARY SCALE

OIGIS BAND	APS LEVEL	SALARY RANGE 1 JULY 2018– 30 JUNE 2019 (\$)
OIGIS Band 4	EL2	119,442 – 142,153
OIGIS Band 3	EL1	102,620 – 114,398
OIGIS Band 2	APS 6	84,955 – 95,471
	APS 5	74,442 – 80,751
	APS 4	66,872 – 72,759
OIGIS Band 1	APS 3	60,143 – 64,768
	APS 2	52,570 – 58,458
	APS 1	47,896 – 51,310



ANNEXURE 5.2

KEY MANAGEMENT PERSONNEL

OIGIS had four executives who meet the definition of key management personnel. 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	Part year – appointed 28 February 2019

In the notes to the financial statements for the period ending 30 June 2019, OIGIS disclosed the following KMP expenses:

Note 9: Key management personnel remuneration for the reporting period

	2019 \$
Short-term benefits:	
Base salary	901,374
Bonus	-
Other benefits and allowances	110,734
Total short-term benefits	1,012,108
Superannuation	125,197
Total post-employment benefits	125,197
Long service leave	15,805
Total other long-term benefits	15,805
Termination benefits	-
Total key management personnel remuneration	1,153,110

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



		SHORT-TERM BENEFITS			POST-EMPLOYMENT BENEFITS	OTHER LONG-TERM BENEFITS		TERMINATION BENEFITS	TOTAL REMUNERATION
Name	Position title	Base salary	Bonuses	Other benefits and allowances	Superannuation contributions	Long service leave	Other long-term benefits		
Margaret Stone	Inspector-General (CEO)	435,414	-	50,677	31,955	-	-	-	518,046
Jake Blight	Deputy Inspector-General	212,357	-	25,667	35,856	6,869	-	-	280,749
Stephen McFarlane	Assistant Inspector-General	182,776	-	25,917	42,348	6,669	-	-	257,710
Bronwyn Notzon-Glenn	Assistant Inspector-General	70,827	-	8,472	15,038	2,267	-	-	96,604
Total		901,374	-	110,734	125,197	15,805	-	-	1,153,110



ANNEXURE 5.3

OTHER MANDATORY INFORMATION

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

WORK HEALTH AND SAFETY

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

Due to its small size, the office does not have a Workplace Health and Safety Committee. Instead, workplace health and safety matters are addressed at all-staff meetings, Audit Committee meetings and, as the need arises, directly with the Inspector-General through SES/team leaders 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.

ADVERTISING AND MARKET RESEARCH

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

The office, through its co-location with the Attorney-General's Department (AGD) and previously the Department of the Prime Minister and Cabinet (PM&C), continues to benefit from these Departments' commitments to energy saving measures. These measures include a large number of energy and water saving measures incorporated into the premises occupied by IGIS in 2018-19 (One National Circuit and 3-5 National Circuit), such as energy efficient lighting, heating and cooling.

Neither AGD nor PM&C separately measured the utilities used by the office in 2018-19. For this reason, ecologically sustainable development and details of environmental performance are not able to be quantified in this report.



Nonetheless, the office is committed to ensuring that its activities are environmentally responsible. While the majority of the office's infrastructure is provided and maintained by a host Department, there are a number of areas for which the office is directly responsible in which the IGIS takes into account the environmental impact and acts accordingly to minimise it.

These include:

- recycled paper was used for approximately 98% of the office's photocopying and document printing in 2018-19;
- printers are configured to print double-sided by default;
- all unclassified office paper and cardboard waste is recycled;
- empty toner cartridges are recycled; and
- the selection of a hybrid vehicle to replace the office car.

ANNEXURE 5.4

REQUIREMENTS FOR ANNUAL REPORTS

PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
17AD(g)	Letter of transmittal			
17AI	Preliminaries	A copy of the letter of transmittal signed and dated by accountable authority on date final text approved, with statement that the report has been prepared in accordance with section 46 of the Act and any enabling legislation that specifies additional requirements in relation to the annual report.	Mandatory	i
17AD(h)	Aids to access			
17AJ(a)	Preliminaries	Table of contents.	Mandatory	ii
17AJ(b)	Annexures	Alphabetical index.	Mandatory	116
17AJ(c)	Preliminaries	Glossary of abbreviations and acronyms.	Mandatory	v
17AJ(d)	Annexures	List of requirements.	Mandatory	107-115
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
17AD(a)	Review by accountable authority			
17AD(a)	Section 1	A review by the accountable authority of the entity.	Mandatory	2-8
17AD(b)	Overview of the entity			
17AE(1)(a)(i)	Section 1	A description of the role and functions of the entity.	Mandatory	3-4
17AE(1)(a)(ii)	Section 1	A description of the organisational structure of the entity.	Mandatory	5
17AE(1)(a)(iii)	Section 1	A description of the outcomes and programmes administered by the entity.	Mandatory	6,7-10



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	10
17AE(1)(aa)(i)	Section 2	Name of the accountable authority or each member of the accountable authority.	Mandatory	10
17AE(1)(a)(ii)	Section 2	Position title of the accountable authority or each member of the accountable authority.	Mandatory	10
17AE(1)(a)(iii)	Section 3	Period as the accountable authority or member of the accountable authority within the reporting period.	Mandatory	103
17AE(1)(b)	n/a	An outline of the structure of the portfolio of the entity.	Portfolio departments mandatory	n/a
17AE(2)	n/a	Where the outcomes and programs administered by the entity differ from any Portfolio Budget Statement, Portfolio Additional Estimates Statement or other portfolio estimates statement that was prepared for the entity for the period, include details of variation and reasons for change.	If applicable, Mandatory	n/a
17AD(c)	Report on the Performance of the entity			
	<i>Annual Performance Statements</i>			
17AD(c)(i); 16F	Section 2	Annual performance statement in accordance with paragraph 39(1)(b) of the Act and section 16F of the Rule.	Mandatory	10
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	78-81
17AF(1)(b)	Section 4	A table summarising the total resources and total payments of the entity.	Mandatory	79, 80

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.	81
17AD(d) Management and Accountability				
<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	68-71



PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
17AG(2)(d) – (e)	n/a	A statement of significant issues reported to Minister under paragraph 19(1)(e) of the Act that relates to non compliance with Finance law and action taken to remedy non compliance.	If applicable, Mandatory	n/a
<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	71
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	71
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	71
17AG(3)(c)	n/a	Information on any capability reviews on the entity that were released during the period.	If applicable, Mandatory	71
<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	65, 72-73

PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
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	72
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"> • Statistics on staffing classification level; • Statistics on full-time employees; • Statistics on part-time employees; • Statistics on gender; • Statistics on staff location; and • Statistics on employees who identify as Indigenous. 	Mandatory	72
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	73
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	73
17AG(4)(c)(ii)	Annexures	The salary ranges available for APS employees by classification level.	Mandatory	102
17AG(4)(c)(iii)	Section 3	A description of non-salary benefits provided to employees.	Mandatory	73



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.	If applicable, mandatory	73
<i>Purchasing</i>				
17AG(6)	Section 3	An assessment of entity performance against the <i>Commonwealth Procurement Rules</i> .	Mandatory	74-75
<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	74

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	74
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	74
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	74
<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	75
<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	74
17AG(10)(b)	Section 3	An outline of the ways in which the procurement practices of the entity support small and medium enterprises.	Mandatory	74
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	83-100

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	103-104
17AD(f)	Other Mandatory Information			
17AH(1)(a)(i)	n/a	If the entity conducted advertising campaigns, a statement that <i>"During [reporting period], the [name of entity] conducted the following advertising campaigns: [name of advertising campaigns undertaken]. Further information on those advertising campaigns is available at [address of entity's website] and in the reports on Australian Government advertising prepared by the Department of Finance. Those reports are available on the Department of Finance's website."</i>	If applicable, Mandatory	n/a
17AH(1)(a)(ii)	Annexures	If the entity did not conduct advertising campaigns, a statement to that effect.	If applicable, Mandatory	105
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	75
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	75
17AH(1)(e)	n/a	Correction of material errors in previous annual report.	If applicable, mandatory	n/a
17AH(2)	Annexures	Information required by other legislation.	Mandatory	105-106

INDEX

A

- abbreviations, v
- accountable authority, 10
- Activity performance statements *see* performance
- administrative tribunal decisions (external scrutiny), 71
- advertising and market research, 105
- AGO *see* Australian Geospatial-Intelligence Organisation (AGO)
- analytic tradecraft, 27
- ANAO *see* Australian National Audit Office
- annual performance statement *see* performance
- Anti-Money Laundering and Counter Terrorism Financing Act 2006*, 51
- ASD *see* Australian Signals Directorate (ASD)
- ASIO *see* Australian Security Intelligence Organisation (ASIO)
- ASIS *see* Australian Secret Intelligence Service (ASIS)
- assets management, 73
- Assistant Inspectors-General, 2, 5
- assumed identities, 50
- Attorney-General, 3, 39
 - ASIO reporting obligations, 24, 28, 29, 33
 - Guidelines under ASIO Act, 7, 30, 32, 33
 - powers, 7, 28
 - requests to, 30
 - submissions to, 35
- Audit Committee, 68
- Auditor-General *see* Australian National Audit Office
- audits, internal, 69
- AusTender, 75
- AUSTRAC *see* Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Australian Commission for Law Enforcement Integrity, 63
- Australian Criminal Intelligence Commission, 2, 52
- Australian Federal Police, 2, 52
- Australian Geospatial-Intelligence Organisation (AGO)
 - compliance oversight, 47
 - inspections of, 46–8
 - Ministerial authorisations, 47
 - privacy rules compliance, 48
 - role and functions, 8, 48

- Australian Human Rights Commission, 63
- Australian Hydrographic Office, 48
- Australian Information Commissioner, 71
- Australian National Audit Office
 - access clauses in contracts, 74
 - audit report, 71, 83–4
- Australian persons
 - intelligence collection on, 39, 40, 44, 45–6, 47
 - privacy protection, 34, 40, 44, 50
- Australian Secret Intelligence Service (ASIS)
 - AUSTRAC information access and use, 51
 - compliance incident reports, 39
 - inquiries relating to, 23
 - inspections of, 37–41
 - Ministerial authorisations, 39
 - Ministerial submissions, 38
 - privacy rules compliance, 40
 - review of operational files, 38
 - role and functions, 7
 - use of force, 2, 41
 - weapons use and issues, 41
- Australian Security Intelligence Organisation (ASIO)
 - analytic tradecraft, 27
 - Attorney-General’s Guidelines, 7, 30, 32, 33
 - AUSTRAC information access and use, 51
 - human source management, 27
 - information exchange with other agencies, 34–5
 - inquiries relating to, 25–6
 - inspections of, 26–37
 - investigative activities, 27
 - Ministerial submissions, 35
 - powers, 2, 33
 - role and functions, 7
 - special intelligence operations, 33
 - special powers, 31
 - telecommunications interception and data, 28–30, 32, 34
 - use of force, 32
 - warrants, 28–30
- Australian Security Intelligence Organisation Act 1979*, 31
 - breaches of, 35–6



Australian Signals Directorate (ASD), 2

inquiries relating to, 22, 24

inspections of, 42–6

Ministerial authorisations, 43, 45

Ministerial submissions, 43

privacy rules compliance, 44

public interest disclosure matters, 61

role and functions, 8

Australian Transaction Reports and Analysis Centre (AUSTRAC), 2, 51, 52

Australians *see* Australian persons

B

Blight, Jake, 5, 68

C

capability reviews, 71

citizenship-related complaints, 2, 53, 54–5

Civil Society Reference Group, 21

Commonwealth Ombudsman, 63, 71

complaints handling

‘contacts’ versus ‘complaints’, 61

IGIS function and powers, 3

non-visa related, 53, 56–9

performance results and discussion, 14–15, 53–9

protecting complainant information, 37

visa or citizenship related, 2, 53, 54–6

see also inquiries

Comprehensive Review of the Legal Framework Governing the National Intelligence Community, 2, 20

consultants, 74

‘contacts’ versus ‘complaints’ *see* complaints handling

Cornall, Robert, 36

corporate and operational planning, 3, 68–9

corporate governance, 68–71

cross-agency inspections, 50–2

D

Defence Intelligence Organisation (DIO)

- AUSTRAC information access and use, 51

- inquiries relating to, 23

- inspections of, 48–9

- privacy guidelines compliance, 49

- role and functions, 8

Department of Home Affairs, 2, 52

Deputy Inspector-General, 5

detention warrants *see* questioning and detention warrants

DIO *see* Defence Intelligence Organisation (DIO)

disability reporting, 75

E

ecologically sustainable development and environmental performance, 105–6

emergency authorisations, 39, 43

enterprise agreement, 65, 73

ethical standards, 4–5, 70

Executive Committee, 68

exempt contracts, 75

external scrutiny of IGIS, 71

F

finance law compliance, 71

financial intelligence *see* sensitive financial information

financial management summary, 78–81

financial statements, 83–100

firearms *see* weapons use and issues (ASIS)

Five Eyes Intelligence Oversight and Review Council, 2, 63–4

force, use of, 2, 32

foreign liaison

- IGIS, 62

- intelligence agencies, 35

fraud control, 70

Freedom of information Act 1982, 75

functions *see* roles and functions

G

geospatial intelligence agency *see* Australian Geospatial-Intelligence Organisation (AGO)
government agencies, liaison with, 62

H

human resources management, 65, 72–3 *see also* staff
Human Rights Law Centre, 21
human source operations, 27

I

identities, assumed, 50
imagery intelligence *see* Australian Geospatial-Intelligence Organisation (AGO)
Independent Reviewer of Adverse Security Assessments, 36
Information Publication Scheme, 75
information security authority *see* Australian Signals Directorate (ASD)
informing the public (Objective 3), 11–12, 20–1
infrastructure, 52
inquiries
 employment of persons for a particular inquiry, 71
 IGIS function and powers, 3
 notification and reporting requirements, 18
 performance results and discussion, 14, 22–6
inquiries by parliamentary committees *see* parliamentary committees
inspections, 3
 AGO activities, 46–8
 ASD activities, 42–6
 ASIO activities, 26–37
 ASIS activities, 37–41
 cross-agency inspections, 50–2
 DIO activities, 48–9
 interim inspection plans for other agencies, 52
 ONA and ONI activities, 49–50
 performance results and discussion, 13, 26–52
 see also names of agencies
Inspector-General of Intelligence and Security
 jurisdiction, 2, 52
 powers, 3
 review of year, 2–8
 role, 3–4

Inspector-General of Intelligence and Security Act 1986, 3, 10, 18, 52

Inspector-General of the Australian Defence Force, 63

Intelligence Services Act 2001, 37

incident reports, 45–6

privacy rules *see* privacy rules compliance

internal audit, 69

international engagement, 2, 63–4

J

Joint Councils for Civil Liberties, 21

judicial decisions, 71

jurisdiction, 2, 52

K

Key Management Personnel, 68, 103–4

L

Law Council of Australia, 21

legislation, 2

letter of transmittal, i

liaising with other accountability or integrity agencies, 62

M

market research, 105

McFarlane, Stephen, 5, 68

Minister for Defence, 8, 24, 43, 44, 45, 46, 47, 48

Minister for Foreign Affairs, 7, 37, 38, 39, 40

Minister for Home Affairs, 7, 35

ministerial and other authorisations to collect intelligence, 39, 43, 45, 47

Ministerial submissions, 35, 38, 43

Ministers

assisting Ministers (Objective 1), 11, 18

IGIS portfolio relationships, 3

N

- non-salary benefits, 73
- Notzon-Glenn, Bronwyn, 5, 68

O

- Office of National Assessments (ONA)
 - inspections of, 49–50
- Office of National Intelligence Act 2018*, 49
- Office of National Intelligence (ONI), 2
 - AUSTRAC information access and use, 52
 - inspections of, 49–50
 - privacy rules compliance, 49–50
 - role and functions, 8
- Office of National Intelligence Rules to Protect the Privacy of Australians*, 49
- Office of the Australian Information Commissioner, 63
- Office of the Commonwealth Ombudsman, 63
- ONA *see* Office of National Assessments (ONA)
- ONI *see* Office of National Intelligence (ONI)
- organisational structure, 2, 5, 68
- outcome and program, 6, 10 *see also* performance
- outreach program, 21, 52

P

- Parliament
 - assuring Parliament (Objective 2), 11, 18–20
- parliamentary committees
 - IGIS submissions and appearances, 3, 18–20
 - scrutiny of IGIS, 71
- Parliamentary Joint Committee on Intelligence and Security, 2, 18–19
- performance
 - accountable authority statement, 10
 - Objective 1: Assisting Ministers, 11, 18
 - Objective 2, Assuring Parliament, 11, 18–20
 - Objective 3, Informing the public, 11–12, 20–1
 - Objective 4, Inquiries, inspections and investigation of complaints, 12–15, 22–61
 - Objective 5, Infrastructure and relationships, 15–16, 62–4
 - Objective 6, High-performing workforce, 16–17, 65–6

performance pay, 73
 personal information protection *see* privacy rules compliance
 personal security *see* protective security
 plans and planning, 3, 68–9
 police services *see* Australian Federal Police
 Portfolio Budget Statements, 6, 10, 78
 portfolio relationship, 3
 premises, 62
 privacy rules compliance, 34, 40, 44, 45–6, 48, 49–50
 protective security, 69
 public engagement, 20–1
Public Governance, Performance and Accountability Act 2013, iv, 71
 public interest disclosure matters, 53, 59–61
Public Service Act 1999, section 24(1) determinations, 73
 purchasing, 74–5
 purpose, 6–7, 10

Q

questioning and detention warrants, 32

R

recruitment (IGIS), 2
 relationships, 52–64
 remuneration, 70, 73, 102–4
 Richardson Review *see* Comprehensive Review of the Legal Framework Governing the National Intelligence Community
 risk management, 69–70
 roles and functions
 IGIS, 3–4
 intelligence agencies, 7–8
Rules to Protect the Privacy of Australians *see* privacy rules compliance

S

security, protective, 69
 security assessments by ASIO, 36–7
 complaints, 56, 57, 60
 Senate Estimates hearings, 18
 Senate Finance and Public Administration Committee, 20

- Senate Legal and Constitutional Affairs Committee, 19–20
- senior management committees, 68
- senior positions, 68, 103–4
- sensitive financial information, 51–2
- signals intelligence *see* Australian Signals Directorate (ASD)
- small business participation in procurement, 74
- special intelligence operations, 33
- staff
 - employment arrangements, 73
 - enterprise agreement, 65, 73
 - immersive placements, 65
 - remuneration, 70, 73, 102–4
 - secondments, 2
 - training and development, 65
 - workforce profile, 72
- stakeholder engagement, 21, 52, 62
- Stone, Hon Margaret, 3, 68 *see also* Inspector-General of Intelligence and Security
- submissions to Ministers *see* Ministerial submissions
- surveillance devices, 36

T

- taxation information, 34–5
- Telecommunications (Interception and Access) Act 1979* (TIA Act)
 - ASD compliance, 44–5
 - ASIO compliance, 28–30, 32
 - ASIO new powers, 2, 33
- telecommunications interception and data, 28–30, 32, 34

V

- values, 4–5
- visa-related complaints, 2, 53, 54–6

W

- weapons use and issues (ASIS), 41
- whistle-blower protection scheme *see* Public Interest Disclosure matters
- work health and safety (IGIS staff), 105

