



IGIS

INSPECTOR-GENERAL OF
INTELLIGENCE AND SECURITY

2017–2018

ANNUAL REPORT



IGIS CONTACT INFORMATION

LOCATION

One National Circuit
BARTON ACT 2600

WRITTEN INQUIRIES

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

PARLIAMENTARY AND MEDIA LIAISON

Phone: (02) 6271 5692
Email: info@igis.gov.au

GENERAL INQUIRIES

Phone: (02) 6271 5692
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) 6271 5692. 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 2018



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

Design and typesetting by Spectrum Graphics www.spectrumgraphics.com.au

Printed by Elect Printing www.electprinting.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 2017 to 30 June 2018.

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

Margaret Stone

Inspector-General

24 September 2018

CONTENTS

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

SECTION ONE

OVERVIEW **1**

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**

Activity 1	Inquiries	11
Activity 2	Inspections	15
Activity 3	Responding to complaints	44
Activity 4	Public interest disclosures	50
Activity 5	Advice to Parliamentary Committees and others	53
Activity 6	Evidence to the AAT and the Australian Information Commissioner	55
Activity 7	Engagement with the intelligence agencies and the public	56
Activity 8	Liaising with other accountability or integrity agencies	59

SECTION THREE

MANAGEMENT AND ACCOUNTABILITY 63

Part 3.1: Corporate governance	64
Part 3.2: Management of human resources	67
Part 3.3: Other information	69

SECTION FOUR

FINANCIAL MANAGEMENT 71

Part 4.1: Financial summary	72
Part 4.2: Financial statements	76

SECTION FIVE

ANNEXURES 97

Annexure 5.1: IGIS salary scale	98
Annexure 5.2: Other mandatory information	99
Annexure 5.3: Requirements for annual reports	100
Index	109

ABOUT THIS REPORT

This is the Inspector-General of Intelligence and Security's annual report for the period from 1 July 2017 to 30 June 2018.

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 2018-19. Section One also outlines our role and functions, 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 2017-2021.

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

AAT	Administrative Appeals Tribunal
AML/CTF Act	<i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i>
ACLEI	Australian Commission for Law Enforcement Integrity
ACIC	Australian Criminal Intelligence Commission
ADF	Australian Defence Force
AFP	Australian Federal Police
AGO	Australian Geospatial-Intelligence Organisation
AHRC	Australian Human Rights Commission
AIC	Australian Intelligence Community
APS	Australian Public Service
ASIO	Australian Security Intelligence Organisation
ASIO Act	<i>Australian Security Intelligence Organisation Act 1979</i>
ASIS	Australian Secret Intelligence Service
ASD	Australian Signals Directorate
AUSTRAC	Australian Transaction Reports and Analysis Centre
CIR	Compliance Incident Report
DIO	Defence Intelligence Organisation
FOI	Freedom of information
FOI Act	<i>Freedom of Information Act 1982</i>
IGIS	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>
OCO	Office of the Commonwealth Ombudsman
ONA	Office of National Assessments
ONA Act	<i>Office of National Assessments Act 1977</i>
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PGPA Act	<i>Public Governance, Performance and Accountability Act 2013</i>
PGPA Rule	Public Governance, Performance and Accountability Rule 2014
PID Act	<i>Public Interest Disclosure Act 2013</i>
PID	Public Interest Disclosure
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

Democratic values require intelligence agencies to be subject to independent oversight and review. Australia's intelligence agencies have significant human and technical capabilities and some extraordinary legal powers and immunities. Without strong and credible oversight there may be a loss of trust between the agencies and the public. Intelligence agencies must act, and must be seen to act, with legality, with propriety and with proper regard for human rights. It is the core work of this office to hold intelligence agencies to account and to assist Ministers and the Parliament in overseeing and reviewing the work of intelligence agencies.

This report contains an account of the past year's core work, in particular, in the performance statement in Section 2. In brief, two inquiries commenced in the previous reporting period and were finalised and two more were initiated in this reporting period. We have continued the development of our inspection program to target high risk areas, focusing on in-depth investigations rather than on the breadth of the inspection program. Inspections covered a wide range of ASIO's activities including investigative activities, analytic products, human source management, telecommunications interception warrants and special powers functions. Oversight of the activities of agencies governed by the *Intelligence Services Act 2001* focused on the performance of their statutory functions and their compliance with ministerial authorisations and directions including Privacy Rules applicable to ASIS, ASD and AGO and, in this time of dual citizenship, the difficulty of determining who is an "Australian person" as defined in section 3 of the *Intelligence Services Act 2001*.

The office is gratified by the co-operation it received from all agencies. They responded willingly to our briefing requests, assisting us to understand the complexities and challenges of their work and the impact of compliance requirements. Increasingly there is a culture of self-reporting compliance breaches and prospectively briefing this office about proposed operations, thus enabling us to make useful comments about compliance aspects. We have frequent meetings with each agency in which we discuss issues of compliance (both legality and propriety) relevant to their current activities.

An important aspect of our work is responding to and resolving complaints from the public or from members of the intelligence agencies. This includes complaints falling within the Public Interest Disclosure scheme which is designed to encourage public officials to report suspected wrongdoing in the public sector and protect them from reprisals. In the last year the number of visa-related complaints continued to rise (by 10%) however public interest disclosures and other complaints were relatively stable.

Communication with the public, with other Government bodies and with Parliamentary members and officials is an important aspect of our work in monitoring and supporting compliance. My officers and I give presentations to the agencies both in Australia and overseas explaining the importance of compliance, our approach to oversight and how we can assist with compliance. Appearances before Senate Estimates committees and the Parliamentary Joint Committee on Intelligence and Security, as well as presentations to the general public help us to assure the Parliament and the public that intelligence and security matters are subject to rigorous scrutiny.

We continue to develop links with international counterpart bodies, primarily, but not limited to, our five-eyes colleagues. In October 2017, I attended the annual conference of the Five-Eyes Intelligence Oversight and Review Council meeting in Canada together

with the Deputy Inspector-General. In October this year, this office will be hosting the 2018 conference in Canberra.

In addition to the core work of the office significant resources have been directed to preparing for the additional oversight responsibilities flowing from the recommendations of the *2017 Independent Intelligence Review*. The Government accepted that the role of the Inspector-General of Intelligence and Security be extended to oversight of the intelligence functions of four additional agencies, the Australian Federal Police, the Department of Immigration and Border Protection – now the Department of Home Affairs, the Australian Criminal Intelligence Commission, and the Australian Transaction Reports and Analysis Centre.

Effective oversight of the intelligence functions of the four additional agencies will require an in-depth understanding of the intelligence activities of each of these agencies and how those activities fit into their broader operations. Work has already begun on developing this understanding and the task will be ongoing. Each of these four agencies is also subject to oversight by other bodies including the Office of the Commonwealth Ombudsman, Australian Commission for Law Enforcement Integrity, Australian Human Rights Commission and the Office of the Australian Information Commissioner. We are working closely with these bodies to avoid any duplication of effort.

The Review also recommended increasing the office resources to enable effective oversight of these additional agencies and to enhance the oversight of the additional powers given to intelligence agencies in recent years. The 2018-19 Budget allocated the funds necessary to allow the agency to sustain a full time staff of 55 and to move to new premises necessary to accommodate the additional staff. Expanding the size of the office from 17 to 55 staff by the end of 2019-20 requires significant internal resources for recruiting and training and depends on the efficient completion of high level security vetting clearances by the Australian Government Security Vetting Agency. The move to new premises involves the construction of a very high security facility as well as upgrading information and computer technology facilities. Together these two elements amount to a very substantial challenge.

While much will be done in the coming year it is clear that the future of this office and its oversight responsibilities will be shaped in response to the contemporary and future challenges recognised by the *2017 Independent Intelligence Review* “as a result of transforming geopolitical economic, societal and technological changes”.

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 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.

ORGANISATIONAL STRUCTURE

As at 30 June 2018, the office had 23 APS staff. The Inspector-General is supported by a Deputy Inspector-General and an Assistant Inspector-General. The Deputy Inspector-General has responsibility for legal and parliamentary matters, as well as finance and office management. The Assistant Inspector-General manages the staff responsible for inspection programs, complaints handling and projects.

Figure 1.1: IGIS organisational structure at 30 June 2018



IGIS APPROACH TO ROLE

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.

OUTCOME AND PROGRAM STRUCTURE

The office has one outcome, as noted in our 2017-18 Portfolio Budget Statement (PBS). Our outcome is:

The provision of independent assurance for the Prime Minister, senior Ministers and Parliament as to whether Australia's intelligence agencies act legally and with propriety by inspecting, inquiring into and reporting on their activities.

The "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 2017-21* describes the responsibilities of the office as:

to assist Ministers in the oversight and review of the Australian intelligence agencies, to provide assurance to Parliament and the public about the scrutiny of the operation of those agencies, and to assist in investigating intelligence and security matters.

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
- 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
- oversee the operation of the PID scheme in the intelligence agencies

Under the *Archives Act 1983* and the *Freedom of Information Act 1982*, the Inspector-General may also be called on to provide expert evidence concerning national security, defence, international relations and confidential foreign government communications exemptions to the Administrative Appeals Tribunal and the Australian Information Commissioner.

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 (the Organisation) 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.

During the reporting period, the Attorney-General was responsible for ASIO until 10 May 2018 when responsibility for the Organisation was transferred to the Minister for Home Affairs. The Attorney-General continues to exercise 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.

OFFICE OF NATIONAL ASSESSMENTS (ONA)

ONA is established by the *Office of National Assessments Act 1977* (ONA Act) and provides "all source" assessments on international political, strategic and economic developments to the Prime Minister and the Government. ONA uses information collected by other intelligence and government agencies, diplomatic reporting and open sources, including the media, to support its analysis.

Under its Act, ONA is responsible for coordinating and reviewing Australia's foreign intelligence activities and issues of common interest in Australia's foreign intelligence community, and the adequacy of resourcing provided to Australia's foreign intelligence effort.

The responsible Minister for ONA is the Prime Minister.

DEFENCE INTELLIGENCE AGENCIES

During the reporting period, three of the six intelligence agencies were within the Department of Defence (Defence): the Defence Intelligence Organisation (DIO), the Australian Geospatial-Intelligence Organisation (AGO), and the Australian Signals Directorate (ASD). The functions of ASD and AGO are set out in the ISA and their activities are regulated by a series of ministerial directions, ministerial authorisations and Privacy Rules.

The responsible Minister for the Defence agencies is the Minister for Defence.

DEFENCE INTELLIGENCE ORGANISATION (DIO)

DIO is 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 Australian Defence Force (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.

AUSTRALIAN GEOSPATIAL-INTELLIGENCE ORGANISATION (AGO)

AGO is Australia's national geospatial intelligence agency. AGO's geospatial intelligence, derived from the fusion of analysis of imagery and geospatial data, supports Australian Government decision making and assists with the planning and conduct of ADF operations. AGO also gives direct assistance to Commonwealth and State bodies responding to security threats and natural disasters.

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 establishes ASD as a statutory agency, the *Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Act 2018*, was assented to on 11 April 2018 and commenced on 1 July 2018.

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 2017-18 annual performance statement of the Office of the Inspector-General of Intelligence and Security, 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

Inspector-General of Intelligence and Security

Figure 2.1: Results at a glance

PERFORMANCE RESULTS AT A GLANCE

Inquiries were conducted in a timely way. All findings and recommendations were accepted. At the end of the reporting period not all recommendations had yet been implemented.

We inspected more than 75% of agency activity categories for five of the six agencies we oversee.

We acknowledged 99% of complaints and referrals within five business days, and 82% of visa-related complaints were resolved within two weeks.

We acknowledged 100% of public interest disclosures within five business days.

All advice to parliamentary committees was provided by the agreed date.

All evidence to the Australian Information Commissioner was provided by the agreed date.

We conducted 15 presentations to AIC employees.

We conducted 16 presentations to raise public awareness of the office.

Regular liaison with other accountability and integrity agencies was conducted as required.

ACTIVITY 1 INQUIRIES

ABOUT INQUIRIES

Under the IGIS Act, the Inspector-General can conduct an inquiry on the basis of a complaint, on the IGIS's own motion, or in response to a ministerial request. In respect of inquiries the Act provides certain immunities and protections. It also allows the Inspector-General to use strong coercive powers including to compel the production of information and documents, to enter premises occupied or used by a Commonwealth agency, to require the attendance of persons to answer questions relevant to the matter under inquiry, to administer an oath or affirmation and examine the person on that oath or affirmation.

The IGIS Act protects persons who have given information under compulsion from any penalty under Commonwealth or Territory law that would ordinarily arise from disclosing that information. The responsible Minister is advised when the Inspector-General begins an inquiry into an agency and is also advised of any conclusions or recommendations arising from the inquiry. The Inspector-General also provides opportunities for Ministers, agency heads and affected individuals to comment during the course of an inquiry.

PERFORMANCE SUMMARY

Conducting inquiries as appropriate (which may be "own motion", in response to complaints or referrals, or at the request of intelligence agency Ministers or the Prime Minister).

Performance criteria: timeliness of completion of inquiries; level of acceptance by intelligence agencies of findings and recommendations of inquiries conducted.

Targets: 100% of inquiry recommendations accepted; 100% of inquiry recommendations implemented.

Other activity measures: Number of inquiries conducted; duration of each inquiry completed.

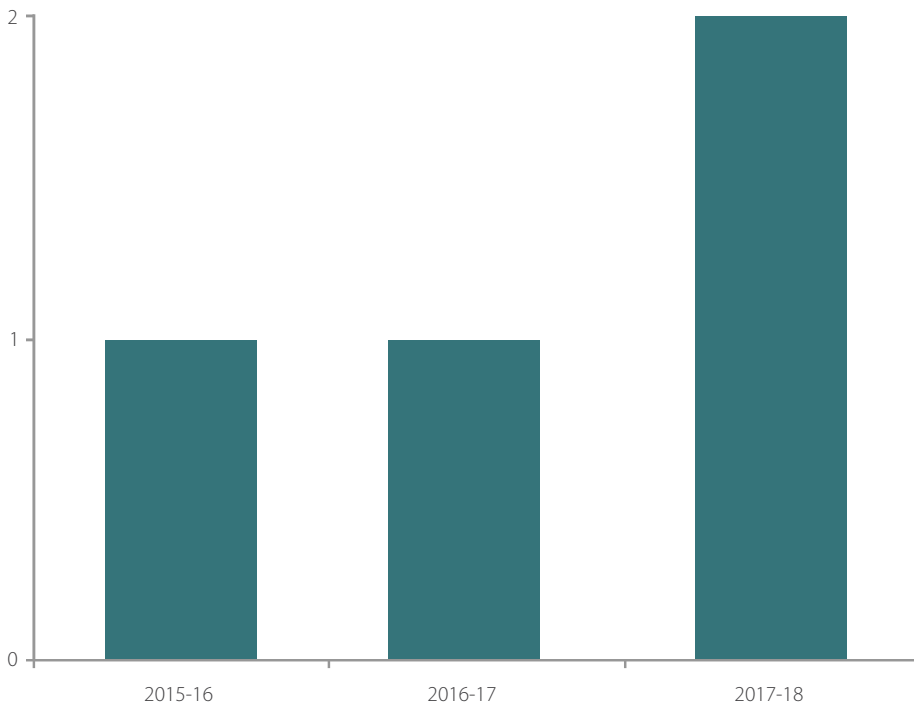
Source: Portfolio Budget Statements 2017-18, p. 257; IGIS Corporate Plan 2017-2021, p. 5.

QUANTITATIVE PERFORMANCE INDICATORS

Figure 2.2: Performance indicators – conducting inquiries

SUBJECT OF INQUIRY	DIO ANALYTIC INDEPENDENCE	ASD MATTER 2017	ASD MATTER 2018	ASIO MATTER
Agency	DIO	ASD	ASD	ASIO
Source	IGIS own motion	IGIS own motion	Requested by the Minister for Defence	IGIS own motion
Date initiated	14 November 2016	2 February 2017	30 May 2018	14 February 2018
Date finalised	8 September 2017	14 July 2017	Open	Open
Duration (days)	299 days	163 days	N/A	N/A
Number of recommendations	2	5	N/A	N/A
Percentage of recommendations accepted	100%	100%	N/A	N/A
Percentage of recommendations fully implemented	0%	60%	N/A	N/A

Figure 2.3: Number of inquiries concluded by year



INQUIRIES CONDUCTED DURING 2017-18

During the 2017-18 reporting period two inquiries were concluded. One inquiry had a duration of 299 days and the other 163 days. These durations were considered reasonable taking into account IGIS staffing levels. Two inquiries were in progress at the end of the reporting period. A short summary of these four inquiries is provided below.

No inquiries were conducted pursuant to sections 8(1)(d) and 8(3)(c) respectively of the IGIS Act.

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

In September 2017 we completed the third inquiry into the analytic independence and integrity of the 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 analytic integrity of the DIO process for producing reports is sound, although some areas for continuing improvement were highlighted in the inquiry. The inquiry made two recommendations relating to analytic tradecraft policy and record keeping and several suggestions for improvement, which DIO accepted. Although the full report is classified, a more detailed unclassified summary of this inquiry can be found on the IGIS website www.igis.gov.au/publications-reports/public-reports.

On 9 March 2018 DIO reported on its progress in implementing the two recommendations and in June 2018 the office sought a further update. Although progress in implementing recommendation one was initially slow, DIO has developed a new draft policy and we are satisfied that it will address the recommendation once complete. In relation to recommendation two, DIO was incorrectly advised that this had been addressed earlier but in July became aware that a required technical change had not been implemented. DIO undertook to address this, and we are satisfied that the recommendation will be implemented once this occurs.

INQUIRY INTO AN AUSTRALIAN SIGNALS DIRECTORATE MATTER 2017

In July 2017 this office completed an inquiry into an ASD matter pursuant to section 8(2) of the IGIS Act. Although this matter was finalised in the current reporting period, a summary of the findings and outcomes were discussed in the 2016-17 Annual Report. The report included five (classified) recommendations designed to ensure that the situation would not arise in the future and to streamline communications with Ministers and with the Inspector-General. ASD accepted all the recommendations and reported its progress on their implementation in December 2017, and subsequently in June 2018. We reviewed ASD's advice and consider that ASD has sufficiently implemented three of the five recommendations and we are satisfied with the progress on the remaining two.

Soon after the end of the reporting period ASD finalised implementation of the final two recommendations.

INQUIRY INTO AN AUSTRALIAN SIGNALS DIRECTORATE MATTER 2018

On 30 May 2018 this office commenced an inquiry into ASD to examine the circumstances surrounding reported breaches of section 7 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act), including the timeliness and adequacy of reporting by ASD to this office and to the Minister for Defence. The inquiry is ongoing and further details will be provided in the next annual report.

INQUIRY INTO AN AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION MATTER

In February 2018 this office commenced an inquiry into an ASIO matter pursuant to section 8(2) of the IGIS Act. The inquiry will examine the conduct and details around a multi-faceted, multi-agency foreign intelligence collection operation led by ASIO in 2017. The inquiry is ongoing and further details will be provided in the next annual report.

ACTIVITY 2 INSPECTIONS

ABOUT INSPECTIONS

The office regularly examines selected agency records to ensure that the activities of the intelligence agencies comply with the relevant legislative and policy requirements and to identify issues before there is a need for major remedial action. These inspections include IGIS staff directly accessing electronic records, reviewing hardcopy documentation as well as retrieving and checking information independently.

Inspections concentrate on the potential impact of intelligence collection on the privacy of Australians. For this reason our inspections mainly focus on the activities of ASIO, ASIS, AGO and ASD, each of which has intrusive powers and investigative techniques. Inspections relating to DIO and ONA are generally limited to ensuring that their assessments comply with administrative privacy guidelines, and that their independence is not compromised. The small size of the office compared to the size of the agencies the office oversees, combined with the breadth and complexity of the operations of intelligence agencies, means that the office has to be well informed to target our inspection activities to the areas of highest potential risk.

Inspections of these agencies focus on whether the agency is acting in accordance with its statutory functions, its compliance with any guidance provided by the responsible Minister and its own internal policies and procedures. Inspection may consist of routine inspections and inspection projects that target specific issues as determined by the Inspector-General.

PERFORMANCE SUMMARY

Undertaking comprehensive inspection and program of visits to monitor and review intelligence agencies' operational activities.

Performance criteria: Range of inspection work undertaken.

Targets: Inspection of at least 75% of each agency's activity categories.

Other activity measures: N/A.

Source: Portfolio Budget Statements 2017-18, p.257, *IGIS Corporate Plan 2017-21*, p. 5.

The IGIS PBS provides for performance to be measured by both quantitative and qualitative information. One performance indicator listed in both the IGIS PBS 2017-18 and IGIS Corporate Plan 2017-21 is "range of inspection work undertaken", with the associated quantitative target of inspecting at least 75% of an agency's activity categories. The categories are determined by the Inspector-General and are based on the underlying functions of the agency laid down in the relevant legislation, namely, the ISA for AGO, ASD and ASIS; the ASIO Act for ASIO; and the ONA Act for ONA. The role of DIO is set out in a mandate agreed by the Minister for Defence, rather than in legislation. As a result, and given it is an assessment agency without the intrusive powers of the collection agencies, activity categories for DIO have been established with reference to its mandate, organisational structure and product types.

A summary of this office's performance is outlined in the following table.

Figure 2.4: Performance indicators - Inspections

AGENCY	NUMBER OF ACTIVITY CATEGORIES	ACTIVITY CATEGORIES INSPECTED	OUTCOME
ISA agencies and ASIO			
AGO	8	7	Target achieved
ASD	6	6	Target achieved
ASIS	8	8	Target achieved
ASIO	7	6	Target achieved
Assessment agencies			
DIO	4	4	Target achieved
ONA	3	1	Due to staffing constraints the target was not achieved.

INSPECTION OF ASIO ACTIVITIES

ASIO's activities have been categorised based on the functions of the agency set out in section 17 of the ASIO Act, namely:

- intelligence collection
- intelligence communication
- advice about security of Ministers and Commonwealth authorities in relation to their functions and responsibilities
- furnishing security assessments to States and state authorities
- advice to Ministers and Commonwealth authorities about protective security
- collection of foreign intelligence
- co-operation with and assistance to other agencies

During this reporting period the ASIO inspection team met the office target of inspecting at least 75% of ASIO's activity categories. Priority was given to reviewing the Organisation'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.

An ASIO operation which is the subject of a current inquiry pursuant to section 8(2) of the IGIS Act, is reported separately (see page 14).

REGULAR INSPECTIONS OF INVESTIGATIVE CASES

It is not possible to monitor all ASIO activities. Accordingly, IGIS staff inspect a sample of activities selected on the basis of risk and available resources. IGIS staff have direct access to some of ASIO's information technology and records management systems. During the reporting period, IGIS staff liaised with ASIO to acquire increased direct access to ASIO systems beyond that granted in the previous reporting period. The increased direct access improved our ability to view and analyse a wider range of ASIO's records without relying on ASIO providing the required documents.

Throughout the reporting period IGIS staff concentrated on reviewing those cases involving the most intrusive methods and activities, as well as those activities that presented an increased likelihood of non-compliance with legislation or policy – for example, warrants approved by the Attorney-General, access to prospective data authorisations, and investigative activity targeting minors. Inspections of ASIO's investigative cases focused on:

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

The Organisation 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.

Deficiencies in record keeping were evident in almost all areas inspected in ASIO during the reporting period. While ASIO instituted a number of measures to improve record keeping in 2017-18, the office will maintain a strong focus on this aspect in all future inspections to provide assurance that ASIO officers meet their record keeping obligations.

ANALYTIC TRADECRAFT

ASIO produces a range of analytic products including security assessments, applications for warranted powers, investigative reviews and published analytic products. Within the AIC, ASIO's unique role in collection and assessment means that these products have greater potential to intrude into the privacy of Australians than those of DIO and ONA. Also these assessments may adversely affect the interests of individuals; for example, ASIO's security assessments may recommend that the Government take adverse action against a person by cancelling their passport. These assessments may also result in ASIO providing specific policy guidance to the Government.

IGIS staff inspections of these analytic products gave rise to some concerns about adherence to ASIO policies; specifically, policies relating to tradecraft, quality assurance, referencing, record keeping and critical review. However, during the reporting period ASIO made considerable progress in addressing these issues.

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. No substantive issues of concern were identified by IGIS staff when reviewing these activities.

ASIO WARRANTS

ASIO can intercept telecommunications and use other intrusive powers following the issue of warrants by the Attorney-General. Authority for telecommunications interception is provided in the TIA Act. The ASIO Act provides the authority for other powers, including searches, computer access and surveillance devices.

Throughout the reporting period IGIS staff inspected a large number of warrants, primarily as part of the regular inspection of investigative cases. As with the last reporting period, IGIS staff identified a number of typographical errors in warrant documents. While some typographical errors are minor and may be overlooked, others have the potential to mislead or to cause breaches; consequently we continue to draw these errors to ASIO's attention. ASIO has strong practices in place, intended to limit the frequency of typographical errors in warrant documentation. In response to IGIS findings, ASIO has further refined its processes to help ensure that warrant documentation is accurate.

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 minor increase in the number of breaches in this reporting period. The circumstances in which these occurred are summarised below.

BREACHES OF THE TIA ACT

Unlawful intercept

Section 7 of the TIA Act prohibits the interception of communications passing over a telecommunications system. In the reporting period ASIO self-reported three breaches of section 7.

In the first instance, ASIO caused the interception of communications to and from a particular telecommunications service, without warrant authorisation; the problem was caused by the erroneous transcription of a telephone number. Once it became aware of the incident, the Organisation immediately took steps to cease interception of the service and the intercepted communications were deleted. ASIO subsequently amended their practices to ensure such transcription errors are less likely to occur.

In the second instance, a breakdown in internal processes led the Organisation to intercept the communications of a particular telecommunications service for two months without a warrant. In the third instance, data was collected on two services for 20 days in breach of a warrant condition. In both cases, ASIO advised the office that the unauthorised intercept was deleted.

ASIO advised the office of four instances of over-collection arising from incorrect information given by the service provider. In all instances, ASIO advised that the non-target interception was deleted.

ASIO also notified the office of an issue which occurred during the previous reporting period. In this instance a change in the subscriber of the service led to the interception of communications not relevant to security. Here, the service listed on the warrant was initially used by a person of interest to ASIO. During the period of the warrant the service was disconnected and re-sold to a new customer. The new customer's communications were intercepted for four days before ASIO recognised the error. Although ASIO was aware that the number had been disconnected, the Organisation incorrectly assumed that the service would be reconnected to the person of interest. ASIO deleted the non-target interception and modified internal procedures to reduce the risk of this type of issue arising in the future.

Another agency identified instances of unlawful interception of telecommunications executed under ASIO warrants involving section 12 of the TIA Act. Section 12 of the TIA Act enables the Director-General of Security, or his delegate, to authorise any person to execute a warrant on ASIO's behalf. In one case, despite ASIO's advice to the agency, the section 12 authorisation list for this warrant did not authorise the agency's officers to execute the warrant on ASIO's behalf. Consequently, the agency's officers executed the warrants without authorisation. The error was discovered when the agency requested a copy of the section 12 list. The agency advised ASIO of the omission and ASIO issued a revised section 12 list authorising the agency officers to execute the warrant on ASIO's behalf. In the second case, a number of the agency's officers not included in the section 12 authorisation list undertook unlawful collection activities. The office is currently conducting an inquiry into another agency relating to this second case. Additional information on this matter is reported on page 36.

Breach of section 16(2)

During the reporting period, IGIS staff identified an instance that occurred in 2016 where ASIO took two days to notify a carrier that interception of a service was no longer required. Section 16(2)(c) of the TIA Act requires ASIO advise the carrier "immediately". This office considers that, in the absence of special circumstances, a lapse of two days does not meet the requirement of immediate notification. The office has requested ASIO provide advice to carriers more promptly.

BREACHES OF THE ASIO ACT

ASIO notified the office of one instance where ASIO officers executed a warrant without authority. Section 24 of the ASIO Act allows the Director-General or an authorised person to approve a person, or class of persons, as authorised to exercise authority conferred by the warrant. Although ASIO obtained a warrant allowing the Organisation to undertake a particular activity, the activity was undertaken by ASIO officers who were not on the authorisation list. ASIO is considering measures to minimise the risk of similar breaches.

ASIO advised the office of errors relating to two identified person warrants. An ASIO internal investigation to determine whether the errors were in breach of the ASIO Act was ongoing at the end of the reporting period.

BREACH OF REPORTING REQUIREMENTS IN THE TIA ACT AND ASIO ACT

Section 17 of the TIA Act requires ASIO to furnish the Attorney-General with a report detailing the extent to which the warrant assisted the Organisation. Section 7(2) imposes additional requirements for reports relating to "named person warrants" issued under sections 9A or 11B. These reports must include details of the telecommunications service to or from which each intercepted communication was made.

IGIS staff identified that ASIO furnished a report to the Attorney-General advising that all services named on a warrant had been intercepted, without establishing the accuracy of this advice. The office requested ASIO to confirm whether the advice provided to the Attorney-General was accurate and whether any other warrant reports were affected by this issue. ASIO advised that it had not sought confirmation prior to drafting the report, due to ASIO's confidence that all services targeted for interception would be intercepted. From ASIO's response it is apparent that, during the reporting period, ASIO did not take the requisite steps to comply with the Organisation's reporting obligations under section 17(2) of the TIA Act.

Section 34 of the ASIO Act requires the Director-General of Security to provide a report to the Minister describing the extent to which the action taken under the warrant has assisted ASIO in carrying out its functions. During the reporting period the office found that ASIO provided section 34 reports to the Attorney-General prior to the expiry of warrants; for example, in one case, ASIO's warranted access continued 19 days after the report was provided to the Attorney-General. As the warrant was not renewed, any activity during this 19 day period was not the subject of legislative reporting.

On inquiry, ASIO confirmed that its standard practice was to provide warrant reports to the Attorney-General prior to the conclusion of the warrant. Accordingly, the problem affected a significant number of warrants granted under both the ASIO Act and TIA Act. Although this has been an accepted practice for many years, this office is of the view that this procedure does not comply with the requirements of section 34 of the ASIO Act or section 17 of the TIA Act. In accordance with this view, ASIO changed its practices so that warrant reports are now provided to the Attorney-General after the warrant authorisation has ended.

On 29 June 2017 ASIO notified this office that it had erroneously advised the Attorney-General that a surveillance device authorisation, made pursuant to an identified person warrant, was not executed. ASIO provided a supplementary warrant report to the Attorney-General to correct the error. During this reporting period IGIS staff reviewed the supplementary report and discussed the circumstances surrounding this error with ASIO staff.

OTHER WARRANT MATTERS

Use of inappropriate warrant type

Under the TIA Act the Director-General of Security may request the issue of telecommunication service warrants under section 9 and named person warrants under section 9A. In 2016, ASIO obtained a section 9 warrant for coverage of a legitimate and proper subject of ASIO attention. This approach was taken in at least one other warranted operation.

While it was accepted that throughout the operation ASIO had taken reasonable steps to ensure that it only intercepted appropriate information; and that there was no evidence of improper interference with the privacy of Australians, IGIS staff queried whether a section 9 warrant was the most appropriate warrant for this matter. The office expressed concern that the expansive interpretation adopted by ASIO of the phrase "telecommunications service" did not accord with the narrow interpretation courts traditionally apply when interpreting the scope of intrusive statutory powers. ASIO agreed to replace the warrant with a named person warrant which resolved the matter.

Authorisation to execute ASIO warrants

Both the TIA Act and ASIO Act empower the Director-General of Security, or his delegate, to authorise any person or a class of persons to execute a warrant granted to ASIO on the Organisation's behalf. In a number of inspections IGIS staff raised issues regarding the use of these powers. Poor record keeping practices meant that in several cases it was unclear who was authorised to exercise the Organisation's warranted powers, and how ASIO had instructed those persons to exercise them. In one matter, discussed earlier at page 19, this approach caused the unlawful interception of communications by incorrectly advising a partner agency that the agency's staff were authorised to execute the warrant when this was not the case. This was not an isolated incident (see also page 36). The office is currently considering ASIO's use of authorisations and the outcome of these considerations will be included in the next reporting period.

Description of services

When ASIO submits a request to the Attorney-General to obtain a named person warrant under sections 9A or 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 the reporting period IGIS staff queried whether ASIO's warrant documentation made clear the nature of the services ASIO intended to target. ASIO's consideration of this matter is ongoing.

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 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, ASIO did not advise this office of any use of force against persons during the execution of ASIO warrants by ASIO or law enforcement officers.

SPECIAL INTELLIGENCE OPERATIONS

ASIO's special intelligence operations 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 a special intelligence operation ASIO can seek these authorisations to assist in the performance of its special powers functions. The legislation requires ASIO to notify the Inspector-General as soon as practicable after an authority is given. All special intelligence operations approved during the reporting period were notified to the Inspector-General on the same day as approval was granted by the Attorney-General.

The legislation also requires ASIO to provide a written report on each special intelligence operation to the Attorney-General and the Inspector-General. As the details of special intelligence operations are highly sensitive and cannot be included in a public report it is not possible to give more information about the operations here. However, IGIS staff reviewed documentation on special intelligence operations and found no outstanding reporting requirements for the reporting period. During the reporting period one authorisation reviewed contained a discrepancy which was corrected prior to any operational activity occurring. No other substantive issues or concerns were identified when reviewing these activities.

ACCESS TO TELECOMMUNICATIONS DATA

Sections 175 and 176 of the TIA Act empower certain ASIO personnel to authorise 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. Our inspections of ASIO's access to prospective telecommunications data and historical telecommunications data showed that the prospective data authorisations were authorised at the appropriate level, were undertaken in connection with ASIO's functions and demonstrated regard for the Attorney-General's Guidelines (the 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. IGIS staff identified a number of breaches of the Guidelines during the reporting period, mainly relating to authorisation for investigative activity and the use of personal information. Some of these issues are discussed later in this report at page 23.

The Guidelines require that the initiation of an 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. IGIS staff assess this is not a systemic issue.

The Guidelines also require ASIO to review each of the Organisation's investigations on an annual basis. IGIS staff identified a number of breaches of this requirement across the Organisation. There were a number of investigations that, as a consequence of administrative error, were overlooked until IGIS staff identified and raised the breach with the relevant investigative area.

PROVISION OF INACCURATE AND MISLEADING INFORMATION

The Guidelines require that ASIO take all reasonable steps to ensure that personal information it discloses is accurate and not misleading. In one instance IGIS staff found that ASIO did not specifically advise another Australian intelligence agency of a person's Australian status under the ISA, when making a request of that agency as it is required to do so. This had the effect of the other agency considering the individual not to be an Australian, resulting in inaccurate information being entered into the partner agency's repository for target data.

ASIO proactively reviewed all such requests for information made by the relevant branch in 2016 and 2017. ASIO's review identified a small number of errors and an inconsistent approach to identifying subjects as Australian persons in requests to other agencies. The errors have been corrected in the other agency's databases. All staff in the relevant branch have undertaken additional training to reduce the risk of this type of problem recurring. The office is satisfied with ASIO's actions directed to preventing the provision of inaccurate information.

RETENTION OF PERSONAL INFORMATION

The office also raised issues regarding ASIO's retention of sensitive financial records and telecommunications data. The Guidelines require the Director-General of Security to take all reasonable steps to ensure that ASIO does not use or handle personal information, unless reasonably necessary for the performance of ASIO's statutory functions or as otherwise required by law. IGIS staff identified a small number of cases in which personal information was retained by ASIO in circumstances where ASIO had assessed that the records were not relevant to security. See also page 43.

IGIS staff identified a small number of instances in which ASIO retained metadata, or telecommunications interception data that was not relevant to security. In one case ASIO intercepted a telecommunications service for two months before realising that the service was not used by ASIO's investigative target. ASIO ceased interception, but did not delete the data for over a year. The office raised concerns that the significant period taken to delete the data indicated deficiencies in ASIO's internal processes.

ASIO EXCHANGE OF INFORMATION WITH AUSTRALIAN GOVERNMENT AGENCIES

ASIO's relationship with other Australian Government agencies includes the exchange of information. Exchanges of sensitive personal information are of particular interest to the office and are subject to IGIS staff review as part of our 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. Some areas of concern were identified during these inspections. These concerns are addressed in ASIO's sharing of AUSTAC information which is discussed separately (see page 43).

ACCESS TO TAXATION INFORMATION

Sections 355-70 of Schedule 1 to the *Taxation Administration Act 1953* provide 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 access to sensitive tax information carried over from the previous financial year. No issues of concern were identified in this inspection. The office reviewed ASIO access to taxation information for the 2017-2018 period in August 2018. The results for this inspection will be included in next year's annual report.

ASIO EXCHANGE OF INFORMATION WITH FOREIGN LIAISONS

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 co-operate with foreign authorities approved by their Minister. ASIO has guidelines for the communication of information on Australians and foreign nationals to approved foreign authorities.

During the reporting period IGIS staff inspected a sample of foreign liaison exchanges through the regular inspections of ASIO cases. These inspections have focused primarily on areas of increased risk to Australian persons, such as persons involved in the Syrian conflict.

In a small number of cases, IGIS staff found that delays in responses from foreign liaison partners contributed to delays, some significant, in ASIO being able to finalise security assessments. IGIS staff noted that inconsistent practices in following up outstanding requests contributed to some of these delays.

MINISTERIAL SUBMISSIONS

IGIS staff regularly review a range of submissions to the Attorney-General. These reviews continue to be useful in obtaining an overview of legality and propriety issues and to keep the office informed of current operations and emerging issues. In 2018-2019 the office will review ASIO submissions to both the Attorney-General and the Minister for Home Affairs.

SECURITY ASSESSMENTS

Security assessments can lead to cancellation or refusal of visa or passports. In this reporting period IGIS staff continued to review a sample of cases where ASIO had requested passport suspension, passport cancellation or emergency visa cancellations.

SECTION 38(7) OF THE ASIO ACT

The ASIO Act requires that, where ASIO has issued a qualified or adverse security assessment of a person to a Commonwealth agency or to a State or authority of a State, that agency, state or authority shall notify the person of the assessment within 14 days. The ASIO Act provides for an exception to this requirement where ASIO's Minister certifies in writing that withholding the notice is essential to the security of the nation. Section 38(7) of the ASIO Act requires that if such certification is issued, ASIO's Minister must consider annually whether to revoke the certificate and notify the subject of the relevant assessment. While the ASIO Act does not impose a direct obligation on ASIO it is clear that in determining whether to issue the certificate and in reconsidering the matter every 12 months ASIO's Minister will need to rely on the Organisation's advice in order to meet this statutory obligation.

In October 2017, IGIS staff found that ASIO had not provided the Attorney-General with the information necessary to enable the Attorney-General to consider whether a certificate should be revoked. Seven months lapsed between IGIS staff raising this issue and ASIO advising the Attorney-General and the Minister for Home Affairs.

ASIO's repeated failure to provide the Minister with the information necessary to make a decision under section 38(7) of the ASIO Act is of significant concern. This office identified and reported on a number of such instances in the 2016-17 reporting period. As with last year, this office is concerned by the considerable time ASIO has taken to rectify this ongoing problem. It is disappointing that ASIO has shown no improvement in remedying breaches of this kind, despite instituting new procedures. At the conclusion of the current reporting period ASIO's processes and procedures remain deficient in this respect.

PROCEDURAL FAIRNESS

In one case, IGIS staff expressed concern that the subject of an ASIO adverse security assessment had not been afforded procedural fairness. ASIO officers held serious concerns regarding the threat this subject posed to security and sought to interview the person prior to issuing an adverse security assessment. In seeking to set up the interview ASIO officers advised the subject that they "wanted to discuss a minor issue." The person of interest terminated the call. Within the hour ASIO officers made two subsequent calls to the person that went unanswered. ASIO did not pursue alternative methods to inform the person of the consequences of not participating in the interview, as ASIO procedures required.

We raised concerns that ASIO did not comply with its own policy to ensure that the person of interest was informed and understood the consequences of not engaging with ASIO officers. ASIO determined that the actions of its officer had sufficiently afforded the subject of the assessment procedural fairness. This case was the subject of ongoing discussions with ASIO at the end of the reporting period.

DELAYS IN FINALISING SECURITY ASSESSMENTS

In addition to responding to complaints received by visa applicants, IGIS staff also review ASIO's security assessment investigations. In these inspections IGIS staff identified a number of security assessments affected by processing delays.

In one matter, a visa application was referred to ASIO in 2013 for assessment. By November 2014, ASIO had drafted the security assessment; however our inspection in November 2017, some three years later, found that the assessment had not yet been finalised. This case was highlighted to ASIO, noting concerns about the number of times the case had been reassigned to different case officers and the long periods of no activity. In response, ASIO advised the delay was due to numerous factors including ASIO's prioritisation, workloads and staffing issues. While the office accepts that ASIO has a very heavy workload and that, ultimately, it is for ASIO to manage that load, the extreme delay in this case was such that the Inspector-General has strongly recommended the case be finalised as a matter of urgency. At the end of the reporting period, the security assessment remained unresolved.

ASIO INSPECTION PROJECTS

ASIC/MSIC

During the reporting period the office finalised a review of ASIO's management of security assessments related to the Aviation Security Identification Card (ASIC) and the Maritime Security Identification Card (MSIC). The project examined complex cases, with a particular focus on the length of time taken to finalise the cases. It is acknowledged that not all aspects of investigating complex cases are within ASIO's control; resource limitations among others are significant factors. However, it was considered appropriate to examine this issue because of the implications for applicants' livelihoods.

ASIO prioritises advice and services for stakeholders by consulting them on their priorities and focusing on areas of greatest security risk. The project found that as a consequence of this approach lower risk complex cases, those least likely to result in an Adverse Security Assessment, experience the longest delays.

Despite these problems, overall, there was a significant improvement in the time taken to finalise security assessments for complex ASIC and MSIC security assessments between 2015 and 2017. The responsibility for ASIC and MSIC security assessments changed divisions in 2015 and the new division inherited ten cases that had suffered serious delays; all took more than 600 days to finalise the security assessments. The area in ASIO currently responsible for ASIC/MSIC security assessments cleared the backlog of cases and has significantly reduced the average processing time for complex cases.

DEVICES PROJECT

In November 2016 the IGIS initiated an inspection project focusing on ASIO staff access to surveillance devices and other technical devices used for surveillance. This project was suspended due to higher priority inspection activities and staffing shortages in this office.

ONLINE INVESTIGATIONS

In November 2016 the office initiated an inspection project focused on ASIO's online investigative activities. The project did not arise in response to a specific concern or complaint, but was considered to be timely noting the proliferation of social media activity amongst the investigative targets and broader public alike. During the reporting period, the project was cancelled to make way for higher priority investigations.

PROTECTING COMPLAINANT INFORMATION

In 2011 ASIO and the office agreed on a protocol for the management of information concerning complaints or public interest disclosures made to the Inspector-General. 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 reported on the identification by IGIS staff of breaches of this protocol and ASIO's subsequent comprehensive review. ASIO and the office have reviewed the protocol and proposed changes that will reduce the possibility of recurrence. The revised protocol was not yet finalised at the end of the reporting period.

AGENCIES SUBJECT TO THE *INTELLIGENCE SERVICES ACT 2001*

LIMITS TO THE FUNCTIONS OF INTELLIGENCE AGENCIES

The functions of agencies governed by the ISA are set out in sections 6, 6B and 7 of the ISA. For example, ASIS functions include to obtain and communicate, in accordance with the Government's requirements, intelligence about the capabilities, intentions or activities of people or organisations outside Australia. The work of ASIS, ASD and AGO is guided by the national intelligence priorities, which are reviewed and agreed by the National Security Committee of Cabinet each year.

The ISA also requires that ASIS, ASD and AGO only perform their functions in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being; and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia.

MINISTERIAL AUTHORISATIONS

All activities undertaken by ASIS, ASD or AGO to produce intelligence on an Australian person require individual consideration and approval by the responsible Minister, with the following exceptions:

- intelligence can be produced by ASIS on an Australian person without ministerial authorisation if doing so assists ASIO in the performance of its functions
- class authorisations can be given by the Minister where the intelligence is produced by ASIS in the course of providing assistance to the ADF
- subject to conditions, agency heads may give an authorisation in an emergency when Ministers are not available

Ministers are able to direct that other activities require prior ministerial approval, and each Minister has done so. In AGO's case, any intelligence collected over Australian territory requires authorisation by the head of the agency. Another example is that ministerial approval is required before ASD conduct certain cyber operations.

PRIVACY RULES

Section 15 of the ISA provides that the Ministers responsible for ASIS, ASD and AGO must make written rules to regulate the communication and retention of intelligence information concerning Australian persons (Privacy Rules). The term "Australian persons" includes citizens and certain permanent residents and companies. The rules regulate the agencies' communication of intelligence information concerning Australian persons to other Australian agencies and to foreign authorities, including to Australia's closest intelligence partners. Communication to foreign authorities is also subject to additional requirements. The Privacy Rules are unclassified and appear on the agencies' websites. No changes were made to the Privacy Rules in this reporting period.

Privacy Rules require that agencies may only retain or communicate information about an Australian person where it is necessary to do so for the proper performance of each agency's functions or where retention or communication is required under another Act.

If a breach of an agency's Privacy Rules is identified, the agency in question must advise the IGIS of the incident and the measures taken by the agency to protect the privacy of the Australian person, or 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 Inspector-General is required.

THE PRESUMPTION OF NATIONALITY

The Privacy Rules require that, unless there is evidence to the contrary, ASIS, ASD and AGO are to presume that a person in Australia is an Australian person and that a person who is not in Australia is not an Australian person. An initial presumption of nationality may be rebutted at a later date. For example:

- new information or evidence may indicate that a person overseas is an "Australian person". If it was not reasonable for this information to have been known and considered at the time the initial assessment was made then the presumption of nationality could be rebutted. There would have been no breach of the Privacy Rules in this circumstance.
- the agency may discover that it, or another agency, was already in possession of evidence that a person was an Australian person and which should have been considered in the initial assessment. In this case the presumption of nationality would be rebutted and if intelligence information had already been communicated about the Australian person there may have been a breach of the Privacy Rules. There may also be a breach of the ministerial authorisation rules if intelligence collection actually was undertaken.

If the agency made a reasonable assessment of the nationality status of that person, based on all the information that was available at the time, there is no breach of the Privacy Rules. Where a presumption of nationality is later rebutted, ASIS, ASD and AGO must advise the office of this and the measures taken to protect the privacy of the Australian concerned.

INSPECTION OF ASIS ACTIVITIES

IGIS oversight of ASIS's activities generally fall into eight categories, which are based on the underlying functions of the agency in accordance with section 6(1) of the ISA. These categories are:

- intelligence collection
- intelligence communication
- support to the ADF
- counter-intelligence
- foreign liaison
- co-operation and assistance to intelligence agencies and prescribed authorities
- actions undertaken in relation to ASIO
- other activities as the Minister responsible directs

During the reporting period, IGIS staff met the target of inspecting at least 75% of ASIS's activity categories. IGIS staff conducted a range of regular inspections of ASIS activities as part of the comprehensive inspection and visits program. These inspections included reviewing operational files, advice to the Foreign Minister, compliance incident reports, 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. IGIS staff also reviewed ASIS activities to ensure that they were consistent with human rights and did not constitute discrimination.

These inspections are supplemented by ASIS briefings on various matters throughout the year. Such briefings allow us to stay abreast of emerging issues and to follow up on observations from inspection activities.

REVIEW OF OPERATIONAL FILES

ASIS activities involve the use of human sources. 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.

IGIS staff visited ASIS several times each month during the reporting period to review ASIS's operational case files. These inspections considered a sample of files, focusing on high risk areas and ASIS's application of the Privacy Rules. While the sensitive nature of ASIS's operational activities means that specific detail of the nature and range of issues inspected cannot be provided in a public report, we can advise that these reviews are thorough and rigorous.

Overall, IGIS staff were satisfied with ASIS operational activities and that ASIS staff were appropriately identifying and considering risks associated with these activities. Inspections also allow IGIS staff to work with ASIS to identify and mitigate against unnecessary levels of risk. For example, in one inspection IGIS staff identified an area that had not sufficiently considered the Privacy Rules; the ASIS Compliance Branch addressed this issue and increased Privacy Rules training for this area. In another inspection, IGIS staff raised concerns regarding the level of oversight by senior ASIS staff of certain activities. The office has been working with ASIS to identify and appropriately manage this risk.

Where IGIS staff have identified areas requiring further investigation, ASIS has been forthcoming in providing additional information or briefing. In one case, it was judged that ASIS should have obtained a warrant to conduct an activity while in Australia. ASIS records showed that seeking a warrant was considered, but ultimately ASIS decided one was not necessary. This has led to constructive discussions to identify the risks and policy thresholds for warrants.

In another operational file review IGIS staff raised concerns about a delay in finalising internal guidance to ASIS staff on section 13B of the ISA, and identified a record keeping issue relating to a particular section 13B notice. Section 13B of the ISA allows ASIS to produce intelligence on an Australian person, or a class of Australian persons, to support ASIO in the performance of its functions, without first obtaining authorisation from the Minister for Foreign Affairs. In response to concerns raised, ASIS promptly finalised internal guidance on section 13B notices and reviewed all other section 13B notices to ensure that the problem was limited and not systemic.

MINISTERIAL SUBMISSIONS

IGIS staff reviewed all ministerial submissions produced by ASIS and found that the majority were of a high standard. In essence, an inspection of ministerial submissions seeks to ensure the responsible Minister is properly informed about sensitive ASIS operational issues. In most cases IGIS staff were satisfied that the information provided to the Minister was appropriate; however, IGIS staff did observe delays in providing some information to the Foreign Minister.

In one case, ASIS did not provide timely advice to the Minister for Foreign Affairs about unauthorised interception of communications by another agency, but related to a foreign intelligence collection warrant. Complicating the matter, ASIS staff wrote to the Foreign Minister about the foreign intelligence collection warrant but omitted any reference to the unauthorised interception. When the issue was identified by IGIS staff ASIS promptly rectified the omission through a separate submission to the Minister. The Inspector-General reminded ASIS of the importance of providing timely and accurate advice to Ministers as a matter of propriety, especially where there has been a breach of Australian law even by another agency.

In a second case, ASIS delayed fulfilling its reporting requirements under the ISA; section 13F of the ISA requires the Director-General of ASIS to provide a written annual report to the Foreign Minister in respect of activities undertaken by ASIS in accordance with section 13B. The report is to be provided “as soon as practicable after each year ending on 30 June”. The report for the period 2016-2017 was provided to the Minister for Foreign Affairs in January 2018. While not a breach of the ISA, the provision of the report to the Minister more than six months after the conclusion of the reporting period is not satisfactory. We will continue to monitor the timeliness of information provided to the Minister.

MINISTERIAL AUTHORISATIONS TO PRODUCE INTELLIGENCE ON AUSTRALIAN PERSONS

In the reporting period, IGIS staff reviewed all ASIS ministerial authorisations to produce intelligence on Australian persons. These inspections did not identify any issues of legality or propriety. However, inconsistencies were observed in the wording of authorising instruments, which resulted in variations to the commencement date and expiry dates of the authorisations. While no compliance issues were observed, the lack of consistency will inevitably increase the risk of error.

COMPLIANCE INCIDENT REPORTS

Since mid-2015 ASIS has provided the office with Compliance Incident Reports (CIRs) when ASIS identifies an issue or when an ASIS officer self-reports an issue relating to compliance or propriety. ASIS investigates the issue or incident and initiates remediation activities, including additional training for the staff and teams involved. This office reviews all ASIS CIRs and undertakes its own independent investigation of the incident where necessary. In this reporting period, ASIS provided 12 such reports, down from the 16 reports provided in the last reporting period. Of the 12 incidents, six related to Privacy Rules breaches, three involved weapons-related incidents and one related to ASIS’s handling of sensitive financial information. These incidents are addressed later in this report. The remaining two incidents involved activities not in accordance with section 8 of the ISA and are outlined below.

In August 2017 ASIS self-reported an incident to IGIS staff where ASIS had accessed an electronic device in Australia without informed consent from the owner of the device. Although ASIS had asked the individual if it could access the device, the purpose for

accessing the device was not communicated clearly enough for ASIS to be satisfied that the individual was sufficiently informed. Without informed consent, this activity was in breach of section 8 of the ISA and also section 25A of the ASIO Act. ASIS informed the individual and apologised for the incident, as recommended by the Inspector-General. The office considered that the actions of the ASIS officers did not give rise to a criminal offence and was satisfied with the measures ASIS put in place to prevent incidents of this nature from recurring.

In the second CIR, ASIS reported on two activities ASIS had undertaken in relation to an Australian person without having first obtained a ministerial authorisation. At the time of conducting the activities, the ASIS officer was unaware the individual was an Australian citizen and relied on the presumption of nationality; that is, a person outside Australia is to be presumed not to be an Australian person. Upon learning that the person was an Australian citizen, ASIS sought a ministerial authorisation to produce intelligence on the Australian person. The office views this as an appropriate course of action under the circumstances.

EMERGENCY MINISTERIAL AUTHORISATIONS

In the reporting period there were two instances where ASIS sought an oral authorisation from the Minister in an emergency using the section 9A provisions in the ISA. In both instances, 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 office did not identify any issues of concern relating to these authorisations.

PROTECTING THE PRIVACY OF AUSTRALIAN PERSONS

IGIS staff pay close attention to the distribution of intelligence about Australian persons during regular inspection activities. ASIS continued to provide training to its staff on producing intelligence on Australian persons and introduced initiatives to mitigate the risk of unintentionally reporting on Australian persons.

Throughout the reporting period there were a small number of instances where the Privacy Rules were not applied prior to ASIS reporting on an Australian person or company. While most were the result of human error, the effect of an ageing IT system and not identifying a person as an Australian citizen, the office found only one where reporting on an Australian person would not have been reasonable and proper had the Privacy Rules been applied at the time. In this case, the report was released in error and once the incident had been identified, ASIS immediately recalled the report and advised recipients of the incorrect details. IGIS staff reviewed this matter and the Inspector-General was satisfied that remediation was appropriate and measures to prevent recurrence were effective.

PRESUMPTION OF NATIONALITY

ASIS reported six occasions in the reporting period where the presumption of nationality was overturned; that is, information became known that an individual was actually an Australian person or that an individual was originally assumed to be Australian but later identified as non-Australian. In these instances there was no breach of the Privacy Rules, as the presumption of nationality was reasonable at the time it was made and the information indicating the individuals were Australian was not available at that time.

AUTHORISATIONS RELATING TO THE USE OF WEAPONS

Schedule 2 of the ISA requires:

- the Minister for Foreign Affairs to provide the Inspector-General with copies of all approvals issued by the Minister for Foreign Affairs in respect of the provision of weapons and the training in and use of weapons and self-defence techniques in ASIS, and also
- the Director-General of ASIS to give the Inspector-General a written report if a staff member or agent of ASIS discharges a weapon other than in training.

These requirements were met during the reporting period and the Inspector-General was satisfied that there was a need for limited numbers of ASIS staff to have access to weapons for self-defence in order to perform their duties. IGIS staff also examined ASIS weapon and self-defence policies, guidelines and training records in 2017–18. The reviews found that ASIS's approach to governance and record keeping on this matter continued to be satisfactory.

ASIS advised this office of three weapons-related incidents during the reporting period, two of which involved non-compliance with ASIS procedures and the third related to a firearms discharge. The first compliance issue arose when ASIS officers undertook firearms training (target practice) at a range that was not approved by ASIS. Australian security contractors who provide assurance to other Australian Government agencies had assessed this range and found it suitable for use; however, ASIS had not provided separate approval for its officers to use that training facility as required by ASIS policy. This was an administrative oversight rather than an operational incident or breach of legislation.

The second incident arose when ADF and ASIS personnel conducted joint weapons-related training prior to formal exchange of letters approving the training, as required by a memorandum of understanding between Defence and ASIS. As soon as the ASIS team responsible for the training became aware that the formal letters were not signed they immediately stopped the training exercise. The training recommenced once the letters of agreement were signed. The office considers that ASIS staff acted appropriately in suspending the training until formal arrangements were in place.

The third incident reported to this office concerned an accidental discharge of an ASIS-issued weapon by an ASIS officer during an approved training session. The weapon was fired in a safe direction and there were no injuries or damage to property resulting from the incident. ASIS took immediate steps to identify the cause of the accidental discharge and put in place measures to reduce the likelihood of another incident occurring. ASIS also notified Comcare of the incident.

INSPECTION OF ASD ACTIVITIES

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

- intelligence collection
- intelligence communication
- advice to Ministers or authorities in matters relating to security
- security assessments
- advice relating to protective security
- foreign intelligence collection
- assistance to intelligence agencies and prescribed authorities

In the reporting period IGIS staff met the target of inspecting at least 75% of ASD's activity categories.

The office's inspection of ASD activities is facilitated by strong working level relationships with ASD's compliance area and regular access to required systems. Given the volume and complex nature of ASD activities, the IGIS inspection program is continuous and includes scheduled activities, proactive reviews of areas of risk or sensitivity, as well as reviews of draft policies.

During the reporting period, the office inspected a number of ASD activities, including:

- ministerial authorisations to produce intelligence on Australian persons
- ASD's compliance with the Privacy Rules
- compliance incident reports
- ASD's access to sensitive financial information (discussed later in the report)

These inspections were supplemented by briefings on various matters across the year either at the request of this office or at the instigation of ASD. These briefings and subsequent investigations allowed the office to stay abreast of emerging issues and to pursue trends observed during inspections.

ASD had a higher number of breaches in this reporting period (12) compared to the previous reporting period (nine), however ASD's compliance area was more actively engaged with the office about breaches or potential breaches.

In this reporting period, the Defence inspection team increased in size. This allowed the team to continue its regular inspection activities and to commence an inquiry into an ASD matter requested by the Minister for Defence.

MINISTERIAL AUTHORISATIONS TO PRODUCE INTELLIGENCE ON AUSTRALIAN PERSONS

During the reporting period the office inspected around 80% of ASD's ministerial authorisations, a small increase on the 75% reviewed in the last reporting period. The submissions were generally of a high standard. However, IGIS staff did identify that, in 2017, numerous submissions seeking to renew a ministerial authorisation incorrectly stated the expiry date of the preceding authorisation. The office highlighted these errors to ASD because of the heightened potential to breach the ISA as a result of such inaccuracies. ASD's response to feedback on this issue was appropriate. IGIS staff will continue to monitor this aspect of ministerial submissions in future inspections.

A change of circumstances may prompt the Minister to cancel a ministerial authorisation, or it may expire at the end of the authorisation period. In either case, within three months ASD is required to provide the Minister with a report on its activities that relied on the authorisation. IGIS staff reviewed a number of these cancellation and non-renewal reports and did not identify any significant issues.

In December 2017 this office completed in-depth reviews of two ministerial authorisations provided under section 9(1A) of the ISA (acting for, or on behalf of, a foreign power). The selection of these cases was not prompted by any particular concern with these ministerial authorisations. IGIS staff reviewed the accuracy, balance and currency of the information provided to the Minister; end-product reporting; exchanges with other agencies; record keeping; and team-level procedures. The reviews did not identify issues of legality or propriety; indeed they revealed a culture of consistent record keeping within the relevant ASD team and showed that they actively considered compliance issues to manage risks.

EMERGENCY MINISTERIAL AUTHORISATIONS

Situations may arise where, as a matter of urgency, ASD requires a ministerial authorisation to undertake certain activities. Emergency authorisations may be provided orally by the Minister for Defence, other select Ministers where the Minister for Defence is unavailable, or the Director 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.

Nine emergency ministerial authorisations were issued to ASD during the reporting period. IGIS staff found no significant issues with these authorisations. In one case, an analyst accidentally conducted activity under an emergency ministerial authorisation that was not yet authorised, however this office acknowledged that this was not intentional and occurred in a high-pressure situation. IGIS staff also found that due to extraordinary circumstances, one emergency ministerial authorisation was signed slightly late. These cases are detailed as compliance incident reports later in this section.

MINISTERIAL SUBMISSIONS

During the reporting period IGIS staff also conducted a quarterly review of ministerial submissions that were not related to ministerial authorisations. The purpose of these reviews was to ensure the responsible Minister is provided timely and accurate information about critical ASD issues. These inspections began in mid-2017, and the results of the reviews were sent to ASD as part of the quarterly inspection letters. Over this reporting period, IGIS staff found that the majority of ASD ministerial submissions were of a high standard, and were provided to the Minister with sufficient time for approval. IGIS staff appreciated ASD actively consulting with the office in relation to a number of submissions reviewed.

PROTECTING THE PRIVACY OF AUSTRALIANS

The Minister for Defence makes written rules, the Rules to Protect the Privacy of Australians, to regulate how ASD communicates and retains intelligence information concerning Australian persons. ASD is required to report to this office any breaches of the Privacy Rules. In accordance with its obligations under the Privacy Rules, ASD reported cases during the reporting period where the presumption that an individual was not an Australian 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. Separately, ASD consulted with this office in relation to its efforts to expand information sharing with foreign partners, and the implications for protecting the privacy of Australian persons.

IGIS staff reviewed such cases reported by ASD and found that many of the 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.

However, the office review of several cases uncovered matters of concern. In August 2017 the office reviewed submissions from ASD relating to overturned presumptions of nationality. As part of this review, IGIS staff identified that ASD had breached section 63(1) of the TIA Act which restricts the communication of lawfully intercepted information. This breach occurred when ASD communicated lawfully intercepted information, but did not have authorisation to do so. The Inspector-General recommended ASD review the relevant arrangements to ensure they were consistent with the relevant authorisations. Later in the year, an IGIS review of another case encouraged ASD to consider informing foreign partners about overturned presumptions of nationality, as a further safeguard to protect privacy.

In September 2017 ASD advised this office of its investigation into a breach of the Privacy Rules. The breach occurred when ASD conducted activity on an individual, relying upon an incorrect presumption of foreign nationality. Given the information available at the time, this office considered that ASD should have presumed the individual was an Australian person and applied the Privacy Rules. ASD's investigation found that inconsistent work practices, human error and a high operational tempo resulted in the relevant area not taking into account all available information. IGIS staff reviewed ASD's findings and recommendations in regard to this incident and were satisfied the implementation of the recommendations would minimise the risk of future recurrence. In December 2017, ASD provided the office with a revised policy relating to this incident which helped to clarify specific processes across ASD.



COMPLIANCE INCIDENT REPORTS

Matters identified by ASD involving breaches of legislation and significant or systemic matters of noncompliance with ASD policy are investigated by ASD and reported to the IGIS in Compliance Incident Reports (CIRs). This office reviews these reports and undertakes an investigation of the incident where necessary. ASD provided 11 such reports during 2017-18 and one report on 30 June 2017. These incidents are outlined below.

On 30 June 2017 ASD advised this office of its investigation into a breach of section 8(1) of the ISA, in which ASD produced intelligence on an Australian person without a ministerial authorisation. A breach of section 10A of the ISA was also investigated as part of this case, as ASD failed to report to the Minister within one month of the date on which an emergency ministerial authorisation ceased to have effect. This office reviewed ASD's investigation and considered most of the findings to be reasonable, and agreed with the remedial actions proposed to prevent recurrence. Our office formed the view that ASD had an interest in the target prior to the date identified in the report and therefore should have obtained a ministerial authorisation sooner.

In the reporting period, ASD also advised this office of its investigation into four breaches of section 8(1) of the ISA, which involved ASD producing intelligence on an Australian person without a ministerial authorisation. In the first case, ASD assessed that the breach had occurred due to an incomplete process; IGIS staff reviewed the investigation and were satisfied with the conclusions and recommendations. In the second case, a breach occurred due to a failure of process following an update to an ASD user interface; IGIS staff reviewed ASD's investigation, identified that the required paperwork for the Minister was unsatisfactory and recommended that ASD re-submit the relevant documents. The circumstances of the third breach were that ASD had incorrectly overturned a presumption of nationality on the basis of citizenship status without proper regard to the residential status of an individual. The office was satisfied with ASD's subsequent investigation and remedial action proposed to prevent recurrence. In the final instance the breach occurred in the context of an emergency situation, lasted for a period of five minutes, and was identified and reported to this office within an appropriate time period.

In September 2017 ASD advised this office of its investigation into a breach of the Ministerial Directions that give effect to section 8(2) of the ISA. The breach occurred in the context of an emergency situation, was identified immediately by ASD, and reported to this office the day it occurred. This office was satisfied with ASD's investigation and remedial actions. In May 2018, this office also provided ASD with comments on an updated policy document related to this case, noting that this updated guidance will assist with preventing future related incidents.

In the 2017-18 reporting period, ASD informed this office of its investigation into four breaches of section 7 of the TIA Act. Two of these cases involved interception by unauthorised persons under section 12 of the TIA Act. These breaches highlighted an inconsistent approach to ASD's management of warrants, including a lack of communication within ASD teams, and a failure to adhere to, and formalise, team procedures. This office is currently conducting an inquiry into ASD that relates to these cases. In the third case, ASD conducted unauthorised interception of certain communications. ASD assessed the breach occurred due to a gap in process and application of compliance requirements. This office was satisfied with the investigation and proposed actions to prevent recurrence, including updating

procedures and related policies. The final such breach also involved the interception of certain communications, which ASD assessed occurred due to its failure to review collected intelligence in a timely manner. This office was satisfied with ASD's investigation and remedial actions.

In mid-2018, ASD informed this office of two further breach investigations. The first involved a breach of section 7 of the TIA Act, in which ASD intercepted certain communications data without the appropriate authorisation. The second concerned a breach of section 8 and section 15(5) of the ISA, which relates to the Privacy Rules, and involved ASD conducting activities against an Australian person without a ministerial authorisation. ASD completed its investigation into both incidents outside the reporting period. These incidents will be reported on in the next annual report.

POTENTIAL BREACHES OF THE TIA ACT

ASD considers that matters are classed as potential breaches when it is unclear, due to data limitations or the absence of essential details, whether a breach has occurred. The office reviews these matters in the same manner as its reviews compliance incidents.

In July 2017 ASD advised this office of its investigation into a potential breach of section 7 of the TIA Act. The incident involved possible collection of certain communications; however, ASD judged that it was not possible to determine whether certain communications had been collected. This office reviewed ASD's investigation and is satisfied with the final assessment and proposed measures for mitigating future risk associated with this matter.

In February 2018 ASD advised this office of its investigation into a potential breach of section 7 of the TIA Act. The incident involved the possible interception of certain communications over approximately one day; however, ASD was unable to determine if certain collection occurred because the system had automatically deleted the data after a period of time ASD's system. The cause of the incident was unable to be determined and it is likely it was a result of factors outside of ASD's control. The office was satisfied with the timeliness of ASD's investigation of the incident and reporting to this office.

In March 2018 ASD informed this office it was investigating two further potential breaches of section 7 of the TIA Act. The first was a result of a quality control process system misconfiguration, and this office was satisfied with ASD's investigation and remedial action. The second incident involved collection of potentially non-compliant data after a system upgrade. Following the update, collection of large amounts of data that was not collected during the testing phase occurred. ASD was unable to determine if there was domestic interception and if the data collected is considered a "communication" for the purposes of the TIA Act. This issue continues to be investigated by ASD and if necessary will be included in the next annual report.

In May 2018 ASD advised this office that it was investigating a further potential breach of section 7 of the TIA Act. This involved the possible collection of certain communications for a short period of time. ASD advised this office that it deleted the data in question, as it could not readily confirm whether it was compliant or not. ASD completed its investigation and reported the findings to this office in July 2018 and we were satisfied with ASD's investigation and actions.

INSPECTION OF AGO ACTIVITIES

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

- intelligence collection in support of the Government
- support to the ADF
- intelligence collection in support of Commonwealth and State authorities national security functions
- intelligence communication
- provision of imagery and other geospatial products
- assistance to intelligence agencies and prescribed authorities
- co-operation with, and assistance to, other intelligence agencies
- functions of the Australian Hydrographic Office

During the reporting period, this office achieved the target of inspecting 75% of AGO's inspection categories. These included:

- Ministerial authorisations to produce intelligence on Australian persons
- Director's approvals and post activity reporting
- AGO's compliance with the Privacy Rules
- AGO's access to sensitive financial information (discussed later in the report)

The office also received briefings from AGO teams for a better understanding of the agency's functions and to identify emerging issues. These briefings enabled the office to enhance working-level relationships within AGO and to follow up on matters observed during inspections.

Based on inspection and review activities, the office is satisfied that AGO met its statutory obligations under the ISA and that AGO has in place systems to encourage compliance.

MINISTERIAL AUTHORISATIONS TO PRODUCE INTELLIGENCE ON AUSTRALIAN PERSONS

AGO is required to seek authorisation from the Minister for Defence to produce intelligence on an Australian person. This authorisation is ordinarily requested in conjunction with ASD. During the reporting period, our inspections did not identify any concerns relating to AGO's ministerial authorisations, renewals, cancellations or non-renewals. Four emergency ministerial authorisations were issued to AGO during the reporting period; IGIS staff reviewed these emergency authorisations and did not identify any issues of concern.

DIRECTOR'S APPROVALS AND POST ACTIVITY REPORTING

The Minister for Defence requires the Director of AGO personally to approve AGO activities intended to obtain or communicate geospatial imagery intelligence of Australian territory. The Director of AGO is also required to provide the Minister with quarterly reports on approved intelligence activities. The accuracy of these and other reports provided to the Minister for Defence were reviewed during the reporting period. IGIS staff identified minor date errors in two of these quarterly reports, however these errors had no practical impact on the authorised activities.

At the conclusion of approved activities, AGO staff prepare a post-activity compliance report for the Director, which this office regularly examines. During the reporting period, IGIS staff identified no significant issues with AGO's post-activity compliance reports. However, IGIS staff noted one instance of non-compliance with a set of special conditions. Special conditions are regularly noted in Director's approvals as caveats for certain activities. In this instance, the special condition was not addressed in the post-activity compliance report, and the Director was incorrectly informed that all conditions had been met. This office provided guidance to AGO that all special conditions approved by the Director should be accurately referenced and addressed in the post-activity compliance reports, noting that this procedure would give the Director greater assurance that activities are conducted as directed. The office is satisfied that AGO has taken appropriate remedial action and steps in response to this matter.

AGO COMPLIANCE WITH PRIVACY RULES

The Minister for Defence makes written rules, namely Rules to Protect the Privacy of Australians, to regulate how AGO communicates and retains intelligence information concerning Australian persons. During the reporting period, IGIS staff did not identify any concerns in relation to issues AGO's compliance with the Privacy Rules. This is the second consecutive year that AGO has been fully compliant with the Privacy Rules.

AUSTRALIAN HYDROGRAPHIC OFFICE

In October 2017 legislative changes enabled the transfer of the Australian Hydrographic Office functions from Royal Australian Navy to AGO, which was based on the findings of the *2015 First Principles Review*. The office consequently now has oversight of the functions of the Australian Hydrographic Office in relation to any intelligence collection or application of the Privacy Rules. In May 2018, AGO advised the office that the Australian Hydrographic Office had fully incorporated ISA requirements into daily workflows and had received relevant compliance training. Due to current differences in task tracking and recording in separate systems, we have not yet reviewed any Hydrographic office products, but we intend to review and report on these in the next annual report.

INSPECTION OF DIO ACTIVITIES

DIO's role is set out in a mandate agreed by the Minister for Defence, rather than in legislation. As a result, activity categories for DIO have been established with reference to its mandate, organisational structure and product types. 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 over those of the assessment agencies DIO and ONA.

In this reporting period the office achieved the target of inspecting 75% of DIO's inspection categories. The office's inspection of DIO's activities included following up on matters identified during the inquiry into the analytic independence and integrity of DIO, 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 in the Cross Agency Inspection section of this report.

In addition to these inspection activities, we were briefed by DIO in relation to its co-operation with other agencies. This co-operation has been important in maximising the efficiency of its processes which are subject to review by this office.

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 respecting the privacy of Australians. IGIS staff did not identify any significant issues or concerns in this reporting period and there was no evidence that DIO breached the privacy guidelines.

INSPECTION OF ONA ACTIVITIES

The activity categories assigned to ONA are derived from the way in which ONA's statutory functions are structured under section 5 of the ONA Act, namely:

- assessment
- coordination
- evaluation

Due to staffing constraints, in this reporting period the office did not meet the target of inspecting at least 75% of ONA's activity categories. As ONA is an assessment agency the office considers that ONA's activities are consequently less likely to intrude upon the personal affairs of Australian persons than the activities of the intelligence collection agencies, which for that reason are given priority.

During 2017–18, IGIS staff conducted inspections examining ONA's compliance with its Privacy Guidelines and reviewed ONA's policies and handling of open source information as part of a cross agency project. The results of this inspection project are reported in the Cross Agency Inspections section of this report.

COMPLIANCE WITH PRIVACY GUIDELINES

At the end of the last reporting period, ONA updated its Privacy Guidelines. ONA reviewed and updated its existing privacy related guidance and developed a revised training package to be delivered to relevant staff.

During the reporting period, IGIS staff undertook two inspections of ONA's compliance with its Privacy Guidelines. The first of these inspections found no errors of consequence. The second identified a small number of instances where Privacy Guidelines were not applied appropriately by ONA before publication. ONA self-reported these incidents. We assessed that these errors did not result in the dissemination of intelligence information about an Australian person without an appropriate reason.

OTHER ACTIVITIES

This year IGIS staff increased their engagement with ONA's Open Source Centre (OSC), particularly focusing on its governance arrangements. The OSC systematically collects and researches publicly available information to support Australian Government intelligence priorities and the work of the National Intelligence Community. In accordance with ONA's mandate under the ONA Act, the OSC focuses on international developments that affect Australia's national interests. IGIS staff will continue to focus on this aspect of ONA's work during 2018–19.

CROSS AGENCY INSPECTIONS

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

OPEN SOURCE INFORMATION PROJECT

This project assessed the intelligence agencies' understanding of open source information, including the distinction between open source and private information, as well as whether their handling of open source information is appropriate and in accordance with respective statutory obligations. The project also provided guidance as to how the office should review activities in relation to the intelligence agencies' handling of open source information.

The project concluded that there is a common understanding of the meanings of open source and private information. All agencies distinguish between open source information (meaning unprotected publicly available information) and private information (where the originator of the information has taken steps to protect or add privacy restrictions) even though the information may be accessible via an open source medium, such as a social media platform.

There is no evidence to suggest that the intelligence agencies use open source material illegally or inappropriately. All agencies understand that collection of open source information must be legal and proportionate to the threat and that covert and intrusive collection requires different authorisation and procedures. Each agency has developed processes to identify and exploit open source information and carefully considers the issues of online security when conducting online research.

USE OF ASSUMED IDENTITIES

Part 1AC 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 a circumstance that would otherwise be considered unlawful. Similarly, the legislation protects the Commonwealth, State and Territory agencies who provide the evidence of an assumed identity in accordance with the Act.

The legislation also imposes reporting, administration and audit regimes on those agencies using assumed identities. Section 15LG of the *Crimes Act 1914* requires ASIO and ASIS to conduct six monthly audits of assumed identity records and section 15LE requires that each agency provide the Inspector-General with an annual report detailing the activities of their respective agencies during the year. The Director-General of Security and the Director-General of ASIS provided the Inspector-General with reports covering the activities of their respective agencies for the 2016-17 reporting period. There was nothing in the reports to suggest that the agencies were not complying with their legislative responsibilities, or which otherwise caused concern.

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 AUSTRAC. All intelligence agencies and the office are designated agencies for the purposes of the AML/CTF Act.

The office has a memorandum of understanding (MOU) with AUSTRAC which provides an agreed understanding of the office's role in monitoring access to, and use of, AUSTRAC information by agencies.

In overseeing an agency's use of AUSTRAC information, IGIS staff check that there is a demonstrated intelligence purpose applicable to that agency's functions; that access is appropriately limited; searches are focused; and information passed to Australian agencies and foreign intelligence counterparts is correctly authorised. Each year we prepare a statement summarising compliance monitoring in respect of the intelligence agencies access to, and use of, AUSTRAC information in the previous reporting period. As required under the MOU, during the reporting period, this statement was sent to the Attorney-General, the Minister for Foreign Affairs and the Minister for Defence. ONA advised us that, during the reporting period, it did not access or use any AUSTRAC related data.

Review of access to sensitive financial information by ASD, AGO and DIO during the reporting period did not reveal any issues of material concern. There were no instances of non-compliance by ASD, AGO and DIO regarding use and protection of and access to 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 the Defence intelligence agencies have effective procedures in place with regard to handling of this information.

Review of ASIS access to AUSTRAC information found that ASIS governance and recordkeeping on this matter continued to be effective. In addition, ASIS self-reported a case where ASIS staff passed AUSTRAC information to a liaison partner without seeking prior

approval from the Director-General. This was in breach of section 133A of the AML/CTF Act and ASIS procedures. In this case, the Inspector-General was satisfied that the disclosure by ASIS was for the purpose of the ASIS staff members' duties and therefore not a criminal offence under section 127(2) of the Act.

The office's review of ASIO's access to and use of AUSTRAC material identified extensive non-compliance with the requirements of ASIO's MOU with AUSTRAC and with ASIO internal policy, as well as a potential breach of the AML/CTF Act.

In particular, the MOU requires ASIO to maintain a log of all transmission of AUSTRAC information. IGIS staff found that this requirement was only complied with once during the review period. Further, IGIS staff identified a number of ASIO communications addressed to agency officials in circumstances where ASIO staff did not first ascertain whether the receiving officers were authorised to receive AUSTRAC information. ASIO advised that ASIO had passed AUSTRAC information to a foreign intelligence service without acquiring the requisite level of internal approval, in breach of the MOU.

In relation to the AML/CTF, IGIS staff identified that ASIO had disseminated a particular subset of AUSTRAC information – suspicious matter reporting – to a non-designated agency on a number of occasions. ASIO's view was that ASIO is able to share information with non-designated agencies reliant upon section 127(3)(a) of the AML/CTF Act. The Inspector-General views that, as a matter of propriety, if not legality, ASIO should not communicate suspicious matter reporting to non-designated agencies and that ASIO should communicate AUSTRAC information in accordance with the requirements of sections 128 and 133 of the AML/CTF Act.

In response to the issues raised by this office, ASIO conducted an internal review. As a result, ASIO made a number of recommendations, all of which were accepted by ASIO's Intelligence Committee. The office is satisfied that these measures will improve ASIO's handling of AUSTRAC material and mitigate against the risk of these errors recurring.

The office's inspection of ASIO's handling of AUSTRAC information also raised concerns in relation to compliance with the Attorney-General's Guidelines. The Guidelines require ASIO to take reasonable steps to ensure that personal information is not collected, used, handled or disclosed by ASIO unless it is reasonably necessary for the performance of its statutory functions. IGIS staff identified two instances in which a number of AUSTRAC records on file did not relate to the subject of ASIO inquiry. In both instances these records related to another person with the same name as the subject of inquiry, but who were not themselves the subject of ASIO's inquiries. The Inspector-General recommended that ASIO should consider how this sensitive information could be de-identified, quarantined and prevented from being incorporated into other ASIO databases and used, handled or disclosed at some later date. ASIO is yet to advise how this concern will be addressed.



ACTIVITY 3 RESPONDING TO 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 it is apparent on the face of the communication that the grievance is not credible or not intelligible.

A matter is categorised 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. They may also 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 many cases, complaints and other matters can be resolved quickly and efficiently by our staff speaking to the relevant agency or reviewing their records. Among other things, 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.

All persons contacting the office are given advice about actions taken in response to their concerns and the outcomes, to the extent possible within the security obligations of this office.

PERFORMANCE SUMMARY

Providing effective and timely response to complaints or referrals received from members of the public, Ministers or members of Parliament.

Performance criteria: Timeliness of complaint resolution.

Targets: 90% of complaints acknowledged within five business days and 85% of visa-related complaints resolved within two weeks.

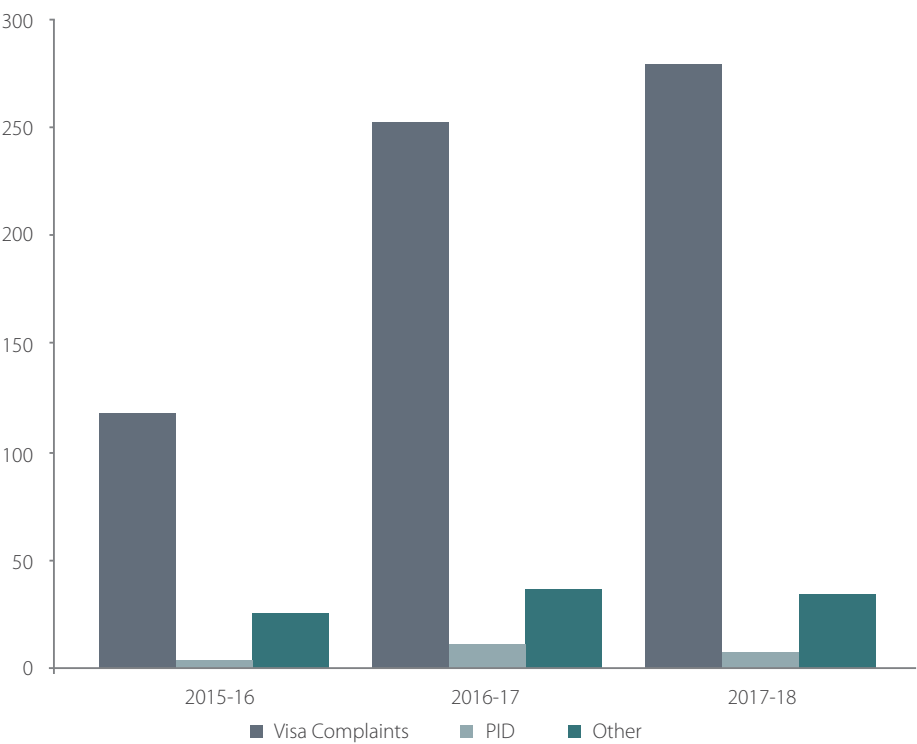
Source: Portfolio Budget Statements, p.257; IGIS Corporate Plan 2017-21, p. 5.

QUANTITATIVE PERFORMANCE MEASURES

Figure 2.5: 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	279	100%	82%
PID	7	100%	N/A
Other	34	92%	N/A
TOTAL	320	99%	82%

Figure 2.6: Complaint trends 2015-16 to 2017-18



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

In the reporting period, the office received 279 visa or citizenship-related complaints, an increase of 10% on the last reporting period. The average number of visa or citizenship-related complaints received per month was 23 in this reporting period, compared to an average of 21 complaints per month in 2016-17 and 10 complaints per month in 2015-16.

In previous years, the largest number of complaints made to the office has come from individuals seeking skilled business or work visas (21%). However, this was not the case for this reporting period. This year the largest number of complaints received related to citizenship applications (37% in 2017-18 compared to 5% in 2016-17). The reason behind the sharp increase in citizenship complaints will be explored in 2018-19.

In this reporting period, there has been a reduction in the complaints relating to family reunion visas (from 8% in 2016-17 to 5% in 2017-18) and protection and refugee visas (from 9% to 6%). The most frequent complaint about visa or citizenship applications was the length of time taken to finalise an application beyond that listed on the Department of Home Affairs website. Ordinarily the office will only take action on a complaint about a permanent visa, including citizenship, where 12 months have passed since the visa application was lodged with the Department of Home Affairs. In the case of temporary visa applications, the office will review a complaint where three months have passed since the temporary visa application was lodged.

During the reporting period, 100% 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 2017-18, 82% were resolved within 14 days of receipt, slightly lower than the office's target of 85%. During the reporting period there was an increased number of complex cases that took longer than 14 days to resolve. The office considers a complaint about a delay in visa or citizenship security assessments to be resolved once IGIS staff have completed our administrative inquiries and responded to the complainant.

UNDUE DELAY IN FINALISING VISA APPLICATIONS

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 for a complex case however, in a number of cases, this office found that ad hoc processes for following up requests for information contributed to delays in finalising assessments. This office has drawn these instances to ASIO's attention and emphasised that standard procedures or, at a minimum, guidance on following up information requests would reduce the risk of such delays.

OTHER COMPLAINTS

The office received 34 non-visa or citizenship-related complaints in this reporting period (excluding PID matters), a decrease of 6% on the previous reporting period. Unsurprisingly, since it has direct dealings with members of the public, the majority of the complaints (24) were about ASIO. Three complaints were about ASD; there were two each about ASIS, ONA and AGO and one for DIO.

The average time taken to acknowledge non-visa or citizenship-related complaints was two business days. IGIS staff responded to 92% of such complaints within five business days, which exceeded our performance target of 90%.

Of the 34 complaints received, 27 were finalised at the end of the reporting period, with an average of 30 days from the initial complaint to the date of the final response. In addition, two complaints were carried over from the previous reporting period.

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

- the way in which ASIO conducted interviews with members of the public
- the return of goods seized under warrant
- the release of information
- security assessments for employment
- surveillance

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

Five complainants received direct remedies:

- three complainants were granted their employment-related security clearances following periods of delay. It should be noted, however, that some delays were due to processing errors in agencies outside the AIC
- in two cases, ASIO returned seized items to the complainant following their complaint to this office

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, however, 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 our 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 suitable alternative avenues to pursue, if this is appropriate.

RETURN OF SEIZED PROPERTY

This complaint was about the time taken by ASIO to return property seized under an authorised warrant operation. The office noted ASIO had offered to return items separately once they had been examined and had also offered to provide the complainant with the temporary use of similar items until the property was returned. As the complainant had declined these offers, the Inspector-General considered ASIO's offer to return all items as soon as examination was completed was not unreasonable.

EMPLOYMENT-RELATED SECURITY CLEARANCES

Six complaints were made about the time taken by ASIO to finalise an assessment for an employment-related security clearance. The office considered ASIO's management of personnel security assessments for clearances and the steps in place to ensure all applications were receiving appropriate consideration. No issues of legality or propriety were identified. The Inspector-General recognises that lengthy waits can be frustrating and may affect employment opportunities, however ASIO prioritises cases based on advice from the Australian Government Security Vetting Agency (AGSVA), and the office is pleased with the initiatives ASIO has implemented to improve efficiency and finalise cases.

In another case, an unsuccessful applicant for employment with ASD alleged that their failure to pass the psychological assessment part of the security vetting process was the result of unauthorised interference with the result. The applicant also complained that the security vetting process was unethical as the extensive testing and the duration of the process did not result in employment. The office found that the complainant had participated in a voluntary process, the psychological assessment was conducted in accordance with routine procedures with appropriate accountability measures in place and there was no interference in the process.

OTHER CONTACTS

The office also received contacts from approximately 155 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 a decrease of 26% from the 210 individuals who made contact with the office in 2016-17 and reflects a steady decline since 2015-16's high of 325. While this decrease is encouraging, many of the individuals contacting the office do so on multiple occasions raising the same, or similar, issues. IGIS staff apply a consistent, fair approach to managing such matters.

When the office is contacted about matters we 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 other complaint-handling bodies, such as the 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.

REFERRALS FROM THE AUSTRALIAN HUMAN RIGHTS COMMISSION

The Australian Human Rights Commission (AHRC) is required by section 11(3) of the *Australian Human Rights Commission Act 1986* to refer to the Inspector-General human rights and discrimination matters relating to an act or practice of the intelligence and security agencies.

In this reporting period no cases were referred to the Inspector-General.



ACTIVITY 4 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.

PERFORMANCE SUMMARY

Facilitating the investigation of public interest disclosures relating to intelligence agencies and undertaking other responsibilities under the PID Act.

Performance criteria: timeliness of our response to public interest disclosures.

Target: 90% of public interest disclosures acknowledged within five business days.

Source: *IGIS Corporate Plan 2017-2021*, p. 6.

QUANTITATIVE PERFORMANCE MEASURES

Figure 2.7: Timeliness of response to public interest disclosures

TOTAL NUMBER OF PID	ACKNOWLEDGED WITHIN 5 BUSINESS DAYS	AVERAGE NUMBER OF BUSINESS DAYS FOR ACKNOWLEDGEMENT (TARGET: 90% ACKNOWLEDGED WITHIN 5 BUSINESS DAYS)
7	7	2

Figure 2.8: Public interest disclosures by agency and source

AGENCY	NUMBER OF PUBLIC INTEREST DISCLOSURES	FROM PUBLIC	FROM INTELLIGENCE AGENCY EMPLOYEE OR EX-EMPLOYEE
ASIO	4	0	4
ASIS	2	0	2
ASD	0	0	0
AGO	1	0	1
DIO	0	0	0
ONA	0	0	0

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
- overseeing the operation of the PID scheme in the intelligence agencies

There were seven public interest disclosures handled during the reporting period, four fewer than in the previous reporting period.

Most of the seven public interest disclosures raised allegations of maladministration covering a range of issues, including termination of employment, conduct relating to the withdrawal of security clearances and conduct relating to internal investigations into staffing matters.

PROCEDURAL FAIRNESS

An ASIO staff member alleged a lack of procedural fairness during a review of their suitability to retain a Positive Vetting security clearance. The individual said ASIO had provided written advice which indicated there would be an opportunity to respond to ASIO's preliminary views and that opportunity was not provided. Instead, ASIO's investigators had moved directly to the final outcome.

The office's investigation included a review of all relevant records and discussions with senior staff responsible for the process. While the investigation substantiated the claim that procedural fairness had not been afforded to the individual in that ASIO had not followed the procedure outlined in their written advice, IGIS staff were pleased to see that, as soon as ASIO was alerted to the PID, ASIO proposed to address the problem by offering the staff member additional opportunities to provide written and oral responses to the concerns raised. After the staff member provided additional information, ASIO initiated further investigation to inform their decision about the staff member's suitability to retain a PV clearance. We assess ASIO's remedial actions were appropriate.

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 inform the Inspector-General when a PID is allocated for investigation by an intelligence agency and must meet other reporting obligations.

The office was informed of two PIDs received by the intelligence agencies in the reporting period, one from ASIO and one from ASD.

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

ACTIVITY 5 ADVICE TO PARLIAMENTARY COMMITTEES AND OTHERS

ABOUT ADVICE TO PARLIAMENTARY COMMITTEES AND OTHERS

The IGIS is invited on a regular basis to participate in the proceedings of parliamentary committees and other similar bodies.

PERFORMANCE SUMMARY

Providing advice to parliamentary committees and others on oversight issues relating to intelligence agency powers and functions.

Performance criteria and indicators: timeliness of advice provided to parliamentary committees and similar bodies.

Target: written submissions provided by the date requested or agreed.

Source: *IGIS Corporate Plan 2017-21*, p. 6.

All advice was provided by the requested or agreed dates.

During the reporting period the IGIS contributed to six parliamentary committee inquiries.

DISCUSSION

SENATE ESTIMATES HEARINGS

The Inspector-General appeared before the Senate Standing Committee on Finance and Public Administration on 23 October 2017 for Supplementary Budget Estimates, on 27 February 2018 during the 2017-18 Additional Estimates hearings and on 21 May 2018 for the 2018-19 Budget Estimates.

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY (PJCIS)

The Inspector-General participated in five inquiries conducted by the PJCIS during the reporting period:

- *Review of ASIO's questioning and detention power*
- *Security of Critical Infrastructure Bill 2017*
- *Home Affairs and Integrity Agencies Legislation Amendment Bill 2017*
- *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017*
- *Review of Administration and Expenditure 2016-17*

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 potential impact on the performance by the Inspector-General of her functions. The Inspector-General's evidence was reflected in the findings and recommendations of the Committee, which were, in turn, implemented in parliamentary amendments to the relevant Bills.

The passage of the *Home Affairs and Integrity Agencies Legislation Amendment Act 2018* was particularly significant for the office, as was the PJCIS inquiry that preceded it. In the Bill as originally introduced, the Government had proposed that the Attorney-General should have the power to direct the Inspector-General to inquire into a matter. The Inspector-General appeared before the committee and submitted that in order to preserve the actual and perceived independence of the office the Prime Minister alone should have this power. The PJCIS agreed with the submissions and evidence of the Inspector-General about this matter. The Government accepted the PJCIS's recommendation that the Prime Minister alone should have this power.

In relation to the PJCIS inquiry into the *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* the Inspector-General gave evidence about the potential effect of the new secrecy offences on IGIS staff and on others who may want to provide the office with information. The Committee's report was tabled on 7 June 2018, and its recommendations for amendments, including to the secrecy provisions of the Bill, were implemented in Parliamentary amendments. The Bill was passed on 28 June 2018.

Broadly, the three other inquiries involved proposals to amend functions or powers in intelligence legislation. The Inspector-General typically provided comments on the oversight implications (including resource impact) of these proposals.

SENATE FOREIGN AFFAIRS, DEFENCE AND TRADE COMMITTEE

The Inspector-General participated in one inquiry conducted by the Senate Foreign Affairs, Defence and Trade Committee during the reporting period:

- *Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Bill 2018*

The Inspector-General made a submission to the inquiry into the establishment of ASD as a statutory agency to explain how the new measures and functions, including those relating to cybercrime, might be overseen. The submission noted that the existing inspections regime of ASD activity by the IGIS would continue largely unaffected by the changes. The Inspector-General added that from 1 July 2018 the office would gain jurisdiction for employment-related complaints by ASD staff. The new ASD function relating to cybercrime was viewed as consistent with the existing framework of the ISA and the office would oversee this new function including through review of ministerial authorisations.

ACTIVITY 6 EVIDENCE TO THE AAT AND THE AUSTRALIAN INFORMATION COMMISSIONER

ABOUT EVIDENCE TO THE AAT AND THE AUSTRALIAN INFORMATION COMMISSIONER

The *Freedom of Information Act 1982* (FOI Act) provides a number of exemptions to the requirement for government agencies to provide documents. One of the exemptions applies to documents affecting national security, defence or international relations. Before deciding that a document is not exempt under this provision, the Administrative Appeals Tribunal (AAT) and the Information Commissioner are required to seek evidence from the Inspector-General. There are equivalent provisions in the *Archives Act 1983* for the AAT. The Inspector-General is not required to give evidence if, in the Inspector-General's opinion, she is not appropriately qualified to do so.

PERFORMANCE SUMMARY

Providing evidence to the Administrative Appeals Tribunal and the Information Commissioner as required under relevant legislation.

Performance criteria: timeliness of evidence provided to the AAT and the Information Commissioner, when requested.

Target: evidence provided by the date requested or agreed.

Source: *IGIS Corporate Plan 2017-2021*, p. 6.

There were no quantitative performance measures identified in the *IGIS Corporate Plan 2017-21* that were directly applicable to the evidence we provided to the AAT and the Information Commissioner.

DISCUSSION

During the reporting period the Inspector-General provided written evidence on one aspect of one matter to the Information Commissioner, but did not provide oral evidence to the AAT.

The volume of cases referred to the Inspector-General by the Information Commissioner and the AAT is similar to previous reporting periods.

ACTIVITY 7 ENGAGEMENT WITH THE INTELLIGENCE AGENCIES AND THE PUBLIC

ABOUT ENGAGEMENT WITH THE INTELLIGENCE AGENCIES AND THE PUBLIC

Each year, the office engages with new and current members of intelligence agencies to increase their awareness of their compliance responsibilities as well as their understanding of the role of this office. In addition to discussions with agency heads and senior staff the Inspector-General and IGIS staff have given presentations to new and current staff explaining this office's approach to compliance issues and illustrating this with reference to some of the more common problems that we encounter.

This office also has a regular program of presentations to the broader intelligence community, and public groups with an interest in national security and intelligence matters. This program is designed to create greater public awareness of the role and activities of this office and "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"; section4(d), IGIS Act.

PERFORMANCE SUMMARY

Undertaking presentations to new and existing employees of intelligence agencies to ensure awareness and understanding of their responsibilities and accountability.

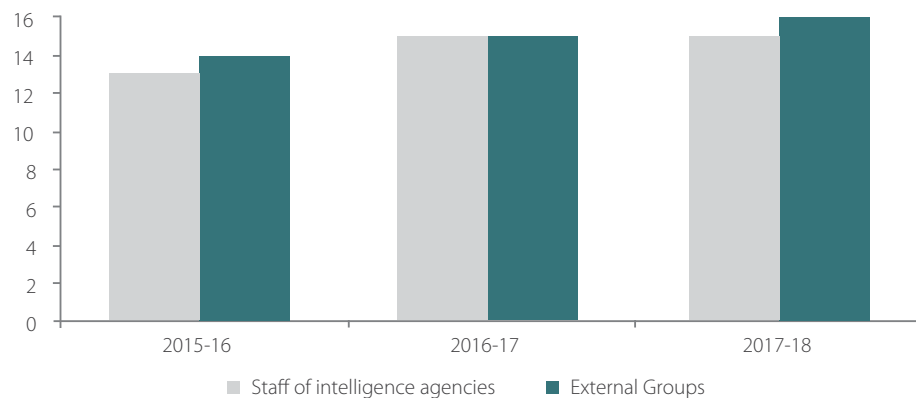
Raising awareness of the role and functions of the office outside the Australian intelligence agencies in order to increase public awareness of the scrutiny applied to the agencies.

Performance criteria: completion of at least 15 outreach activities per year.

Target: frequency of presentations to staff in intelligence agencies, frequency of outreach activities delivered to audiences outside the intelligence community.

Source: Portfolio Budget Statements, p.257; IGIS Corporate Plan 2017-2021, p. 6.

Figure 2.9: Number of presentations by year and audience



OUTREACH ACTIVITIES

In the reporting period the office exceeded the performance target for outreach activities delivering 31 presentations, 15 of which were to members of the intelligence agencies and 16 were provided to external groups to raise public awareness of the office. On average, the office delivered at least one presentation a month to members of the intelligence community as well as to audiences outside the intelligence community. Over the last three reporting periods the office has increased the number of presentations as part of a deliberate strategy to increase understanding of our role both within the agencies we oversee and the public.

PRESENTATIONS AND AGENCY ENGAGEMENT

Presentations delivered to staff in the intelligence agencies, and other related bodies, provide an opportunity to explain the role and functions of the office and to discuss matters relating to compliance, professionalism, accountability and ethical conduct.

The Inspector-General meets regularly with intelligence agency heads and their senior staff to discuss current issues or concerns and to highlight issues arising from inspection and inquiry activities. Typically agencies use these discussions to brief the office on emerging risks or potential concerns and how they plan to respond to these challenges. These discussions enhance our understanding of each intelligence agency's operational environment and also provide a forum to resolve issues informally. The Inspector-General continued the practice of meeting with ASIS heads of station and other officers from intelligence agencies to remind them of the functions of the office, to explore any particular challenges they encounter and to increase our understanding of their activities. These may vary depending on the particular locations and operations at their post.

Each agency has also established regular points of contact to facilitate our visits and to coordinate our various requirements, while within our office, designated officers lead interactions with each intelligence agency.

ENGAGEMENT WITH THE PUBLIC

In the reporting period there were 16 outreach activities delivered to audiences outside the Australian intelligence agencies. In October 2017, the Inspector-General presented to a meeting of the Integrity Agency Heads and to the Five-Eyes Intelligence Oversight and Review Council Conference in Canada (additional detail regarding this conference is provided later in this report). The Inspector-General was invited to address a number of leadership groups external to the intelligence agencies, including the Senior Executive Development Program at the National Security College in November 2017 and the National Public Sector Managers and Leaders Conference in March 2018. In May 2018 the Inspector-General delivered a keynote address at the 5th General Counsel Summit and to the Australian Government Solicitor Forum. The Inspector-General and Deputy Inspector-General also delivered guest lectures at universities and presentations to government departments during the reporting period.

A similar program of presentations will continue in the coming year.



ENGAGEMENT WITH NEW AGENCIES

The 2017 *Independent Intelligence Review* recommended that the jurisdiction of the office be expanded to include the intelligence functions of the ACIC, AFP, AUSTRAC and Department of Home Affairs. While the commencement of this expanded oversight is contingent on legislative change, during the reporting period the office commenced engagement with key contacts and senior leaders in those agencies to expand our understanding of their intelligence functions and to ensure the agencies understand our approach prior to commencement of legislative changes. Proactive engagement ahead of legislative changes to the jurisdiction of the office provides a strong foundation for our future oversight program.

ACTIVITY 8 LIAISING WITH OTHER ACCOUNTABILITY OR INTEGRITY AGENCIES

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.

PERFORMANCE SUMMARY

Liaising with other accountability or integrity agencies in Australia and overseas.

Performance criteria and indicators: frequency of interaction with other accountability and integrity agencies, including the OCO and the AHRC.

Target: regular interactions as required.

Source: *IGIS Corporate Plan 2017-2021*, p. 6.

DOMESTIC LIAISON WITH ACCOUNTABILITY AND INTEGRITY AGENCIES

Our engagement with other domestic accountability and integrity agencies during the reporting period focused on the practicalities of implementing the recommendation 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 Department of Home Affairs. In particular the office is working with other accountability and integrity agencies to ensure that our oversight activities are complementary and any overlap is minimised.

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 the reporting period the office liaised with the AHRC in relation to the potential impact of changes to the jurisdiction of the office, information sharing and complaint-handling practices.

COMMONWEALTH OMBUDSMAN

The work of the office complements the work of the Office of the Commonwealth Ombudsman (OCO) and there is a memorandum of understanding that provides guidance to handling complaints that overlap the jurisdiction of each office. During the reporting period, we continued to hold regular face-to-face meetings at the Deputy Inspector-General/Deputy Ombudsman level as well as staff level engagement and coordinated engagement between the office, OCO and Australian Commission for Law Enforcement and Integrity. The purpose of these meetings was to ensure the coordination of our current investigative activities and to consider coordination of future activities in view of the recommended changes to the jurisdiction of the office. During the reporting period the office and OCO agreed to temporary placement of some IGIS staff with the OCO, early in the 2018-19 reporting period, to enhance our understanding of their practices and procedures.

The most frequent area of overlap between our respective offices continues to be in the handling of immigration and visa-related security assessment complaints. Where appropriate, IGIS staff either refer matters directly to the OCO or where the matter does not come within the Inspector-General's jurisdiction, advise the visa applicant that they may lodge a complaint directly with the OCO. Cases where the matter does not come within the Inspector-General's jurisdiction, would include for example, those where the application was never referred to ASIO for security checks. Our staff also raise with the OCO any systemic issues that appear to relate to the Department of Home Affairs, for example, in cases where there has been prolonged delay by the Department of Home Affairs in processing certain visa applications.

The office also liaised closely with the OCO during the reporting period on the management of the Commonwealth's PID scheme. While the OCO has overarching responsibility for the operation of the PID scheme, the IGIS is responsible for overseeing the scheme for the intelligence and security agencies. Further information on the IGIS's responsibilities under the PID scheme can be found at Activity 4 of this report.

AUSTRALIAN COMMISSION FOR LAW ENFORCEMENT INTEGRITY

The Australian Commission for Law Enforcement Integrity (ACLEI) assists the Integrity Commissioner to provide independent assurance to Government about the integrity of prescribed law enforcement agencies. The changes to the jurisdiction of the Inspector-General recommended by the *2017 Independent Intelligence Review* will establish complementary oversight of the intelligence functions of some of the prescribed law enforcement agencies. Coordinated engagement between the office, OCO and ACLEI during this period focused on the coordination of future oversight activities including minimising duplication of effort and other issues of mutual interest. Additionally, the office reached an agreement with ACLEI regarding the placement of staff with ACLEI in the last quarter of the reporting period to enhance our understanding of their practices and procedures.

INTERNATIONAL ENGAGEMENT WITH ACCOUNTABILITY AND INTEGRITY AGENCIES

In October 2017 the Inspector-General and the Deputy Inspector-General attended the Five-Eyes Intelligence Oversight and Review Council Conference in Ottawa, Canada. The conference provided an opportunity to develop understanding of the ways in which different countries manage oversight of intelligence and security matters. During the reporting period, the Inspector-General additionally liaised with members of this Five-Eyes Council on key national developments and matters of mutual interest, including preparations for the October 2018 conference (which the Inspector-General will host). This activity will be reported in the 2018-2019 annual report.

In November 2017 the Inspector-General attended the International Intelligence Oversight Forum in Belgium. The theme of this conference was 'Democratic Oversight of Intelligence: Challenges and Choices'. The forum provided an opportunity to discuss global issues and engage with key leaders in intelligence and security oversight from outside of the five-eyes community.



SECTION THREE

MANAGEMENT AND ACCOUNTABILITY



PART 3.1

CORPORATE GOVERNANCE

ORGANISATIONAL STRUCTURE

Senior positions occupied during 2017–18 were as follows:

Inspector-General of Intelligence and Security (Statutory officer)

The Honorable Margaret Stone, appointed 24 August 2015

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

Mr Jake Blight

During the reporting period Mr Jake Blight had periods of acting as the Inspector-General.

Assistant Inspector-General of Intelligence and Security (SES Band 1)

Mr Stephen McFarlane

Mr Stephen McFarlane joined the Office of the IGIS on 8 February 2018.

SENIOR MANAGEMENT COMMITTEES

The Audit Committee is the only senior management committee for the agency.

The functions of this committee are detailed 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 IGIS and senior staff members, to review and document operational priorities
- monthly meetings between the IGIS and all office staff, during which internal guidelines, procedures and governance issues are discussed
- a forward plan for inspection activities in each intelligence agency, which is determined in consultation with the relevant agency head (in accordance with 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 2018, we were 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. At 30 June 2018 the members were Mr Trevor Kennedy (Attorney-General's Department) as Chair, Ms Sarah Vandenbroek (Department of Communications and the Arts) and Mr Jake Blight (IGIS) as members. 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
- 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
- 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

We maintained our commitment to ethical standards by ensuring staff were aware of the relevant requirements.

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.

EMPLOYMENT OF SES OFFICERS

The office has three SES positions: one SES Band 2 position and two SES Band 1 positions. The SES Band 2 position is filled by Mr Jake Blight on an acting arrangement, and one SES Band 1 position is substantively filled by Mr Stephen McFarlane. As a result of Mr Blight's acting arrangement one SES Band 1 position is currently vacant. The terms and conditions of all SES officer employment, including salary, are set out in a section 24(1) determination and are based broadly on SES remuneration within the Attorney-General's Department.

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. No person was employed under section 32(3) in the reporting period.

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

There were no reports on the operation of the office's (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

No judicial decisions or decisions made by administrative tribunals or the Information Commissioner had, or may have, a significant impact on the operations of the office.

PART 3.2

MANAGEMENT OF HUMAN RESOURCES

ORGANISATIONAL PROFILE

At 30 June 2018, the office had 23 ongoing APS employees located in the Australian Capital Territory (not including the Inspector-General). Five employees worked part-time.

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 2018 (employment level and status)

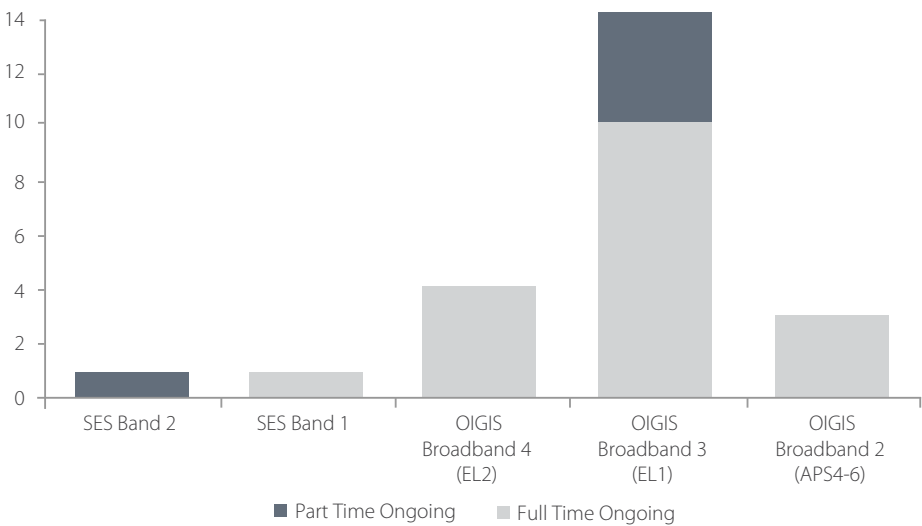
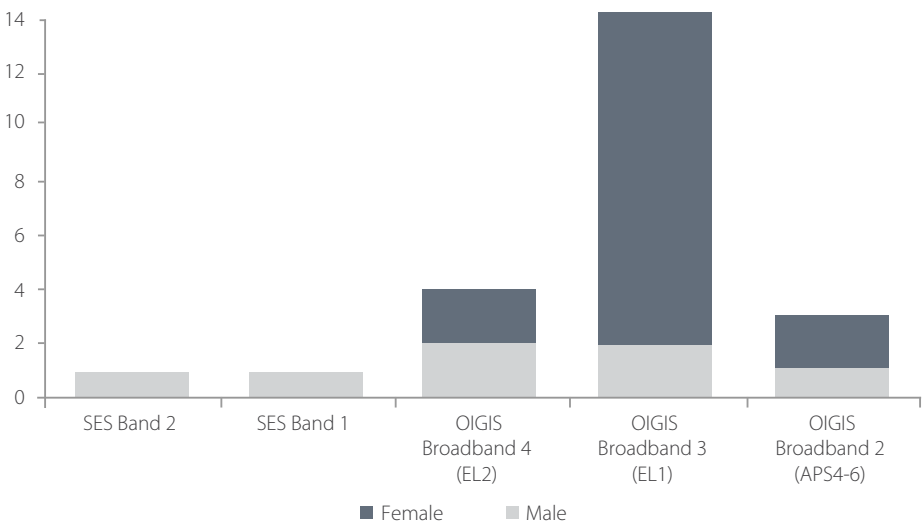


Figure 3.2: Gender Balance as at 30 June 2018 (by employment level)



EMPLOYMENT FRAMEWORKS

Since 6 February 2017, all non-SES staff were employed under *IGIS Enterprise Agreement 2016-2019*. Two SES staff members were employed under a section 24(1) determination.

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 Top Secret Positive Vet clearance, as well as other restrictions placed on employees as a result of reviewing the activities of the intelligence agencies. The annual allowance was \$1,125 until 7 February 2018 when the allowance increased to \$1,148 in line with *IGIS Enterprise Agreement 2016-2019* annual remuneration increases.

TRAINING AND STAFF DEVELOPMENT

The office continued the internal training program introduced in early 2012. The program of short training sessions run regularly ensures that staff develop and maintain specialised knowledge and skills, and supplements on the job training. Topics covered in the reporting period included:

- recent changes to legislation
- complaints handling
- ministerial authorisations
- security awareness

Staff were also provided with regular opportunities throughout the reporting period to attend other training courses and seminars relevant to their roles. A studies assistance scheme is available to reimburse employees for approved courses of study.

PERFORMANCE PAY

The office does not have a performance pay scheme.

PART 3.3

OTHER INFORMATION

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 2017-18, seven new consultancy contracts were entered into, involving total actual expenditure of \$44,720.18 (GST exclusive). In addition, three ongoing consultancy contracts were active during the period, involving total actual expenditure of \$8,257.48 (GST exclusive).

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

No contracts 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 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. As an exempt agency under the FOI Act, the scheme 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

The office received an unqualified audit report from the Australian National Audit Office for its 2017-18 financial statements. A summary of our financial performance follows.

The office operated within available resources in 2017-18 and ended the year with a surplus of \$3,664,131. The summary of financial performance is based on the original budget figures as published in the Portfolio Budget Statements 2017-18.

Appropriation funding levels in 2017-18 increased significantly with the office receiving additional departmental funding in the Portfolio Additional Estimates Statements (PAES) totalling \$3,662,000 to implement recommendations of the *2017 Independent Intelligence Review* which included an expansion of the office and a change in the office's jurisdiction. Other Income also increased following a reassessment of the value of resources received free of charge by the office. The increase in Other Income was matched by a corresponding increase 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 (\$60,554 overspent). This variance occurred due to an increase in staffing levels associated with the additional funding.

Net equity increased from \$3,161,158 in 2016-17 to \$18,406,446 in 2017-18. Movements in equity included a \$3,664,131 increase in retained surplus. Contributed Equity also increased from \$528,126 in 2016-17 to \$12,109,283 in 2017-18. Movements in Contributed Equity included capital funding of \$11,585,000.

The following tables show:

Figure 4.1 – Entity Resource Statement and Resources for Outcomes 2017-18

Figure 4.2 – Expenses and Resources for Outcome 1.

IGIS has one outcome and one program.

ENTITY RESOURCE STATEMENT AND RESOURCES FOR OUTCOMES 2017-18

Figure 4.1: Entity resource statement for 2017-18

		ACTUAL AVAILABLE APPROPRIATION FOR 2017-18 \$'000 (A)	PAYMENTS MADE 2017-18 \$'000 (B)	BALANCE REMAINING 2017-18 \$'000 (A) – (B)
Ordinary Annual Services				
Departmental Appropriation				
Prior year departmental appropriation		4,026	3,369	657
Departmental appropriation		18,404	-	18,404
S74 Relevant Agency Receipts		262	-	262
Total		22,692	3,369	19,323
Administered expenses				
Total		-	-	-
Total ordinary annual services	A	22,692	3,369	19,323
Other services				
Departmental non-operating		-	-	-
Total		-	-	-
Total other services	B	-	-	-
Total available annual appropriations				
		22,692	3,369	19,323
Special appropriations				
Total special appropriations	C	-	-	-
Special accounts				
Total special accounts	D	-	-	-
Total resourcing A + B + C + D		22,692	3,369	19,323
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		22,692	3,369	19,323

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 2017-18 \$'000	ACTUAL EXPENSES 2017-18 \$'000	VARIATION 2017-18 \$'000
	(A)	(B)	(A)-(B)

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

Departmental expenses

Departmental appropriation ¹	3,157	6,819	(3,662)
Special appropriations	-	-	-
Special Accounts	-	-	-
Expenses not requiring appropriation in the Budget year	166	(3,456)	3,622
Total for Program 1.1	3,323	3,363	(40)

**Outcome 1 Totals by
appropriation type**

Departmental expenses

Departmental appropriation ¹	3,157	6,819	(3,662)
Special appropriations	-	-	-
Special Accounts	-	-	-
Expenses not requiring appropriation in the Budget year	166	(3,456)	3,622
Total expenses for Outcome 1	3,323	3,363	(40)

	Budget 2017-18	Actual 2017-18	
Average Staffing Level (number)	17	16	1

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 2017-18 included:

- a \$3,701,000 increase in Revenue from Government
- a \$254,112 increase in Employee expenses arising largely due to recruitment activity associated with the additional funding and expansion of the office
- a \$108,447 increase in Supplier expenses. Increases in expenditure included \$7,479 in stationery expenses, \$36,766 in security vetting expenses, \$33,488 in consultant's fees and \$47,872 in notional rent charge
- an \$11,884 increase in Property, Plant and Equipment following the purchase of office equipment. This was offset by a \$25,254 increase in depreciation expenses. Revised useful lives were applied to assets expected to be disposed of when the office relocates in early 2019
- a \$317,242 decrease in Other Payables largely due to outstanding redundancy payments in the previous year and a decrease in reimbursements to home agencies for seconded staff
- a \$475,841 increase in Employee Provisions due to the increasing staff numbers associated with the additional funding and the changing profile of the staff

Figure 4.3: Trends in finance

		2017-18 OUTCOME 1 \$	2016-17 OUTCOME 1 \$	CHANGE FROM PREVIOUS YEAR
Revenue from Government		6,819,000	3,118,000	+119%
Other Income		208,854	157,705	+32%
TOTAL INCOME		7,027,854	3,275,705	
Employee expenses		2,844,554	2,590,442	+10%
Supplier expenses		474,353	365,906	+30%
Other expenses		44,816	20,067	+123%
TOTAL EXPENSES		3,363,723	2,976,415	
OPERATING RESULT		3,664,131	299,290	
Financial assets	A	19,476,805	4,030,721	+383%
Non-financial assets	B	56,468	89,400	-37%
Liabilities	C	1,126,827	958,963	+18%
NET ASSETS = A + B - C		18,406,446	3,161,158	



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 for the year ended 30 June 2018:

- (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 Office of the Inspector-General of Intelligence and Security as at 30 June 2018 and its financial performance and cash flows for the year then ended.

The financial statements of the Office of the Inspector-General of Intelligence and Security, which I have audited, comprise the following statements as at 30 June 2018 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; and
- Notes to and 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 Office of the Inspector-General of Intelligence and Security 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 Office of the Inspector-General of Intelligence and Security the Inspector-General of Intelligence and Security is responsible under the *Public Governance, Performance and Accountability Act 2013* for the preparation and fair presentation of annual financial statements that comply with Australian Accounting Standards – Reduced Disclosure Requirements and the rules made under that 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 and fair presentation 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 Office of the Inspector-General of Intelligence and Security's ability 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 those charged with governance 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

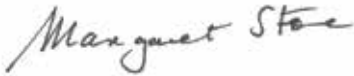
Delegate of the Auditor-General

Canberra
20 September 2018

STATEMENT BY THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2018 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

20 September 2018



OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY
STATEMENT OF COMPREHENSIVE INCOME
for the year ended 30 June 2018

	Notes	2018 \$	2017 \$	Original Budget \$
NET COST OF SERVICES				
Expenses				
Employee benefits	2A	2 844 554	2 590 442	2 784 000
Suppliers	2B	474 353	365 906	500 000
Depreciation	5	44 816	19 562	39 000
Write-down and impairment of asset		-	505	-
Total expenses		<u>3 363 723</u>	<u>2 976 415</u>	<u>3 323 000</u>
Own-Source Income				
Own-source revenue				
Other revenue	3A	208 854	157 705	-
Total own-source revenue		<u>208 854</u>	<u>157 705</u>	<u>-</u>
Gains				
Resources received free of charge		-	-	127 000
Total gains		<u>-</u>	<u>-</u>	<u>127 000</u>
Total own-source income		<u>208 854</u>	<u>157 705</u>	<u>127 000</u>
Net cost of services		<u>3 154 869</u>	<u>2 818 710</u>	<u>3 196 000</u>
Revenue from Government		<u>6 819 000</u>	<u>3 118 000</u>	<u>3 157 000</u>
Surplus /(deficit) on continuing operations		<u>3 664 131</u>	<u>299 290</u>	<u>(39 000)</u>
OTHER COMPREHENSIVE INCOME				
Items not subject to subsequent reclassification to net cost of services				
Changes in asset revaluation surplus		-	5 518	-
Total comprehensive income/(loss)		<u>3 664 131</u>	<u>304 808</u>	<u>(39 000)</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 2018

	Notes	2018 \$	2017 \$	Original Budget \$
ASSETS				
Financial Assets				
Cash and cash equivalents		199 788	200 498	165 000
Trade and other receivables	4	19 277 017	3 830 223	3 289 000
Total financial assets		<u>19 476 805</u>	<u>4 030 721</u>	<u>3 454 000</u>
Non-Financial Assets				
Property, plant and equipment	5	56 468	89 400	126 000
Total non-financial assets		<u>56 468</u>	<u>89 400</u>	<u>126 000</u>
Total Assets		<u>19 533 273</u>	<u>4 120 121</u>	<u>3 580 000</u>
LIABILITIES				
Payables				
Suppliers	6A	22 463	13 198	21 000
Other payables	6B	53 461	370 703	111 000
Total payables		<u>75 924</u>	<u>383 901</u>	<u>132 000</u>
Provisions				
Employee provisions	7	1 050 903	575 062	627 000
Total provisions		<u>1 050 903</u>	<u>575 062</u>	<u>627 000</u>
Total Liabilities		<u>1 126 827</u>	<u>958 963</u>	<u>759 000</u>
Net Assets		<u>18 406 446</u>	<u>3 161 158</u>	<u>2 821 000</u>
EQUITY				
Contributed equity		12 109 283	528 126	553 000
Reserves		21 623	21 623	16 000
Retained surplus		6 275 540	2 611 409	2 252 000
Total Equity		<u>18 406 446</u>	<u>3 161 158</u>	<u>2 821 000</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 2018

	2018 \$	2017 \$	Original Budget \$
CONTRIBUTED EQUITY			
Opening balance as at 1 July	528 126	503 126	528 000
Transactions with Owners			
Contributions by Owners			
Return of Equity	(1 000)		
Departmental Capital Budget	11 582 157	25 000	25 000
Total Transactions with Owners	11 581 157	25 000	25 000
Closing balance as at 30 June	12 109 283	528 126	553 000
RETAINED EARNINGS			
Opening balance as at 1 July			
Balance carried forward from previous period	2 611 409	2 312 119	2 291 000
Comprehensive Income			
Surplus/deficit for the period	3 664 131	299 290	(39 000)
Total comprehensive income	3 664 131	299 290	(39 000)
Closing balance as at 30 June	6 275 540	2 611 409	2 252 000
ASSET REVALUATION RESERVE			
Opening balance as at 1 July			
Balance carried forward from previous period	21 623	16 105	16 000
Comprehensive Income			
Other Comprehensive Income	-	5 518	-
Total comprehensive income	-	5 518	-
Closing balance as at 30 June	21 623	21 623	16 000
TOTAL EQUITY			
Opening balance			
Balance carried forward from previous period	3 161 158	2 831 350	2 835 000
Comprehensive Income			
Surplus/deficit for the period	3 664 131	299 290	(39 000)
Other comprehensive income	-	5 518	-
Total comprehensive income	3 664 131	304 808	(39 000)
Transactions with Owners			
Contributions by Owners			
Return of Equity	(1 000)		
Departmental Capital Budget	11 582 157	25 000	25 000
Total Transactions with Owners	11 581 157	25 000	25 000
Closing balance as at 30 June	18 406 446	3 161 158	2 821 000

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 2018

	Notes	2018 \$	2017 \$	Original Budget \$
OPERATING ACTIVITIES				
Cash received				
Appropriations		3 353 815	2,743 480	3 104 000
Net GST received		14 139	7 600	-
Other cash received		261 646	113 705	-
Total cash received		<u>3 629 600</u>	<u>2 864 785</u>	<u>3 104 000</u>
Cash used				
Employees		(3 042 837)	(2 412 936)	(2 784 000)
Suppliers		(326 042)	(291 283)	(295 000)
Section 74 receipts transferred to OPA		(261 431)	(113 705)	-
Total cash used		<u>(3 630 310)</u>	<u>(2 817 924)</u>	<u>(3 079 000)</u>
Net cash from/(used by) operating activities		<u>(710)</u>	<u>46 861</u>	<u>25 000</u>
INVESTING ACTIVITIES				
Cash used				
Purchase of property, plant and equipment		(11 884)	(26 242)	(50 000)
Total cash used		<u>(11 884)</u>	<u>(26 242)</u>	<u>(50 000)</u>
Net cash from/(used by) investing activities		<u>(11 884)</u>	<u>(26 242)</u>	<u>(50 000)</u>
FINANCING ACTIVITIES				
Cash received				
Contributed equity		11 884	25 000	25 000
Total cash received		<u>11 884</u>	<u>25 000</u>	<u>25 000</u>
Net cash from financing activities		<u>11 884</u>	<u>25 000</u>	<u>25 000</u>
Net increase/(decrease) in cash held		<u>(710)</u>	<u>45 619</u>	<u>-</u>
Cash and cash equivalents at the beginning of the reporting period		200 498	154 879	155 000
Cash and cash equivalents at the end of the reporting period		<u>199 788</u>	<u>200 498</u>	<u>155 000</u>

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

Major Budget Variances for 2018

The following table provides high level commentary of major variances between budgeted information for the OIGIS published in the 2017-18 Portfolio Budget Statements (PBS) and the 2017-18 final outcome as presented in accordance with Australian Accounting Standards for the OIGIS. Adjustments to the original PBS budget during the year included additional funding as published in the 2017-18 Portfolio Additional Estimates Statements (PAES) which included \$3,662,000 departmental funding for the expansion of the office and its jurisdiction. The additional funding also included \$11,560,000 departmental capital budget funding, which is expected to be expended in 2018-19 when the office relocates, resulting in the variance in contributed equity compared to the original budget.

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)
Revenue from Government - \$3,662,000 above budget. The variance relates to additional funding received during Additional Estimates for an expansion of the office and a change in the office's jurisdiction.	Impacted: Statement of Comprehensive Income: Revenue from Government Statement of Financial Position: Appropriations receivable Retained surplus
Other Revenue – approximately \$208,000 above budget which was offset by Gains – Resources Received Free of Charge which was \$127,000 below budget following a reclassification. The increase related largely to a change in the assessed value of resources received free of charge from the Department of the Prime Minister and Cabinet for office space. The matching expense also increased which has no overall impact on the retained surplus.	Impacted: Statement of Comprehensive Income: Other Revenue Supplier expenses
Employee Benefits – \$60,554 above budget. The variance reflects recruitment action associated with the additional funding received at Additional Estimates. Other Payables – approximately \$57,539 below budget. The variance reflects a decrease in salary reimbursements associated with secondees.	Impacted: Statement of Comprehensive Income: Employee expenses Statement of Financial Position: Appropriations receivable Employee provisions Other payables Retained surplus Cashflow Statement: Cash used - operating activities
Suppliers – \$25,647 below budget. The most significant variances related to delayed implementation of Portfolio wide shared service arrangements and expenses associated with the relocation of the office including lease and guard services. Other variances include underspends in expenses driven by the number and scope of inquiry work, including legal and travel expenses.	Impacted: Statement of Comprehensive Income: Supplier expenses Statement of Financial Position: Appropriation receivable Suppliers payables Retained surplus Cashflow Statement: Cash used - operating activities
Property, Plant and Equipment – capital expenditure was approximately \$13,000 below budget due to changes in the scheduled replacement of existing assets	Impacted: Statement of Comprehensive Income: Depreciation

associated with the planned relocation of the office. The variance was also due to the application of accelerated depreciation to assets expected to be disposed of prior to their estimated useful life when the office relocates.		Statement of Financial Position: Property, plant and equipment Appropriations receivable Cashflow Statement: Cash used - investing activities
Employee Provisions - \$423,903 above budget. The variance relates to leave liabilities associated with new staff recruited following receipt of the additional funding for the expansion of the office and its jurisdiction.	Impacted:	Statement of Comprehensive Income: Employee Benefits Statement of Financial Position: Appropriation receivable Other Receivables Employee Provisions Retained surplus Cashflow Statement: Cash used - operating activities



NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2018

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.

Revised estimated useful lives were applied to assets expected to be disposed of during the planned relocation of OIGIS in early 2019.

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 2018

Note 2 – Expenses

	2018	2017
	\$	\$
<u>Note 2A – Employee Benefits</u>		
Wages and salaries	2 123 953	1 897 944
Superannuation:		
Defined benefit plans	162 303	119 336
Defined contribution plans	202 013	210 021
Leave and other entitlements	356 285	195 960
Separations and redundancies	-	167 181
Total employee benefits	2 844 554	2 590 442

Accounting Policy

Accounting policies for employee related expenses are contained in Note 7.

	2018	2017
	\$	\$
<u>Note 2B – Suppliers</u>		
Goods and services supplied or rendered		
Consultants	52 936	19 448
ICT support	46 000	46 000
Legal expenses	-	5 702
Printing non publications	-	8 022
Printing publications	13 614	-
Resources received free of charge:		
Notional Rent Charge	175 872	128 000
Notional Audit Fees	21 000	21 000
Notional IT Support Costs	4 545	4 545
Stationery	16 637	9 158
Training	16 150	18 899
Travel	4 559	14 222
Overseas Travel	35 381	44 981
Security Vetting Expenses	43 146	6 380
Other	24 115	17 523
Total goods and services supplied or rendered	453 955	343 880
Other suppliers		
Motor Vehicle Lease – minimum lease payments	15 994	15 863
Workers compensation premiums	4 404	6 163
Total other supplier	20 398	22 026
Total supplier	474 353	365 906

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2018

Leasing Commitments

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

	2018 \$	2017 \$
Within 1 year	6 903	11 134
Between 1 to 5 years	19 181	1 856
Total operating lease commitments	26 084	12 990

Note 3 – Own-Source Revenue

	2018 \$	2017 \$
<u>Note 3A – Other Revenue</u>		
Employee FBT Contributions	5 262	3 880
Other	2 175	280
Resources Received Free of Charge:		
Department of the Prime Minister & Cabinet	175 872	128 000
Australian National Audit Office	21 000	21 000
Australian Signals Directorate	4 545	4 545
Total other own-source revenue	208 854	157 705

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 2017-18 are the provision of office space (from the Department of the Prime Minister and Cabinet) and the installation and maintenance of the OIGIS owned internal secure computer network (from Australian Signals Directorate).

Note 4 – Financial Assets

	2018 \$	2017 \$
<u>Trade and other receivables</u>		
Appropriations receivable	19 123 295	3 827 406
GST receivable from the Australian Taxation Office	1 803	2 817
Other receivables	151 919	-
Total trade and other receivables (net)	19 277 017	3 830 223

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 2018

Accounting Policy

Receivables for goods and services, which have 30 day terms, are recognised at the nominal amounts due less any impairment allowance account. Collectability of debts is reviewed as at end of reporting period. Allowances are made when collectability of the debt is no longer probable. All financial assets have been assessed for impairment at 30 June 2018. No indicators or impairment have been identified.

Note 5 – Non-Financial Assets

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

Item	Property, plant & equipment \$
As at 1 July 2017	
Gross book value	89 400
Accumulated depreciation and impairment	-
Total as at 1 July 2017	89 400
Additions	
by purchase	11 884
Depreciation expense	(44 816)
Total as at 30 June 2018	56 468
Total as at 30 June 2018 represented by:	
Gross book value	101 284
Accumulated depreciation and impairment	(44 816)
Total as at 30 June 2018	56 468

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 2018 included \$48,718.47 Level 2 assets (including office equipment and furniture) and \$7,750 Level 3 assets (including computer equipment and office furniture).

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

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2018

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 2018. 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 1 – 11 years (2017: 1 – 11 years).

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 – Payables

	2018	2017
	\$	\$
<u>6A - Suppliers</u>		
Trade creditors and accruals	22 463	13 198
Total suppliers	<u>22 463</u>	<u>13 198</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).

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2018

	2018 \$	2017 \$
6B - Other Payables		
Salaries and wages	23 567	16 681
Superannuation	3 492	2 211
Salary reimbursements for seconded officers	26 030	47 564
Redundancy payment	-	301 740
Other	372	2 507
Total other payables	53 461	370 703

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 7 – Employee Provisions

	2018 \$	2017 \$
Employee Provisions		
Leave	1 050 903	575 062
Total employee provisions	1 050 903	575 062

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.

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.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2018

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 8 – 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 Executive. Key management personnel remuneration is reported in the table below:

	2018 \$	2017 \$
Short-term employee benefits:		
Salary	677 030	615 485
Allowances	35 844	41 752
Total short-term employee benefits	712 874	657 237
Post-employment benefits:		
Superannuation	90 563	106 719
Total post-employment benefits	90 563	106 719
Other long-term employee benefits:		
Annual Leave	61 879	47 792
Long Service Leave	13 343	6 582
Total other long-term employee benefits	75 222	54 374
Total senior executive remuneration expenses	878 659	818 330

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 3 individuals (2017: 3 individuals). The 2018 figure includes one of the officers for part of the year whilst the 2017 figure included two officers for part of the year.

Note 9 – 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.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2018

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.

The following transactions with related parties occurred during the financial year:

- The Department of Prime Minister and Cabinet provided OIGIS with access to the Department's unclassified IT system. OIGIS made a \$46,000 contribution towards the operating costs of the system. There is no balance outstanding at year end.
- OIGIS received resources received free of charge from the Department of Prime Minister and Cabinet relating to office lease expenses. The estimated value of \$175,872 is reflected in the Statement of Comprehensive Income as both 'other revenue' and a 'suppliers' expense.

Note 10 - 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 2018 (2017: Nil).

Note 11 – Financial Instruments

	2018 \$	2017 \$
<u>Categories of Financial Instruments</u>		
Financial Assets		
Loans and Receivables		
Loans and receivables		
Cash and cash equivalents	199 788	200 498
Trade and other receivables	151 919	-
Total financial assets	<u>351 707</u>	<u>200 498</u>
Financial Liabilities		
At amortised cost		
Suppliers	22 463	13 198
Total financial liabilities	<u>22 463</u>	<u>13 198</u>

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

Financial Assets

OIGIS classifies its financial assets as 'loans and receivables'. Financial assets are recognised and derecognised upon trade date.

Financial assets are assessed for impairment at the end of each reporting period.

Credit terms are net 30 days (2017: 30 days).

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2018

Financial Liabilities

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

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

Settlement is usually made net 30 days.

Note 12 – Appropriations

Note 12A – Annual Appropriations ('Recoverable GST exclusive')

	2018 \$	2017 \$
Ordinary Annual Services		
Annual Appropriation	6 819 000	3 118 000
PGPA Act – Section 74 Receipts	261 431	113 705
Annual Departmental Capital Budget ¹	11 585 000	25 000
Total appropriation	18 665 431	3 256 705
Appropriation applied (current and prior years)	3 353 815	2 743 480
Variance²	15 311 616	513 225

- 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 recruitment delays associated with security clearance requirements prior to the receipt of the additional funding. The most significant factor was the receipt of additional funding part way through the year and the time involved in recruiting additional staff and expanding the agency's activities.

Note 12B: Unspent Annual Appropriations ('Recoverable GST exclusive')

	2018 \$	2017 \$
Departmental		
Appropriation Act (No 1) 2013-14 - DCB	-	2 843
Appropriation Act (No 1) 2015-16	-	541 858
Appropriation Act (No 1) 2015-16 – DCB	13 116	25 000
Appropriation Act (No 1) 2016-17	-	1 913 825
Supply Act 1 2016-17	419 747	1 317 879
Appropriation Act (No 1) 2016-17 – DCB	14 000	14 000
Supply Act 1 2016-17 – DCB	11 000	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	3 662 000	
Appropriation Act (No 3) 2017-18 – DCB	11 560 000	
Cash	199 788	200 498
Total Departmental	19 323 082	4 026 903



SECTION 4 FINANCIAL MANAGEMENT

SECTION FIVE

ANNEXURES



ANNEXURE 5.1

IGIS SALARY SCALE

OIGIS BAND	APS LEVEL	SALARY RANGE 1 JULY 2017 – 30 JUNE 2018 (\$)
OIGIS Band 4	EL2	118,260 – 140,746
OIGIS Band 3	EL1	101,604 – 113,265
OIGIS Band 2	APS 6	84,114 – 94,526
	APS 5	73,705 – 79,952
	APS 4	66,210 – 72,039
OIGIS Band 1	APS 3	59,548 – 64,127
	APS 2	52,050 – 57,880
	APS 1	47,422 – 50,802

ANNEXURE 5.2

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 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 Department of the Prime Minister and Cabinet (PM&C), continues to benefit from that Department's commitment to energy saving measures. This includes the large number of energy and water saving measures, designed to reduce greenhouse emissions, which are incorporated into the building in which we are among the occupants (One National Circuit). These measures include, but are not limited to, energy efficient lighting, heating and cooling.

Due to the small size of the office, PM&C does not separately measure the utilities used by the office and provides these utilities free of charge. For this reason, ecologically sustainable development and details of environmental performance are not specifically 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 PM&C, 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 2017-18
- printers are configured to print double-sided by default
- all unclassified office paper and cardboard waste is recycled
- empty toner cartridges are recycled

ANNEXURE 5.3

REQUIREMENTS FOR ANNUAL REPORTS

PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
17AD(g)	Letter of transmittal			
17AI	Prelim	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 specified additional requirements in relation to the annual report.	Mandatory	i
17AD(h)	Aids to access			
17AJ(a)	Prelim	Table of contents.	Mandatory	ii
17AJ(b)	Annex	Alphabetical index.	Mandatory	109
17AJ(c)	Prelim	Glossary of abbreviations and acronyms.	Mandatory	v
17AJ(d)	Annexure	List of requirements.	Mandatory	101
17AJ(e)	Prelim	Details of contact officer.	Mandatory	inside front cover
17AJ(f)	Prelim	Entity's website address.	Mandatory	inside front cover
17AJ(g)	Prelim	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
17AD(b)	Overview of the entity			
17AE(1)(a)(i)	Section 1	A description of the role and functions of the entity.	Mandatory	3
17AE(1)(a)(ii)	Section 1	A description of the organisational structure of the entity.	Mandatory	4
17AE(1)(a)(iii)	Section 1	A description of the outcomes and programs administered by the entity.	Mandatory	6



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	6
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	72
17AF(1)(b)	Section 4	A table summarising the total resources and total payments of the entity.	Mandatory	73
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	75

PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
17AD(d)	Management and Accountability			
<i>Corporate Governance</i>				
17AG(2)(a)	Section 3	Information on compliance with section 10 (fraud systems).	Mandatory	65
17AG(2)(b)(i)	Prelim	A certification by accountable authority that fraud risk assessments and fraud control plans have been prepared.	Mandatory	i
17AG(2)(b)(ii)	Prelim	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)	Prelim	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	64
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	66
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	66



PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
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	N/A
17AG(3)(c)	N/A	Information on any capability reviews on the entity that were released during the period.	If applicable, Mandatory	N/A
<i>Management of Human Resources</i>				
17AG(4)(a)	Section 3	An assessment of the entity's effectiveness in managing and developing employees to achieve entity objectives	Mandatory	68
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 • statistics on employees who identify as Indigenous. 	Mandatory	67
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	68
17AG(4)(c)(i)	Section 3	Information on the number of SES and non-SES employees covered by agreements etc identified in paragraph 17AD(4)(c).	Mandatory	66
17AG(4)(c)(ii)	Annexure	The salary ranges available for APS employees by classification level.	Mandatory	98
17AG(4)(c)(iii)	Section 3	A description of non-salary benefits provided to employees.	Mandatory	68

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)		An assessment of effectiveness of assets management where asset management is a significant part of the entity's activities.	If applicable, Mandatory	N/A
<i>Purchasing</i>				
17AG(6)	Section 3	An assessment of entity performance against the <i>Commonwealth Procurement Rules</i> .	Mandatory	69
<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	69



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	69
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	69
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	69
<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)	N/A	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	N/A
<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	69
17AG(10)(b)	Section 3	An outline of the ways in which the procurement practices of the entity support small and medium enterprises.	Mandatory	69
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	

PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
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)	Annexure	If the entity did not conduct advertising campaigns, a statement to that effect.	If applicable, Mandatory	99
17AH(1)(b)	N/A	A statement that <i>“Information on grants awarded to [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	69
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	70
17AH(1)(e)	N/A	Correction of material errors in previous annual report.	If applicable, Mandatory	N/A
17AH(2)	Annexure	Information required by other legislation.	Mandatory	99

INDEX

A

- abbreviations, v
- accountable authority statement, 10
- Activity performance statements *see* performance
- address and contact details, *inside front cover*
- Administrative Appeals Tribunal, evidence to, 55
- administrative tribunal decisions (external scrutiny), 66
- advertising and market research, 99
- agency capability reviews, 66
- AGO *see* Australian Geospatial-Intelligence Organisation (AGO)
- analytic independence (DIO), 13, 40
- analytic tradecraft, 13, 17
- ANAO *see* Australian National Audit Office
- annual performance statement *see* performance
- annual report availability, *inside front cover*
- Anti-Money Laundering and Counter Terrorism Financing Act 2006*, 42–3
- Archives Act 1983*, 7, 55
- ASD *see* Australian Signals Directorate (ASD)
- ASIO *see* Australian Security Intelligence Organisation (ASIO)
- ASIS *see* Australian Secret Intelligence Service (ASIS)
- Assistant Inspector-General of Intelligence and Security, 4, 64
- assumed identities, 42
- Attorney-General, 3, 7, 21, 54
 - ASIO reporting obligations, 19–20, 22, 24–5
 - Guidelines under ASIO Act, 7, 22–3, 43
 - submissions to, 24
- Audit Committee, 64, 65
- Auditor-General *see* Australian National Audit Office
- audits, internal, 65
- AusTender, 69
- AUSTRAC *see* Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Australian Commission for Law Enforcement Integrity, 3, 60
- Australian Criminal Intelligence Commission, 3, 23, 58, 59

- Australian Federal Police, 3, 23, 58, 59
- Australian Geospatial-Intelligence Organisation (AGO)
 - AUSTRAC information access and use, 42
 - complaints, 47
 - compliance oversight, 2, 38
 - inspections of, 16, 38–9
 - ministerial authorisations, 27, 38
 - presumption of nationality, 28
 - privacy rules compliance, 27–8, 39
 - role and functions, 8, 15
- Australian Government Security Vetting Agency, 3, 110
- Australian Human Rights Commission, 3, 49, 59
- Australian Hydrographic Office, 39
- Australian Information Commissioner, 3, 7, 10, 55, 66
- Australian Intelligence Community *see* intelligence agencies
- Australian National Audit Office, 4, 66, 69, 72
- Australian persons
 - definition, 2, 27
 - identifying subjects as, 22–3
 - intelligence collection on, 22–3, 27–8, 29, 30, 31, 34, 35, 36, 37, 38
 - presumption of nationality, 28, 31, 35
 - see also* privacy rules
- Australian Secret Intelligence Service (ASIS)
 - assumed identities, 42
 - AUSTRAC information access and use, 42–3
 - complaints, 47
 - compliance incident reports, 30–1
 - inspections of, 16, 28–32
 - ministerial authorisations, 27, 30, 31
 - presumptions of nationality, 28, 31
 - privacy rules compliance, 27–8, 29, 30–1
 - regulation of activities, 2, 7, 28
 - review of operational files, 29
 - role and functions, 7, 15
 - weapons use and issues, 30, 32

Australian Security Intelligence Organisation (ASIO)

- analytic tradecraft, 17
- assumed identities, 42
- Attorney-General's Guidelines, 7, 22-3, 43
- AUSTRAC information access and use, 43
- complaints handling, 26, 46-8
- foreign liaisons information exchange, 24, 43
- human source management, 18
- information exchange with Australian Government agencies, 23-4
- inquiries relating to, 12, 14
- inspections of, 2, 16-26
- investigative activities, 17, 22
- Minister, 7
- ministerial submissions, 24
- multi-agency foreign intelligence collection operation, 14
- online investigative activities, 26
- personal information, provision and retention, 22-3, 43
- procedural fairness, 25, 52
- protection of complainant information, 26
- questioning and detention warrants, 21
- role and functions, 7, 15, 16
- security assessments, 17, 24-6, 46, 48
- special intelligence operations, 7, 21-2
- surveillance devices, 26
- taxation information access, 23-4
- use of force, 21
- warrants, 7, 18-21, 48

Australian Security Intelligence Organisation Act 1979, 7, 15

- Attorney-General's Guidelines, 7, 22-3, 43
- breaches of, 19-20, 24-5
- security assessment requirements, 24-5

Australian Signals Directorate (ASD)

- AUSTRAC information access and use, 42
- complaints, 47
- compliance incident reports, 33, 36-7
- compliance oversight, 2, 33
- inquiries relating to, 12, 13-14, 36

- inspections of, 16, 33–7
- ministerial authorisations, 27, 33, 34
- ministerial submissions, 34, 35
- presumptions of nationality, 28, 35
- privacy rules compliance, 27–8, 33, 35, 37
- role and functions, 8, 15
- statutory agency status, 8, 54
- warrants management, 36

Australian Transaction Reports and Analysis Centre (AUSTRAC), 3, 42–3, 58, 59

Australians *see* Australian persons

Aviation Security Identification Card, 26

B

Blight, Jake, 4, 64, 65, 66

C

citizenship-related complaints, 45, 46

coercive powers, 11

Commonwealth Disability Strategy, 69

Commonwealth Electoral Act 1918 reporting requirements, 99

Commonwealth Indigenous Procurement Policy, 69

Commonwealth Procurement Rules, 69

Commonwealth Risk Management Policy, 65

community engagement, 2, 56–7

complaints handling, 44–9

- ASIO breach of protocols, 26

- ‘contacts’ versus ‘complaints’, 44, 49

- employment-related, 48

- IGIS function and powers, 2, 4

- non-visa related, 47–8

- timeliness, 45, 46

- visa-related, 2, 45, 46

- see also* inquiries

compliance incident reports, 30–1, 36–7

conferences, 2–3, 57, 61

consultants, 69
contact details, *inside front cover*
contracts, 69
corporate and operational planning, 6, 64–6
corporate governance, 64–6
Crimes Act 1914, 42
cross agency inspections, 41–3 *see also* inspections
cybercrime, 54

D

Defence intelligence agencies, 8
Defence Intelligence Organisation (DIO)
 analytic independence and integrity, 13, 40
 AUSTRAC information access and use, 42
 complaints, 47
 inquiries relating to, 12, 13
 inspections of, 16, 40
 mandate, 15, 40
 privacy guidelines compliance, 40
 role and functions, 8, 15
Department of Defence, 23 *see also* Minister for Defence
Department of Foreign Affairs and Trade, 23
Department of Home Affairs, 3, 23, 46, 58, 59, 60
Department of the Prime Minister and Cabinet, 100
Deputy Inspector-General of Intelligence and Security, 3, 4, 57, 60, 61, 64
detention warrants *see* questioning and detention warrants
disability reporting, 69–70



E

ecologically sustainable development, 100

emergency authorisations, 31, 34, 36, 38

employment frameworks, 66, 68

enterprise agreements, 68

entity resource statement and resources for outcome, 73–4

environmental performance, 100

ethical standards, 65–6

exchange of information

- between Australian agencies, 23–4, 27
- with foreign liaisons, 24, 27, 43

exempt contracts, 69

expert evidence, 7

external scrutiny, 66

F

financial intelligence *see* sensitive financial information

financial performance summary, 72–5

financial statements, 66, 76–96

firearms *see* weapons use and issues

Five-Eyes Intelligence Oversight and Review Council, 2–3, 57, 61

force, use of, 21

foreign liaisons

- IGIS, 61
- intelligence agencies, 24, 27, 43

fraud control, i, 65–6

Freedom of information Act 1982, 7

- exempt documents, 55
- IGIS as exempt agency, 70

functions *see* roles and functions

G

general public, IGIS engagement with, 56–7
geospatial intelligence agency *see* Australian Geospatial-Intelligence Organisation (AGO)
government agencies, liaison with, 59–61
Guidelines to Protect the Privacy of Australian Persons, 40

H

Harradine Order (Senate Continuing Order for Indexed File Lists), 70
Home Affairs and Integrity Agencies Legislation Amendment Act 2018, 54
human resources management, 67–8 *see also* staff
human rights and discrimination matters, 49, 59
human source operations, 18, 29

I

imagery intelligence *see* Australian Geospatial-Intelligence Organisation (AGO)
Independent Intelligence Review 2017, 3, 58, 59
Indigenous businesses, 69
Information Publication Scheme, 70
information security authority *see* Australian Signals Directorate (ASD)
inquiries
 acceptance of recommendations by agencies, 11
 employment of persons for a particular inquiry, 66
 IGIS function and powers, 4, 11
 performance discussion, 11–14
 statistics, 2, 12, 13
 timeliness, 13
inquiries by parliamentary committees *see* parliamentary committees
inspections, 2, 4, 15
 AGO activities, 16, 38–9
 ASD activities, 16, 33–7
 ASIO activities, 2, 16–26
 ASIS activities, 16, 28–32
 AUSTRAC access and use, 42–3
 cross-agency inspections, 41–3
 DIO activities, 16, 40

- IGIS function and powers, 4
- ONA activities, 16, 40–1
- performance summary, 15–16
- Inspector-General of Intelligence and Security
 - jurisdiction, 2–4, 58, 59
 - powers, 4, 11
 - presentations, 2, 4, 5, 56–7
 - purpose, 6
 - review of year, 2–3
 - role, 3–5
 - statutory officer, 3, 64
- Inspector-General of Intelligence and Security Act 1986*, i, iv, 4, 11
 - objects of the Act, 6
 - section 35 requirements, 10
 - subsection 32(3) employment, 66
- intelligence agencies
 - AUSTRAC information access and use, 42–3
 - complaints, 2, 44–9
 - compliance oversight, 2
 - cross-agency inspections, 41–3 *see also* inspections
 - IGIS engagement with, 56–8
 - IGIS jurisdiction, 2–4, 58, 59
 - limits on functions, 27
 - ministerial authorisations, 27
 - privacy considerations *see* privacy rules
 - public interest disclosure scheme, 2, 26, 50–2, 60
 - recruitment complaints, 48
 - see also names of agencies*
- Intelligence Services Act 2001*, 2, 7, 15
 - limits on intelligence agencies' functions, 27
 - privacy considerations *see* privacy rules
- Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Act 2018*, 8, 54
- international engagement, 2–3, 57, 61
- International Intelligence Oversight Forum, Belgium, 61
- Internet home page, *inside front cover*

J

judicial decisions, 66
jurisdiction, 2–4, 58, 59

L

legislative framework, iv, 6–7
letter of transmittal, i
liaising with other accountability or integrity agencies, 59–61

M

Maritime Security Identification Card, 26
market research, 99
McFarlane, Stephen, 4, 64, 66
media liaison, *inside front cover*
memoranda of understanding
 ASIO/ATO, 23
 ASIO/AUSTRAC, 43
 ASIS/Defence, 32
 IGIS/AUSTRAC, 42
 IGIS/Ombudsman, 60
Minister for Defence, 8, 15, 33, 34, 35, 38–40
 Rules to Protect the Privacy of Australians *see* privacy rules
Minister for Foreign Affairs, 7, 30, 32
Minister for Home Affairs, 7, 24, 25
ministerial and other authorisations to collect intelligence, 27, 30, 31, 38
ministerial submissions
 ASD, 34, 35
 ASIO, 24
 ASIS, 30

N

National Disability Strategy, 70

National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017, 54

nationality, presumption of, 28, 31, 35

non-salary benefits, 68

O

Office of National Assessments Act 1977, 7, 15, 40, 41

Office of National Assessments (ONA)

AUSTRAC information access and use, 42

complaints, 47

inspections of, 16, 40–1

Open Source Centre, 41

privacy guidelines compliance, 40–1

role and functions, 7, 15, 40

Office of the Australian Information Commissioner, 3, 66

Office of the Commonwealth Ombudsman, 3, 52, 60, 66

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

ONA *see* Office of National Assessments (ONA)

online investigative activities, 26

Open Source Centre, 41

open source information, 40, 41

operational files (ASIS), review of, 29

operational planning (IGIS), 64–6

organisational profile, 67

organisational structure, 4, 64

outcome and program, 6 *see also* performance

outreach program *see* presentations and outreach

P

parliamentary and media liaison, *inside front cover*

parliamentary committees

IGIS submissions and appearances, 2, 4, 5, 53–4

scrutiny of IGIS, 66

Parliamentary Joint Committee on Intelligence and Security, 2, 4, 53–4

performance

accountable authority statement, 10

financial performance summary, 72–5

performance summaries, 11, 15–16, 44–5, 50–1, 53, 55, 56, 59

quantitative performance measures, 12, 15, 45, 50, 55

results at a glance, 10

results discussion:

Activity 1, Inquiries, 11–14

Activity 2, Inspections, 15–43

Activity 3, Responding to complaints, 44–9

Activity 4, Public Interest Disclosures, 50–2

Activity 5, Advice to parliamentary committees and others, 53–4

Activity 6, Evidence to the AAT and the Australian Information Commissioner, 55

Activity 7, Engagement with the intelligence agencies and the public, 56–8

Activity 8, Liaising with other accountability or integrity agencies, 59–61

performance pay, 68

personal information

ASIO collection and retention, 22–3, 43

exchange between agencies, 23–4, 27

privacy, 27–8

see also Australian persons; privacy rules

personal security, 64–5

plans and planning, 6, 64–6

police services *see* Australian Federal Police; state and territory police services

Portfolio Budget Statements, 6, 15 *see also* performance

portfolio relationship, 3

premises, 3

presentations and outreach, 2, 4, 5, 56–8

presumption of nationality, 28, 31, 35

Prime Minister, 7, 54

privacy rules, 2, 7, 8, 27–8, 35, 39

compliance, 2, 27–8, 29, 30–2, 33, 35, 37, 39, 40–1

procedural fairness, 25, 52

procurement, 69

protective security, 64–5

Public Governance, Performance and Accountability Act 2013, i, iv, 10, 65, 99

Public Interest Disclosure Act 2013, 6, 50

public interest disclosure matters, 2, 26, 50–2, 60

Public Service Act 1999, section 24(1) determinations, 66

purchasing, 69

purpose, 6–7

Q

questioning and detention warrants, 21

R

record keeping, 13, 21, 29

recruitment (IGIS), 3

remuneration, 66, 68, 98

resources for outcome, 3, 72–4

return of seized property, 48

risk management, 65–6

roles and functions

IGIS, 3–5

intelligence agencies, 7–8

Rules to Protect the Privacy of Australians see privacy rules

S

salary scales, 98

section 24(1) determinations, 66

security (IGIS), 64–5

security assessments by ASIO, 24–6

complaints, 45, 46, 48

security clearances (IGIS staff), 3, 68

seized property, 48

Senate Continuing Order for Indexed File Lists (Harradine Order), 70

Senate Estimates committees, 2, 53

Senate Foreign Affairs, Defence and Trade Committee, 54

Senior Executive Service (SES) officers, 66

senior management committees, 64

sensitive financial information, 23–4, 30, 42

signals intelligence *see* Australian Signals Directorate (ASD)

small business participation in procurement, 69

social media, 26

special intelligence operations, 7, 21–2

staff

- employment arrangements, 66, 68
- gender balance, 67
- non-salary benefits, 68
- numbers and profile, 3, 4, 67
- salary scale, 98
- training and development, 68

state and territory police services, 23

Stone, Hon Margaret, 3, 64 *see also* Inspector-General of Intelligence and Security

studies assistance scheme, 68

submissions by IGIS to inquiries and reviews, 2, 4, 5, 53–4

submissions to Ministers *see* ministerial submissions

surveillance devices, 26

T

Taxation Administration Act 1953 (TAA), 23–4

taxation information, 23–4

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

- ASD compliance, 14, 35, 36–7
- ASIO compliance, 18–21
- breaches of, 14, 18–20, 35, 36–7
- potential breaches of, 37

telecommunications interception, 18–19, 35

- data retention, 23

timeliness



complaints handling, 45, 46
inquiries, 12
training and development (IGIS staff), 68

U

use of force, 21

V

values (approach to role), 5
visa process complaints, 2, 25, 45, 46
visa security assessment processes, 24–5

W

warrants (ASIO), 7, 18–21
weapons use and issues (ASIS), 30, 32
website address, *inside front cover*
whistleblower protection scheme *see* public interest disclosure matters
work health and safety (IGIS staff), 99

