



IGIS

INSPECTOR-GENERAL OF
INTELLIGENCE AND SECURITY

2016–2017

ANNUAL REPORT



30 YEARS

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/annual_report/index.cfm

ISSN: 1030-4657

© Commonwealth of Australia 2017



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 Malcolm Turnbull MP
Prime Minister
Parliament House
CANBERRA ACT 2600

Dear Prime Minister

I am pleased to present my annual report for the period 1 July 2016 to 30 June 2017.

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 deal appropriately with fraud relating to the agency.

Yours sincerely

Margaret Stone

Inspector-General

22 September 2017



CONTENTS

IGIS contact information	inside cover
Letter of transmittal	i
Inspector-General's review	v

SECTION ONE

OVERVIEW **1**

Role of the Inspector-General of Intelligence and Security	2
About the Australian intelligence agencies	4

SECTION TWO

IGIS ANNUAL PERFORMANCE STATEMENT **7**

Results at a glance	8
Activity 1 Inquiries	9
Activity 2 Inspections	13
Activity 3 Complaints	35
Activity 4 Public interest disclosures	40
Activity 5 Advice to Parliamentary Committees and others	43
Activity 6 Evidence to the AAT and the Australian Information Commissioner	44
Activity 7 Engagement with the intelligence agencies and the public	45
Activity 8 Liaising with other accountability or integrity agencies	47

SECTION THREE

MANAGEMENT AND ACCOUNTABILITY **49**

Part 3.1: Corporate governance 50

Part 3.2: Management of human resources 53

Part 3.3: Other information 56

SECTION FOUR

FINANCIAL MANAGEMENT **59**

Part 4.1: Financial summary 60

Part 4.2: Financial statements 64

SECTION FIVE

ANNEXURES **83**

Annexure 5.1: Performance criteria 84

Annexure 5.2: Salary scale 86

Annexure 5.3: Other mandatory information 87

Annexure 5.4: Requirements for annual reports 89

Annexure 5.5: Glossary 97

Index 98

ABOUT THIS REPORT

This is the Inspector-General of Intelligence and Security (IGIS)'s annual report for the period from 1 July 2016 to 30 June 2017.

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 Rules, section 35 of the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act), and other legislation.

THE STRUCTURE OF THIS REPORT

The Inspector-General's review summarises the issues and developments affecting the Office of the Inspector-General of Intelligence and Security (OIGIS) during the reporting period, provides an overview of its performance, and discusses the outlook for the year ahead.

Section One provides an overview of the role of the Inspector-General of Intelligence and Security, including the role and functions of the office, our published outcomes and program structure, and the purposes identified in our corporate plan. Part One also contains a brief description of each of the six intelligence agencies which the Inspector-General oversees.

Section Two is the Annual Performance Statement, detailing the office's performance during the reporting period against the indicators identified in our corporate plan.

Section Three contains information about the management and accountability of the office during 2016-17, including its organisational structure, corporate governance, management of human resources and other relevant information.

Section Four contains a summary of the Inspector-General of Intelligence and Security's financial management, and the office's audited financial statements.

Section Five contains the annexures to this report. The annexures contain a range of additional information about the office, including a map of the office's performance criteria, staff salary ranges and a glossary of abbreviations.

An alphabetical index is provided at the end of the report for ease of reference.

INSPECTOR-GENERAL'S REVIEW

This year marked the 30th anniversary of the establishment of the office of the Inspector-General of Intelligence and Security. This is an auspicious moment, both for what has been achieved and for what the future holds for this office.

Over several decades this office has earned a strong reputation for the quality of its oversight of the six intelligence agencies within its jurisdiction. Details of the past year's activities are documented in this report, in particular, in the performance statement in Section 2. Looking ahead, our future work and responsibilities will be shaped by factors recognised in the *2017 Independent Intelligence Review* discussed below.

Consultation and education are important aspects of our work in monitoring and supporting compliance. My officers and I give presentations to the agencies both in Australia and overseas explaining 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 (PJCS), 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 counterpart bodies overseas. To that end, in the last twelve months we have had discussions with representatives from Japan and from the Five Eyes countries (USA, Canada, New Zealand, the United Kingdom). In September 2016 at a meeting in Washington, the oversight bodies of the Five Eyes countries agreed to establish the *Five Eyes Intelligence Oversight and Review Council* to facilitate the sharing of experiences and best practice in oversight and review. The Council will meet in person annually and by means of secure electronic communication on a quarterly basis.

During the reporting period three inquiries were initiated by this office. Two examined the analytic independence of ONA and DIO. The third concerned ASD's interception of certain telecommunications. Inquiries such as these are inevitably intrusive for the agencies concerned and require the allocation of their valuable resources to the issues raised in the inquiries; nevertheless, my officers received the complete cooperation of the agencies concerned. Briefings and documentation were provided without delay and all queries were addressed in a timely manner. The ONA inquiry was finalised during the reporting period; the ASD and DIO inquiries were finalised, respectively, in July and September 2017 and will be reported on in next year's report.

The co-operation received during these inquiries reflects the general approach of all six agencies. They have been unstinting in their responses to our briefing requests, helping 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 facet 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.

The office has a regular program of inspections and, with one exception (see page 14) we have met our goal of inspecting 75% of an agency's activity categories. 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. In addition we have paid considerable attention to compliance with privacy rules applicable to ASIS, ASD and AGO and, in this time of interest in dual citizenship, the difficulty of determining who is an “Australian person” as defined in section 3 of the *Intelligence Services Act 2001*.

The *2017 Independent Intelligence Review* recommended far-reaching changes for Australia’s intelligence bodies. In relation to this office it recommended that the jurisdiction of the IGIS be expanded to include all ten agencies in the National Intelligence Community and that the resources of the office be increased accordingly. This proposal would bring under my jurisdiction the Australian Transactions Reporting and Analysis Centre, as well as the intelligence functions of the Australian Federal Police, the Australian Criminal Intelligence Commission and the Department of Immigration and Border Protection. The *Review* also recommended enabling the PJCS to request the IGIS to inquire into the legality and propriety of particular operational activities of the ten agencies. These recommendations would, if accepted, require a major expansion of this office and increased scrutiny of intelligence activities in Australia. In any event, it is clear that the future of this office and its oversight responsibilities will be shaped in response to “the contemporary and future challenges that our intelligence agencies face as a result of transforming geopolitical economic, societal and technological changes” recognised by the *2017 Independent Intelligence Review*.

SECTION ONE

OVERVIEW





THE ROLE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

The Inspector-General of Intelligence and Security (IGIS) 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 (OIGIS) is an agency within the Prime Minister's portfolio, with separate appropriation and staffing. As an independent statutory office holder, the Inspector-General is not subject to general direction from the Prime Minister, 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 also assists the Government in assuring the Parliament and the public that intelligence and security matters relating to Commonwealth agencies are open to scrutiny.

The OIGIS 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.



OUTCOMES AND PROGRAM STRUCTURE

The Portfolio Budget Statements (PBS) set one planned outcome for the office, which 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 *OIGIS Corporate Plan 2016-20* describes the purpose 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 Attorney-General; 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 illegal conduct or wrongdoing within the intelligence agencies;
- assist current or former public officials employed, or previously employed, by intelligence agencies, in relation to the operation of the PID Act;
- assist the intelligence agencies in meeting their responsibilities under the PID Act, including through education and awareness activities, and
- oversee the operation of the PID scheme in the intelligence agencies.

Under the *Archives Act 1983* 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 is also bound by guidelines issued by the Attorney-General under the ASIO Act. These guidelines include requirements for the collection and handling of personal information. They 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.

Security is defined in the ASIO Act as the protection of the Commonwealth, the States, the Territories and the people in them from espionage, sabotage, politically motivated violence, the promotion of communal violence, attacks on Australia's defence system, acts of foreign interference and fulfilling Australia's responsibilities to any foreign country in relation to any of these matters. Security under the ASIO Act also encompasses the protection of Australia's territorial and border integrity from serious threats.

ASIO collects information using a variety of intelligence methods including the use of human sources, special powers authorised by the Attorney-General, authorised liaison relationships, and open sources.

The Attorney-General is responsible for ASIO.

AUSTRALIAN SECRET INTELLIGENCE SERVICE (ASIS)

ASIS's primary function 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.

ASIS's collection of relevant foreign intelligence generally relies on human sources. This intelligence information is transformed into intelligence reports and related products which are made available to key policy makers and select government agencies with a clear and established need to know.

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

The Minister for Foreign Affairs is responsible for ASIS.

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 Prime Minister is responsible for ONA.

DEFENCE INTELLIGENCE AGENCIES

Three of the six intelligence agencies are 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 Minister for Defence is responsible for these Defence agencies.

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 its reports on this intelligence are provided to key policy makers and select government agencies with a clear and established need to know.

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 2016-17 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 and implemented.	
We inspected more than 75% of agency activity categories.	
We acknowledged 97% of complaints and referrals within five business days, and 87% of visa-related complaints were resolved within two weeks.	
We acknowledged 91% of public interest disclosures within five business days.	
All advice to parliamentary committees was provided by the agreed date.	
All evidence to the AAT and Australian Information Commissioner was provided by the agreed date.	
We conducted 15 presentations to AIC employees.	
We conducted 15 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 IGIS 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 IGIS 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 provides persons who have given information under compulsion with protection from any penalty under Commonwealth or Territory law that would ordinarily arise from disclosing that information. The responsible minister is advised when the IGIS begins an inquiry into an agency, and is also advised of any conclusions or recommendations arising from the inquiry. The IGIS 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 & indicators: 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 2016-17, p.234; *Corporate Plan 2016-20*

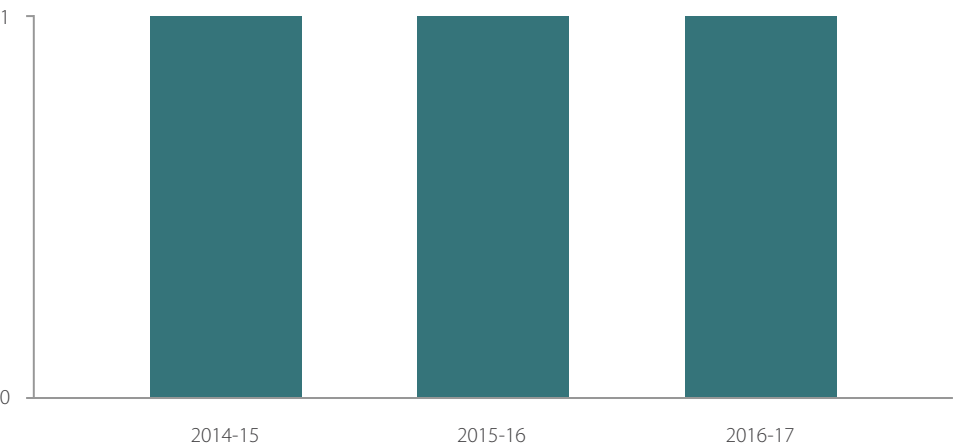


QUANTITATIVE PERFORMANCE

Figure 2.2: Performance indicators – conducting inquiries

SUBJECT OF INQUIRY	ONA ANALYTIC INDEPENDENCE	DIO ANALYTIC INDEPENDENCE	ASD MATTER
Agency	ONA	DIO	ASD
Source	IGIS own motion	IGIS own motion	IGIS own motion
Date initiated	30 August 2016	14 November 2016	2 February 2017
Date finalised	9 January 2017	Open	Open
Duration (days)	133	N/A	N/A
Number of Recommendations	Nil	N/A	N/A
Percentage of recommendations accepted	N/A	N/A	N/A
Percentage of recommendations implemented	N/A	N/A	N/A

Figure 2.3: Number of inquiries concluded by year





INQUIRIES CONDUCTED DURING 2016–17

During the 2016–17 reporting period one inquiry, with a duration of 133 days, was concluded. This duration is considered reasonable taking into account IGIS staffing levels, and the fact that this period encompassed the Christmas holiday period. There were no formal recommendations arising from the inquiry. The inquiry was conducted in accordance with s 8(3)(c) of the *Inspector-General of Intelligence and Security Act 1987* (IGIS Act), that is, an own motion inquiry into the statutory independence of ONA.

Two inquiries were in progress at the end of the reporting period. A short summary of these is provided below, and further details will be provided in the next annual report.

During the reporting period no inquiries were conducted pursuant to a ministerial direction; see s 8(1)(d) of the IGIS Act.

INQUIRY INTO THE ANALYTIC INDEPENDENCE OF THE OFFICE OF NATIONAL ASSESSMENTS

In January 2017, the IGIS completed the fourth inquiry into the analytic independence of the ONA. The inquiry was not prompted by any particular concern, but was intended to update previous inquiries. As with the previous inquiries, this inquiry found no evidence of interference with the independence of ONA assessments. It made no formal recommendations.

The assessments and other documents examined indicated that ONA observes appropriate procedures. Reports reviewed contained comprehensive endnotes that captured information from both formal and informal sources. Lengthy commentary revealing the analyst's consideration of the referenced material was often included. ONA policies and practices encourage contestability, and ONA has an appropriate structure for critically reviewing key judgments made in assessments.

While 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.

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

In November 2016 this office initiated an inquiry into the analytic independence and integrity of the Defence Intelligence Organisation (DIO). This was the third such inquiry in respect of DIO, with similar inquiries completed in 2008 and 2013. It was a routine inquiry, not prompted by any particular concern. The inquiry included a review of DIO policy, meetings with various staff and a detailed review of a sample of DIO reports produced in a twelve month period. Like the previous DIO inquiry, the current inquiry critically examined elements of the report production process directed to ensuring that the reports meet the required standards of independence and integrity.

As at 30 June 2017, a draft of the inquiry was close to finalisation, but DIO had yet to be provided the opportunity to comment on the findings. The outcome of this inquiry will be reported in the next annual report. An unclassified summary of the report will be available on the IGIS website when the inquiry is completed.

INQUIRY INTO AN AUSTRALIAN SIGNALS DIRECTORATE MATTER

In February 2017 this office initiated an inquiry into an Australian Signals Directorate (ASD) matter pursuant to s 8(2) of the IGIS Act. The final report was provided to ASD in July 2017. The Inspector-General found that ASD relied on incorrect legal advice in determining the parameters governing its interception of certain telecommunications. The inquiry also found inadequacies in ASD's reporting of the problem to the IGIS and to Ministers. The details of the incorrect legal advice and relevant contextual information are classified. 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 IGIS.

ASD has accepted all the recommendations and has agreed to report to the Inspector-General on its progress in implementing the recommendations within 6 months. The Inspector-General is satisfied with ASD's corrective measures to date and with the revised reporting arrangements between ASD and this office.

A full account of the inquiry is contained in the classified report which has been provided to the Director of ASD, the Minister for Defence and the Prime Minister and copied to appropriate Australian Government recipients for information. Given the highly classified nature and details of the inquiry, no further information will be released publicly.



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 and reviewing hardcopy documentation.

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.

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. Inspections may consist of routine inspections and inspection projects that target specific issues as determined by the IGIS.

PERFORMANCE SUMMARY

Undertaking comprehensive inspection and visit programs to monitor and review intelligence agencies' operational activity

Performance criteria & indicators: Range of inspection work undertaken

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

Source: Parliamentary Budget Statements 2016-17, *Corporate Plan 2016-20*

The OIGIS Parliamentary Budget Statements (PBS) provide for performance to be measured by both quantitative and qualitative information. One performance indicator listed in both the 2016-17 PBS and *Corporate Plan 2016-20* 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 IGIS and are based on the underlying functions of the agency laid down in the relevant legislation, namely, the *Intelligence Services Act 2001* for AGO, ASD and ASIS; the *Australian Security Intelligence Organisation Act 1979* for ASIO; and the *Office of National Assessments Act 1977* for ONA. The role of DIO is set out in a mandate agreed by the Minister for Defence, rather than in legislation. Because of this, and its role as 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 against this performance indicator is outlined in the following table.

Figure 2.4: Performance indicators - inspections

AGENCY	NUMBER OF ACTIVITY CATEGORIES	ACTIVITY CATEGORIES INSPECTED	TARGET MET? COMMENTS
ISA agencies and ASIO			
AGO	6	6	Yes
ASD	6	5	Yes There was no inspection of ASD's function to provide assistance to Commonwealth and State authorities in relation to certain specialised technologies and in their search and rescue functions.
ASIS	8	8	Yes
ASIO	7	6	Yes There was no inspection of ASIO's function to advise Ministers and other Commonwealth authorities on matters relating to protective security.
Assessment agencies			
DIO	4	4	Yes
ONA	2	1	No Inspections were focused on ONA's compliance with Privacy Guidelines. There were no inspections of ONA's access to and use of AUSTRAC information.

INSPECTION OF ASIO ACTIVITIES

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

- intelligence collection
- intelligence communication
- advice about security to 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 and cooperation with and assistance to other intelligence agencies.

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



REGULAR INSPECTIONS OF INVESTIGATIVE CASES

It is not possible to monitor all ASIO's activities with existing OIGIS resources. Accordingly IGIS officers inspect a sample of activities selected on the basis of risk. The investigation and inspection team has direct access to ASIO's information technology and records management systems. During this reporting period, IGIS staff have liaised with ASIO to acquire increased access to ASIO's systems. This has improved our ability to access, view and interrogate a wider range of ASIO's records.

Throughout 2016-17 the investigation and inspection team focused on reviewing those cases where the most intrusive methods and activities had been used, as well as those activities that presented an increased likelihood of non-compliance with legislation or policy, for example cases with 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 including formal approval processes, the timeliness of periodic reviews and the proportionality of its methods (that is, using less intrusive methods where possible and only progressing to increasingly intrusive methods as required)
- compliance with internal policies and procedures.

ANALYTIC TRADECRAFT

ASIO produces a range of analytic products covering its various functions, including security assessments, applications for warranted powers, investigative reviews and ASIO's published analytic products. Within the Australian intelligence community ASIO has a unique role in collection and assessment. Its assessment activities have a greater potential to intrude into the privacy of Australians than those of the assessment agencies DIO and ONA. They may also result in ASIO providing specific policy guidance to Government. Because of this the OIGIS investigation and inspection team conducts regular reviews of ASIO's intelligence product. These reviews enable the IGIS to monitor the independence, analytic rigour and propriety of the assessments contained in ASIO's products. In the last reporting period the office commenced a new inspection specifically to examine ASIO analytic tradecraft. Two such inspections were conducted in the 2016-17 year. No concerns of legality were identified in the first inspection of the reporting period although the inspection revealed inconsistencies in source referencing indicating the need for some improvement in this area. Following this inspection, ASIO implemented new analytic tradecraft policies which provide more comprehensive advice to analysts concerning referencing practices. The second inspection activity on analytic tradecraft was not finalised at the end of the reporting period.

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, OIGIS officers inspected and reviewed ASIO human source case files and met with ASIO staff to discuss related activities. No substantive issues of concern were identified by OIGIS officers when reviewing these activities. One issue identified related to record keeping. This issue was discussed with senior ASIO staff. We are satisfied this issue will be addressed.

ASIO WARRANTS

In the 2016-17 year IGIS officers inspected a large number of warrants although fewer than in previous years. In part the reduced numbers were due to staffing constraints as well as a move to more in-depth reviews that focus on the analytic integrity of supporting documentation and the execution and conduct of ASIO's warranted operations. The decision to concentrate on these factors rather than procedural aspects of ASIO's warrants reflects ASIO's high degree of compliance with formal and procedural requirements. Notwithstanding the change, it is gratifying to note that during this reporting period ASIO proactively informed this office of three breaches relating to warrants issued under the *Telecommunications (Interception and Access) Act 1979* (TIA Act). IGIS staff identified one additional breach not identified by ASIO staff, relating to a warrant authorised under the ASIO Act. The number of breaches in this reporting period is less than in the most recent reporting period. The circumstances of these breaches are summarised below.

BREACHES OF THE TIA ACT

Two of the three breaches of the TIA Act referred to above were unauthorised interception of communications. One involved ASIO mistakenly identifying an internet protocol (IP) address which was not authorised for interception; the other occurred when a telecommunications service provider made a mistake and sent ASIO data that was not authorised for interception. In each case ASIO staff discovered the error (within 11 and two days respectively), took action to end the unauthorised interception and advised this office of the breaches. During the 2017-18 reporting period this office will review the efficacy of the actions taken by ASIO in response to these errors.

The TIA Act requires ASIO, within 3 months of a warrant expiring, to give the Attorney-General a written report detailing the extent to which the interception of communications assisted ASIO to carry out its functions. In the case of the third breach, ASIO submitted its report one day after expiry of the prescribed period. This error did not raise any concerns of systemic or cultural problems, especially as ASIO proactively informed the IGIS that the report would be one day overdue and, we understand, that the delay was occasioned by matters outside ASIO's control.

BREACH OF WARRANT PROVISION OF THE ASIO ACT

The fourth breach was discovered by IGIS officers during a warrant inspection. The ASIO Act requires that, among other things, a search warrant must authorise "the use of force against persons and things ...". No force was to be used by ASIO in the search conducted under this warrant, nor was force used during the execution of the warrant; nevertheless, the omission of the express authorisation breached the requirements of the Act. The IGIS considered that this breach did not invalidate the warrant. ASIO has assured the IGIS that this provision will be included in the future regardless of whether ASIO expects force to be used in the execution of the warrant. Further information about ASIO's use of force is on page 17 of this report.



OTHER WARRANT MATTERS

During the current reporting period fewer breaches of legislation were identified, however there has been an increase in minor typographic errors in warrant documents. While reference to wrong warrant numbers or in the identification of an email service can cause confusion, most of these errors are not important in themselves. Nevertheless, we consistently note these minor errors to help us determine if, over time, they indicate a systemic or cultural tendency that would be of concern. In response to these incidents and our concerns, ASIO has implemented new processes, including mandatory peer review processes to ensure that warrant documentation is accurate.

QUESTIONING AND DETENTION WARRANTS

The Attorney-General did not authorise any Questioning or Questioning and Detention warrants during the reporting period. The office has procedures in place to oversee ASIO's questioning powers if these powers are used.

In the 2016-17 year, the IGIS made a submission to the Parliamentary Joint Committee on Intelligence and Security regarding ASIO's Questioning and Questioning and Detention powers contained in Division 3 of Part III of the ASIO Act. This submission outlined the role of the IGIS office in relation to ASIO's questioning and detention powers and highlighted a number of safeguards that should be maintained to ensure effective oversight of any new regime of compulsory questioning powers for ASIO that may replace the current regime.

JOURNALIST INFORMATION WARRANTS

During the reporting period ASIO has complied with the legislative requirements in respect of journalist information warrants set out in Division 4C of the TIA Act. In the course of our regular inspections we have observed that ASIO staff are familiar with ASIO internal policies and procedures relating to journalist information warrants. In one case, ASIO mistakenly obtained call charge records for a telephone service belonging to a newspaper's classifieds service. The metadata was collected due to a typographical error and was subsequently deleted. ASIO's response to this mistaken collection of metadata demonstrated ASIO staff's awareness of the legal requirements for obtaining a journalist information warrant.

USE OF FORCE

Warrants issued under the ASIO Act must explicitly authorise the use of force that is 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 IGIS in writing, as soon as practicable. The ASIO Act does not specify a timeframe for the provision of these reports but 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. ASIO can seek these authorisations to assist in the performance of its special intelligence functions, and where the circumstances justify the conduct of a special intelligence operation. The legislation requires ASIO to notify the IGIS as soon as practicable after an authority is given. All special intelligence operations approved during the reporting period were notified to the IGIS 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 IGIS. Reporting was made available to IGIS staff who have reviewed documentation on special intelligence operations. There are no outstanding reporting requirements for the 2016-17 reporting period. The details of special intelligence operations are highly sensitive and cannot be included in a public report, however, during the reporting period no substantive issues or concerns were identified when reviewing these activities.

ACCESS TO TELECOMMUNICATIONS DATA

The TIA Act enables certain persons to authorise the collection of prospective and historical telecommunications data from telecommunications carriers or carriage service providers. Prospective data authorisations are authorised internally at ASIO for the period the authorisation is in force. Collection under a prospective data authority can only be undertaken by ASIO in connection with the performance of its 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 reviewed were authorised at the appropriate level, were undertaken in connection with ASIO's functions, and demonstrated regard for the Attorney-General's Guidelines.

In a small number of instances ASIO obtained data under a prospective data authority that did not relate to the subject of the authority. In these instances ASIO deleted the data. The office also identified some record keeping issues with records not saved in accordance with ASIO's internal policies. None of these events was of significant concern, nor did they indicate a systemic problem at ASIO.

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 OIGIS review as part of our periodic inquiry and investigation inspections.

During the reporting period, ASIO undertook exchanges of information with a number of Australian Government agencies including the Australian Criminal Intelligence Commission, the Australian Federal Police, State and Territory police services, the Department of Immigration and Border Protection and the Department of Foreign Affairs and Trade. Regular inspection activity included reviewing these exchanges to assess ASIO's compliance with legislation, the Attorney-General's guidelines and ASIO policy. No major areas of concern were identified during these inspections. A small number of administrative errors were found however, once notified, these were explained and rectified by ASIO.



ACCESS TO TAXATION INFORMATION

Section 355-70 of Schedule 1 to the *Taxation Administration Act 1953* provides that a taxation officer authorised by the Commissioner of Taxation or their 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. IGIS staff will review ASIO access to taxation information for the 2016-2017 period in July 2017. The results for this inspection will be included in next year's annual report.

ASIO EXCHANGE OF INFORMATION WITH FOREIGN LIAISON

The ASIO Act authorises ASIO to provide and to seek information relevant to Australia's security, or the security of a foreign country, from authorities in other countries. ASIO may only cooperate with foreign authorities approved by the Attorney-General.

ASIO has implemented guidelines for the communication of information on Australians and foreign nationals to approved foreign authorities. These guidelines impose an internal, risk-based framework for assessing and approving the passage of information, based on such factors as ASIO's previous experience dealing with the authority, how the authority manages information, and the authority's history in relation to human rights issues.

During 2016-17 the investigation and inspection team 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 conflict in Syria and other high-risk areas. While no major areas of concern were identified, a small number of administrative and record keeping issues were found and brought to ASIO's attention. We will continue to monitor exchanges with foreign countries.

MINISTERIAL SUBMISSIONS

The office of the IGIS regularly reviews a range of submissions to the Attorney-General. During the current reporting period IGIS staff were provided with improved access to these documents. These reviews continue to be useful in obtaining an overview of legality and propriety issues, and to keep the IGIS informed of current operations and emerging issues.

SECURITY ASSESSMENTS

Security assessments can lead to cancellation or refusal of visas or passports. The investigation and review team continued to review a sample of cases where ASIO had requested passport suspension, passport cancellation or emergency visa cancellations. In 2016-2017 IGIS staff conducted two inspections reviewing security assessments that resulted in visa and passport cancellations. In the first inspection no issues of legality were identified, however the office did raise a number of issues regarding record keeping and referencing. The second inspection is currently being finalised and will be reported on in the 2017-2018 annual report. The office will continue to monitor these issues.

BREACH OF SECTION 38(7) OF THE ASIO ACT

The ASIO Act requires that, where ASIO has issued a qualified or adverse security assessment in respect of a person to a Commonwealth agency or a state or an authority of a state, that agency, state or authority shall give notice the assessment to that person within 14 days. However, the Act also provides that the notice may be withheld, where the Attorney-General certifies that they are satisfied that withholding the notice is essential to the security of the nation. The Act requires that if such certification is issued, the Attorney-General must annually consider if the certificate should remain in force, or whether the subject of the security assessment can be provided with notice of the 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 each year the Attorney-General will need to rely on ASIO advice in order to meet this statutory obligation.

In 2016, ASIO did not provide the Attorney-General with the necessary information to enable the Attorney-General to consider whether a number of certificates should be revoked. Potentially the individuals concerned were denied the benefit of a favourable reconsideration, namely the information that their passports had been cancelled; and that the underlying security assessments could be subject to review.

ASIO identified this oversight and subsequently conducted an internal review of all similar certificates. ASIO did not notify this office of the breach or subsequent review; IGIS staff became aware of the breach and the internal review while inspecting submissions to the Attorney-General.

ASIO's internal review identified four similarly affected cases. In each of those four cases ASIO's subsequent review resulted in ASIO changing its assessment, and recommending to the Attorney-General that withholding notice of the security assessment was no longer essential to the security of the nation. This office had some concern about the length of time taken to rectify ASIO's error; in one instance ASIO took five months to issue its advice to the Attorney-General.

This problem appears to have arisen from an administrative oversight when the provisions came into effect in December 2014. Whilst this oversight has since been rectified, the office was concerned by the significant impact of non-compliance upon the rights of the individuals concerned. Also of great concern was that ASIO had made the determination to delay notifying the Inspector-General of this oversight until after ASIO had fully resolved the matter. This decision was not in accordance with ASIO's longstanding practice of providing timely notification to this office when non-compliance was identified. This issue was further compounded when ASIO incorrectly advised the Attorney-General that ASIO had reported the issue to the IGIS, when this had not occurred. The OIGIS identified this error through the course of its periodic inspections and ASIO subsequently wrote to the Attorney-General to correct this inaccuracy. ASIO has accepted that it should notify this office immediately when issues of non-compliance are identified and has taken a number of steps to ensure that issues of non-compliance are promptly reported to the IGIS.



CITIZENSHIP

In December 2015, Parliament introduced sections 33AA and 35 into the *Australian Citizenship Act 2007*. These amendments provide for the cessation of Australian citizenship where an Australian citizen who also has citizenship of another country engages in conduct specified in section 33AA(2) of that Act. It is noteworthy that these provisions are self-executing, that is they take effect automatically upon a dual citizen engaging in the specified conduct. Formal administrative action by any Australian Government agency is not required for their operation. The office of the IGIS has a continuing interest in the way in which ASIO understands and discharges its responsibilities under the amended legislative framework and this will be a matter of ongoing consideration.

REVIEW OF ATTORNEY-GENERAL'S GUIDELINES

In addition to inspection activities, the IGIS also provided input into the review of the Attorney-General's Guidelines being undertaken by ASIO and the Attorney-General's Department. The Guidelines are issued under section 8A of the ASIO Act and are to be observed by ASIO in the performance of its functions. The Parliamentary Joint Committee on Intelligence and Security, as part of its review of the *National Security Legislation Amendment Bill (No 1) 2014*, recommended that the Government review these Guidelines. Subsequently the Government initiated the review of the Guidelines which was ongoing at the end of the reporting period.

ASIO INSPECTION PROJECTS

DEVICES PROJECT

ASIO staff may deploy a range of technical devices to gather intelligence. In November 2016, the IGIS initiated an inspection project focusing on ASIO staff access to surveillance devices and other technical devices used for this purpose. The aim of the project is to provide assurance that ASIO's internal accountability measures ensure that devices are only deployed for the purposes of conducting authorised investigations. This project will continue through 2017-18.

ONLINE INVESTIGATIONS

In November 2016 the IGIS initiated an inspection project focusing on ASIO's online investigative activities. This 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 investigative targets and the broader public alike. The project is ongoing and will assess the legality and propriety of ASIO's activities and identify high risk activities that may require further consideration by IGIS staff.

PROTECTING COMPLAINANT INFORMATION

Some years ago ASIO and IGIS agreed on a protocol for the management of information concerning complaints or public interest disclosures made to the IGIS. This protocol, which was last updated in 2011, 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 March 2017, the investigation and review team identified a number of instances where this protocol had not been adhered to. ASIO subsequently conducted a comprehensive review, and has proposed a number of improvements to their process to lessen the possibility of recurrence. We will consider the proposed changes in the next reporting period.

AGENCIES SUBJECT TO THE *INTELLIGENCE SERVICES ACT 2001*

LIMITS TO THE FUNCTIONS OF INTELLIGENCE AGENCIES

The functions of agencies governed by the *Intelligence Services Act 2001* (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 Defence Force
- 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 IGIS 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 located in Australia is an Australian person, and that a person who is located outside 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 requirement if intelligence collection 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 IGIS of this and the measures taken to protect the privacy of the Australian concerned.

INSPECTION OF ASIS ACTIVITIES

During 2016–17, IGIS staff conducted a range of regular inspections of ASIS activities. These inspection activities are supplemented by briefings on various matters across the year that either this office requests, or are provided proactively by ASIS. Such briefings and follow up investigations allow the office to stay abreast of emerging issues, or follow up trends observed in inspection activities.

MINISTERIAL AUTHORISATIONS TO PRODUCE INTELLIGENCE ON AUSTRALIAN PERSONS

IGIS staff reviewed all Ministerial submissions produced by ASIS and found that in general they were of a high standard and were complemented by ASIS's habit of self-reporting instances of non-compliance.

During 2016-17, ASIS self-reported an instance of non-compliance with section 8(1)(a)(i) of the ISA that had occurred during the 2015-16 reporting period, that is, where ASIS had collected intelligence on Australian persons without proper authorisation. This instance involved ASIS receiving reporting from a liaison partner after a threat to security ministerial authorisation had expired and before the individual was included in a class section 13B notice. During the intervening period, ASIS was required to alert liaison partners that it does not have the proper authority to collect intelligence on this particular individual.

ASIS notified the IGIS office of four instances where, during 2016-17, it had undertaken an activity without the authorisation required by the ISA. ASIS also conducted internal investigations into how and why the breaches occurred. While the sensitive nature of ASIS's activities means that further details of these matters cannot be provided here, the Inspector-General is satisfied that ASIS's internal investigations and subsequent remediation were methodical and thorough.

There was also one instance where a member of ASIS engaged with a foreign Government agency without the appropriate authority. Section 13(1)(c) of the ISA requires ASIS to seek approval from the Minister for Foreign Affairs before cooperating with authorities of other countries. As such, the engagement with the foreign authority was non-compliant with section 13(1)(c). ASIS subsequently received authorisation to engage with the authority and provided refresher briefings to the officer involved.

EMERGENCY MINISTERIAL AUTHORISATIONS

There were three instances where ASIS sought an oral authorisation from the Minister in an emergency using the section 9A provisions in the ISA. In all three cases, ASIS complied with section 9A(5)(a) of the ISA by ensuring that a written record of an authorisation given under section 9A was made no later than 48 hours after the authorisation.

ASIS reported that it was non-compliant with section 9A(5)(b) of the ISA with one authorisation. That is, ASIS did not provide a copy of the record to the IGIS within three days of the authorisation was given. Due to public holidays, this office was closed during the period when the authorisation being made. As ASIS provided the record on the day the office re-opened, the Inspector-General had no concerns about the delay in notification.

Under s 10A(4) of the ISA, ASIS is required to provide the Minister with a written report in respect of each activity carried out in reliance on an authorisation provided under s 9A or 9B, within one month of the day on which the relevant authorisation ceased to have effect. ASIS



identified a case where it was non-compliant with this requirement relating to an emergency authorisation provided in late 2015-16. ASIS notified the Minister of the error accordingly. The submission to the Minister also noted, erroneously, that it had notified this office of the breach. ASIS subsequently wrote to the Minister and to this office, correcting the advice in its initial submission.

There were two instances during the reporting period where the Director-General of ASIS exercised his power to give an authorisation in an emergency when the minister is not available. As these legislative provisions are relatively new for the intelligence agencies, having come into effect in 2014, the IGIS office has closely examined their use by ASIS.

Section 9B(8A) of the ISA requires the Inspector-General, within 30 days to:

- consider whether the Director-General complied with the requirements of section 9B in giving the authorisation; and
- with respect to ASIS, provide the Minister for Foreign Affairs with “a report on the Inspector-General’s views” of the extent of the Director-General’s compliance with the requirements of section 9B in giving the authorisation; and
- provide the Parliamentary Joint Committee on Intelligence and Security a copy of the conclusions in that report.

In relation to both emergency authorisations, the Inspector-General concluded that the Director-General’s actions in the circumstances were appropriate and reasonable and ASIS provided timely and comprehensive briefings to the Inspector-General. In relation to the first emergency authorisation, however, the Director-General’s approval did not meet a critical statutory requirement. This is because the Director-General gave oral approval followed by a written record of the approval rather than making the authorisation in writing. This was not consistent with the ISA which requires the authorisation itself to be in writing; a later recording of the decision in writing is not in accordance with the Act. The Inspector-General noted that ASIS took immediate steps towards enabling it to address the legislative requirements in any future cases. The IGIS was satisfied that ASIS acted in accordance with the requirements of the ISA for the second emergency authorisation.

The Inspector-General provided the Minister for Foreign Affairs with a report discussing the extent of the Director-General’s compliance with the requirements of s 9B in giving the authorisation. A copy of the conclusions in that report was given to the Parliamentary Joint Committee on Intelligence and Security.

SECTION 13B NOTICES

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. For this power to be enlivened it is necessary for ASIO to provide ASIS with a notice saying that it requires the production of intelligence on the Australian person or class of Australian persons. Alternatively, an authorised ASIS officer must reasonably believe that it is not practicable in the circumstances for ASIO to notify ASIS before the intelligence about the Australian(s) can be collected. The IGIS office continued to monitor the use of s 13 of the ISA throughout 2016-17 and was satisfied there were no instances where ASIS officers authorised collection using the s 13B power without notification from ASIO.

Under s 13F(4) of the ISA, as soon as practicable after each year ending 30 June, ASIS must provide a written report in respect of ASIS activities undertaken in accordance with s 13B during the reporting year. ASIS met this requirement and the IGIS is satisfied that ASIS appropriately advised the Minister of the details of the individual s 13B notices and class s 13B notices.

PROTECTING THE PRIVACY OF AUSTRALIAN PERSONS

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

Throughout 2016-17 a number of occasions were identified where the privacy rules were not applied prior to ASIS reporting on an Australian person or company. The non-application of privacy rules was due either to human or technical error. Of these cases, none was identified where reporting on an Australian person would not have been reasonable and proper had the rules been applied at the time. The IGIS is confident that the total number of cases where there were issues was a very small percentage of the overall amount of intelligence produced by ASIS.

ASIS reported two occasions in 2016-17 where the 'presumption of nationality' was overturned; that is, information became known that an individual was actually an Australian person. In these instances there was no breach of the rules as the presumption of nationality was reasonable at the time they were made and the information indicating the individuals were Australian was not available at that time.

REVIEW OF OPERATIONAL FILES

ASIS activities involve the use of human sources. Its officers are deployed in many countries to support a wide range of activities including counter-terrorism, efforts against people smuggling and support to military operations. These activities are always sensitive and often high-risk.

Reviews of ASIS's operational case files during 2016-17 involved inspecting a sample of files which had been selected by OIGIS officers. The inspections focused on high-risk issues including the appropriate application of the privacy rules. These inspections provide insight into the operational environment in which field officers operate, the extent to which staff in ASIS headquarters evaluate risk and guide sensitive activities, and often indicate the health of inter-agency relations. 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.

During the reporting period, IGIS staff were unable to locate some records and raised concerns with ASIS about its recordkeeping. ASIS conducted an internal investigation into the issue; it identified the source of the error as faults in its information communications technology and implemented several strategies to remedy the problem. The total number of cases where there were issues proved to be a very small percentage of the overall number of records produced by ASIS.



AUTHORISATIONS RELATING TO THE USE OF WEAPONS

Schedule 2 of the ISA requires the Director-General of ASIS to provide the Inspector-General with:

- copies of all approvals issued by the Minister of Foreign Affairs in respect of the provision of weapons and the training in and use of weapons and self-defence techniques in ASIS
- a written report if a staff member or agent of ASIS discharges a weapon other than in training.

This reporting requirement was met during 2016-17 and the Inspector-General was satisfied that there is a genuine need for limited numbers of ASIS staff to have access to weapons for self-defence in order to perform their duties.

During 2016-2017 OIGIS officers also examined ASIS weapons and self-defence policies and guidelines as well as its training records. The inspections found that ASIS's approach to governance and record keeping on these matters to be appropriate.

Throughout the reporting period, the ASIS Compliance Branch focused on training and audit activities in areas that present the greatest risk of a weapons-related incident occurring. It reviewed its controls surrounding drug and alcohol testing associated with weapons qualifications. As a result of that review, ASIS improved the monitoring of its drug testing regime. ASIS regularly updated this office of its activities in this area. ASIS also reported two instances of non-compliance with ASIS's procedures as described in its internal weapons guidelines.

The first involved an ASIS officer transporting a weapon without the proper authority to do so. The officer was travelling with members of the Australian Defence Force who were carrying weapons for force protection. It is understandable that the ASIS officer would also want to carry a weapon for self-defence (force protection) purposes however their actions were not in accordance with ASIS's policies and procedures. The sensitive nature of ASIS's operational activities precludes further details being provided in a public report, however, having reviewed the incident the Inspector-General is confident that, despite the officer's noncompliance with ASIS procedures, at all times the weapon was secure. ASIS provided refresher briefings to the officer on their obligations under the weapons guidelines.

The second incident involved officers purchasing oleoresin capsicum spray (pepper spray) contrary to ASIS's policies and procedures. The spray was not used and was returned to the place of purchase as soon as the non-compliance issue was identified. ASIS provided refresher briefings to those officers on their obligations under the weapons guidelines.

INSPECTION OF ASD ACTIVITIES

During 2016-17 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
- cyber activities
- ASD's access to sensitive financial information (discussed later in the report).

These inspections are 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

allow the office to stay abreast of emerging issues, and to pursue trends observed during inspections.

In this reporting period a significant focus for the office was an inquiry into ASD's interception of certain telecommunications outside authorised parameters. The ASD inquiry was labour intensive and, with the inquiry into the analytic independence and integrity of DIO, completing these inquiries meant diverting some staff from ASD inspections. Consequently, the office reviewed fewer ministerial authorisations to produce intelligence on Australian persons than in the previous reporting period, and was not able to complete any in-depth inspections of these authorisations.

MINISTERIAL AUTHORISATIONS TO PRODUCE INTELLIGENCE ON AUSTRALIAN PERSONS

During 2016–17 the office inspected about two-thirds of ASD's ministerial authorisations, down slightly on the previous reporting period. The submissions were generally of a high standard. In some cases, however, the office was able to suggest possible improvements for future submissions to the Minister. These matters were not significant, and ASD's response to these suggestions was appropriate.

When ASD seeks to renew a ministerial authorisation there can be a period between the expiry of the previous authorisation and approval of the renewal during which ASD must not attempt to produce intelligence or engage in other activities relating to the subject of the ministerial authorisation. In such cases IGIS officers investigate whether ASD ceased relevant activities during the relevant period. The office identified only one case where ASD conducted an activity during a short period between the expiry and renewal of the authorisations. ASD accepted the finding and its investigation into the incident was ongoing at the end of the reporting period.

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 a report on its activities that relied on the authorisation. We reviewed a number of these cancellation and non-renewal reports and did not identify any concerns.

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 Defence Minister, other select ministers where the Defence Minister 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 the relevant activity.

One emergency ministerial authorisation was issued for ASD during the reporting period. This authorisation is associated with an ASD compliance incident report provided to this office on 30 June 2017. This office will report on this matter in the next reporting period.



PROTECTING THE PRIVACY OF AUSTRALIAN PERSONS

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 and during inspections IGIS staff pay close attention to ASD's compliance with the privacy rules and to its distribution of intelligence about Australian persons. In accordance with its obligations under the privacy rules, ASD has continued to report cases where the presumption that an individual is not an Australian is subsequently rebutted and the person is shown to be Australian. These reports include details of the measures taken to protect the privacy of that person. In all such cases reported to this office by ASD, the presumption of nationality was reasonable based on the information ASD had at the time. The actions taken by ASD, including informing other intelligence agencies that the person is Australian, were appropriate and in accordance with the privacy rules. To ensure there are adequate safeguards to protect the privacy of Australians ASD has also consulted with this office in relation to such matters as expanding information sharing with other countries.

There was one breach of the privacy rules, which occurred at the end of 2015–16 but was reported to this office in 2016–17. This breach resulted from human error where intelligence information on an Australian person was not removed from a wider dataset that was passed to a foreign intelligence agency. The office accepted ASD's account of this case, and was satisfied with the remedial actions ASD took to minimise the risk of this recurring.

Before being informed of this breach, the IGIS was briefed on ASD's procedures to redact information about Australians. The circumstances detailed in that briefing were similar to those of the breach, however the breach was not raised. The IGIS subsequently raised with Director ASD the need for ASD staff to be more candid in any future briefings. A lack of timely, detailed advice was also an issue in relation to the compliance incident report that prompted this office to undertake the inquiry into ASD. Subsequently, in the latter part of 2016–17, there has been a marked improvement in the openness of ASD's reporting and in its timeliness.

COMPLIANCE INCIDENT REPORTS

Where ASD identifies matters involving breaches of legislation and significant or systemic matters of non-compliance with ASD policy, these are investigated by ASD and reported to the IGIS in compliance incident reports. This office reviews these reports and undertakes an investigation of the incident where necessary. ASD provided four such reports during 2016–17; one of these was provided on 30 June and, the results of our review will be reported in the next annual report.

In August 2016 ASD advised this office of its investigation into an incident that involved sharing certain types of data in support of operations in Afghanistan. The data intended to be shared included some data that ASD was not authorised to share. There was no resultant legislative breach as technological safeguards ultimately prevented non-compliant data from being shared. The ASD investigation made recommendations to improve the management of information sharing. This office was satisfied with ASD's investigation and remedial action proposed to prevent recurrence.

There was another incident in August 2016 after ASD collected intelligence about an individual in breach of the of the *Telecommunications (Interception and Access) Act 1979*. The Inspector-General formed the view that the cause of this breach was a failure to follow extant policies and

procedures with the requisite care but was satisfied with the remedial actions proposed and implemented by ASD.

In December 2016, ASD reported on three breaches of the *Telecommunications (Interception and Access) Act 1979*. The configuration of an ASD collection system had led to it collecting certain telecommunications beyond the scope of the relevant warrant. In doing so ASD had relied on legal advice to the effect that communications beyond the scope of the warrant could be lawfully collected provided they were later destroyed. This led to the IGIS inquiry into the matter; the inquiry report was finalised and submitted to all relevant parties several weeks after the end of the current reporting period.

Among the concerns discussed in the report was the adequacy and timeliness of ASD's communications about the issues including to Ministers and to this office. An initial communication merely stated that there had been a breach but did not give any further details. It was some months before additional details were provided. This was not consistent with the written guidance given to ASD about IGIS reporting expectations nor was it consistent with this office's reliance on agencies proactively reporting issues of legality and propriety. Since this issue was drawn to ASD's attention, which was well before the inquiry was completed, it has been gratifying to record that there have been noticeable improvements in the reporting on compliance matters to this office. The final report was submitted to all relevant parties some weeks after the end of the current reporting period. It contained classified recommendations designed to improve communications and prevent any future such issue.

As at 30 June ASD had also reported four additional breaches of the ISA and *Telecommunications (Interception and Access) Act 1979*. These matters were being investigated and will be reported on in the next annual report.

CYBER ACTIVITIES

In October 2016 this office concluded an inspection project in relation to ASD computer network operations, including sensitive cyber operations in support of ADF operations in Iraq and Syria. The project noted that ASD's offensive cyber capabilities are evolving rapidly and the governance frameworks underpinning some areas are still developing. This project found guidance in place at the time was appropriate and followed by staff, and no issues of legality or propriety were noted. This office continues to maintain an interest in the cyber activities of ASD.

INSPECTION OF AGO ACTIVITIES

During 2016-17 there were regular inspections of a number of AGO activities, including:

- 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)

Throughout the year, these inspection activities were supplemented by briefings on various matters that either this office requests, or were provided proactively by AGO. Such briefings and investigations allows this office to stay abreast of emerging issues, or followup on trends observed during inspection activities.

Based on inspection and review activities, the IGIS is satisfied that AGO takes its statutory obligations under the ISA seriously and that it has in place systems to encourage compliance. Legislative breaches and other serious issues are brought to the attention of the Director of AGO and this office in a timely manner.

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 2016-17, our inspections of AGO's ministerial authorisations did not identify any concerns relating to AGO's ministerial authorisations, their renewals, cancellations or non-renewals. AGO did not seek any emergency ministerial authorisations.

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 or imagery intelligence of Australian territory. The Director of AGO provides the Minister with quarterly reports on the approved intelligence activities. The accuracy of these and other reports provided to the Minister for Defence were also reviewed by this office. No concerns were identified.

The Director's approval is often subject to conditions. During 2016-17, AGO identified only minor issues of non-compliance in relation to these conditions and this office is satisfied that AGO has taken appropriate remedial action and steps to monitor and respond to issues. At the conclusion of approved activities, AGO staff prepare a post activity compliance report for the Director and this office regularly examines them. No concerns were identified in the current reporting period.

AGO COMPLIANCE WITH PRIVACY RULES

The Minister for Defence makes written rules, the *Rules to Protect the Privacy of Australians*, to regulate how AGO communicates and retains intelligence information concerning Australian persons. During the 2016-17 reporting period, this office did not identify any issues relating to AGO's compliance with the privacy rules.

BREACHES OF THE *INTELLIGENCE SERVICES ACT 2001*

AGO proactively reports issues of legality and propriety to the IGIS. While working on a task in support of another intelligence agency, AGO, in breach of section 8(2) of the ISA, produced imagery intelligence of Australian territory without the Director's approval. In July 2016, AGO provided this office with a clear account of what occurred and the remedial action it had taken to avoid any similar breaches in the future.

In November 2016, AGO reported a breach of sections 8(3) and 12(a) of the ISA. The breach involved AGO collecting intelligence that was not of a geospatial or imagery nature and therefore was outside AGO's functions under the Act. This office was satisfied with the remedial actions taken by AGO to address the specific issue as well as to prevent any future recurrence, which included changes to AGO's training that incorporated lessons learned from this breach.



OTHER ACTIVITIES

AGO has continued to keep this office informed about organisational changes resulting from the Defence *First Principles Review*. Among these changes is the growth in the organisation which has required restructuring its ISA training. This office intends to attend AGO's amended ISA training during the 2017-18 period as well as AGO's internal capability and awareness briefings. These initiatives will provide this office with greater insight into AGO's operations and will enable the office to keep abreast of developments.

INSPECTION OF DIO ACTIVITIES

This reporting period was marked by more involvement in reviewing DIO activities than in the previous year. This greater involvement followed from the inquiry into the analytic independence and integrity of DIO which focused on how DIO develops its intelligence reporting and assessments. The inquiry was ongoing at the conclusion of the 2016-17 financial year. The inquiry was not prompted by any particular concern but is one of a regular series of reviews of DIO's analytic independence, earlier reviews having been carried out in 2008 and 2013.

Routine inspections of DIO have continued to be limited to its compliance with the *Guidelines to Protect the Privacy of Australian Persons*, and its access to sensitive financial information from AUSTRAC. These inspections 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.

COMPLIANCE WITH DIO'S PRIVACY GUIDELINES

DIO's compliance with its privacy guidelines is reviewed twice a year. These guidelines, which are available on DIO's 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. This office did not identify any significant issues or concerns, and there was no evidence that DIO breached the privacy guidelines.

INSPECTION OF ONA ACTIVITIES

This financial year was marked by more involvement in reviewing ONA activities than in the previous year, as the IGIS undertook an inquiry into the analytic independence of ONA. Details about the inquiry are provided on page 11 of this report. Our routine inspections of ONA were limited to two inspections focused on ONA's compliance with its privacy guidelines. In these inspections only a small number of interpretative and administrative errors were identified however none led to intelligence information about an Australian person being disseminated without an appropriate underlying basis for doing so.

CROSS-AGENCY INSPECTIONS

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

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 containing information about the assumed identities created and used during the year. The Director-General of Security and the Director-General of ASIS provided the IGIS with reports covering the activities of their respective agencies for the 2015-16 reporting period. There was nothing in the ASIO report to suggest that the agency was not complying with its legislative responsibilities.

ASIS reported a breach of section 15KE where an officer returning from extended leave resumed use of an assumed identity without the formal variation being authorised at the time. A formal variation for the use of the assumed identity was subsequently authorised. No evidence of fraud or other unlawful activities was identified during the reporting period.

ACCESS TO SENSITIVE FINANCIAL INFORMATION BY INTELLIGENCE AGENCIES

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

The IGIS is party to a memorandum of understanding (MOU) with AUSTRAC. This MOU establishes an agreed understanding of IGIS's role in monitoring access to, and use of, AUSTRAC information by agencies.

In overseeing an agency's use of AUSTRAC information, IGIS officers check that there is a demonstrated intelligence purpose that pertains 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 the IGIS prepares a statement summarising compliance monitoring in respect of ASIO, ASIS, AGO, ASD and DIO concerning, respectively, their access to, and use of, AUSTRAC information in the previous reporting period. As required under the MOU, during 2016-17, this statement was sent to the Attorney-General, the Minister for Foreign Affairs and the Minister for Defence.

Review of access to sensitive financial information by ASIS, ASD, AGO and DIO during 2016-17 did not reveal issues of any material concern. The inspections revealed that ASIS's governance



and record keeping relating to this information continue to be effective, with no breaches of the ISA or non-compliance with the ASIS guidelines. This was also true of ASD, DIO and, with some scope for improvement in its record keeping, of AGO.

Review of ASIO's access to AUSTRAC material during 2016-17 raised two issues:

- ASIO identified a breach of ASIO's memorandum of understanding with AUSTRAC regarding the provision of information to a foreign intelligence service. In this instance the requisite level of internal approval had not been sought. Once the breach was identified ASIO promptly notified this office, and took appropriate measures to reduce the likelihood of this error recurring.
- In two instances ASIO retained AUSTRAC data which did not relate to the intended subject of a search. There are circumstances in which ASIO will require access to information in order to identify whether the person is or could be identical to the subject of the active investigation. In this instance this information was not purged or quarantined from ASIO systems once it was determined that it did not relate to the intended subject. Our office is currently liaising with ASIO, and expects to resolve this matter in the 2017-2018 reporting period.

Due to staffing changes, the IGIS office did not conduct any inspections of ONA's access to and the use of AUSTRAC information.



ACTIVITY 3 RESPONDING TO COMPLAINTS

ABOUT COMPLAINTS

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

We categorise a matter as a 'complaint' if it raises an initially credible allegation of illegal or improper conduct or an abuse of human rights in relation to an action of an intelligence agency within the jurisdiction of the office. Complaints can be made orally or in writing.

Each communication is assessed to determine the most appropriate course of action and whether it falls within the Public Interest Disclosure (PID) scheme. Complaints are usually handled administratively in the first instance. In most cases, complaints and other matters can be resolved quickly and efficiently by our staff speaking to the relevant agency or reviewing their records. This approach can determine whether a particular matter is within jurisdiction and reduce the procedural burden of an inquiry. Administrative resolution usually gives the complainant a timely response, and information sought from agencies in this way can help the IGIS 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.234; *Corporate Plan 2016-20*.



QUANTITATIVE PERFORMANCE MEASURES

Figure 2.5: Timeliness of response to complaints

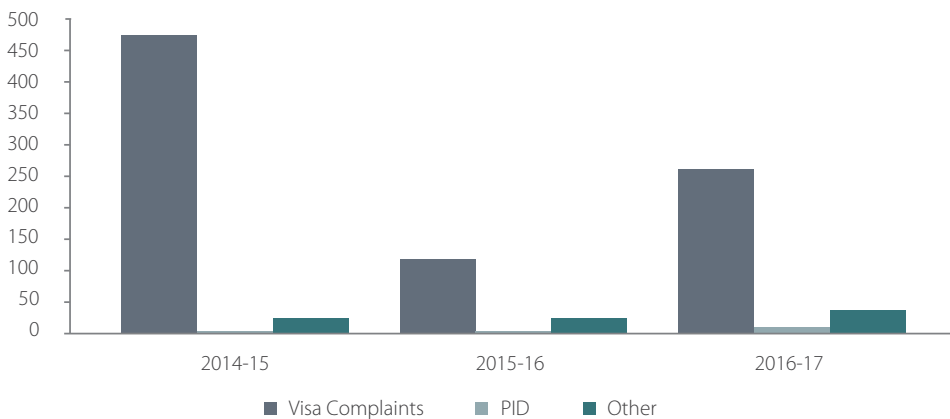
TOTAL COMPLAINTS – TIMELINESS			
Complaint type	Total number of complaints	Complaints acknowledged within five business days (TARGET: 90%)	Visa/citizenship-related complaints resolved within two weeks (TARGET: 85%)
Visa/citizenship-related	253	98%	87%
PID	11	75 %	N/A
Other	36	100 %	N/A
TOTAL	300	97%	87%

Figure 2.6: Public interest disclosures and complaints (not including visa/citizenship-related complaints) by agency and source

COMPLAINTS BY AGENCY AND SOURCE – NON VISA-RELATED			
Agency	Number of complaints*	From public	From intelligence agency employee or ex-employee
ASIO	34	30	4
ASIS	5	2	3
ASD	6	1	5
AGO	1	0	1
DIO	3	2	1
ONA	1	0	1

* A small number of complaints concerned more than one agency.

Figure 2.7: Complaint trends 2014-15 to 2016-17



COMPLAINTS ABOUT VISA AND CITIZENSHIP APPLICATIONS

The Department of Immigration and Border Protection (DIBP) 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 DIBP, ASIO may make a security assessment or provide advice in support of the visa process. The IGIS has the role of reviewing these actions to ensure they are legal and meet the required standard of propriety.

In 2016-17, the office received 253 visa or citizenship related complaints. In 2016-17 the average number of visa or citizenship-related complaints received per month was 21, compared to an average of 10 complaints per month in 2015-16.

As with previous years, the largest number of complaints made to the office came from individuals seeking skilled business or work visas (59 per cent). In 2016-17, there has been a reduction in the complaints relating to family reunion visas (from 20 per cent in 2015-16 to eight percent in 2016-17) and protection or refugee visas (from 21 percent to seven percent). The office also received a small number of complaints relating to security assessments for applications for Australian citizenship (five percent of security referral complaints). The most frequent complaint about visa or citizenship applications was the length of time taken to finalise an application beyond that listed on DIBP's website. Ordinarily the office will only take action on a complaint about a permanent visa where 12 months have passed since the visa application was lodged with DIBP; 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, 98 percent of visa and citizenship-related complaints related received by the office were acknowledged within five working days, well above our performance indicator of 90 percent. Of the visa and citizenship complaints received in 2016-17, 87 percent were resolved within 14 days of receipt. We consider a complaint about delay in visa or citizenship security assessments to be resolved once we have completed our administrative inquiries and responded to the complainant. On average, we resolved visa and citizenship -related complaints within 8 days. We resolved 87 per cent within two weeks, exceeding our target of 85 per cent.

The office routinely engages with DIPB to ensure relevant information has been received from Australian intelligence agencies. In 2016-17, the office has sought to increase engagement with the Commonwealth Ombudsman in relation to visa and citizenship complainants in relation to delays which are not within the jurisdiction of the office.

OTHER COMPLAINTS

We received 36 non visa/citizenship-related complaints in 2016-17 (excluding PID matters), some of which related to more than one agency. This is a 44% increase over the 25 we received in the previous reporting period. The majority of these complaints (31) were about ASIO. Three complaints were about ASIS, one concerned ASD, and one concerned ASIO, ASD and DIO.

The average time taken to acknowledge other complaints was 0.6 business days. We responded to 100% of complaints within five business days, surpassing our performance target of 90%.



Of the 36 complaints received, 34 were closed at the end of the reporting period, with an average of 20 days until a final response was sent.

All 36 of these complaints were investigated administratively. 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
- recruitment practices across the Australian intelligence community, including discrimination on the basis of age and race
- security assessments for employment
- passport cancellation
- surveillance.

All complainants were given advice about the action the office had taken in response to their complaints, noting 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 as a result of their complaints to the office. Three individuals who had complained were granted their employment-related security clearances following significant periods of delay. In one case, ASIO identified that processing errors had led to the delay in its assessment for an Aviation Security Identification Card (ASIC) and sent a written apology to the complainant. ASIO also introduced changes to some of its employment-related security assessment processing methods which are expected to improve processing times.

One complainant was provided advice and assurance by the office as to the safety of an individual overseas and the limits of ASIO's exchange of information with a foreign country. In another case, ASIO returned seized items to the complainant following their complaint to the office.

We do not measure complainant satisfaction, and few complainants contact the office to report either satisfaction or disappointment with the outcome of their complaints. In those instances where we are aware that an issue has remained unresolved when we close a complaint, we may monitor agencies' actions through our inspection program. In all cases, we provide advice about our role, and the role and functions of relevant Australian intelligence agencies. Where we do not address specific concerns, we provide details of suitable alternative avenues to pursue, if this is appropriate.

OTHER CONTACTS

We also received contacts from approximately 210 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 is a third less than the 325 contacts received in 2015-16.

When we are contacted about matters that we cannot pursue, we 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.



ALLEGATIONS OF DISCRIMINATION IN RECRUITMENT PRACTICES

An individual complained that the ASIS recruitment process was unreasonable in that it failed to give reasons why the applicant was unsuccessful and inappropriately took account of the applicant's racial background. IGIS reviewed the ASIS selection process and the individual's application and was satisfied that the recruitment decision was based on fair and reasonable grounds.

Similarly, another individual complained that ASIO's recruitment process was unreasonable, alleging that factors other than merit, such as the applicant's age, had been taken into account, and that no reasons were given for the applicant's lack of success. In this case, too, IGIS reviewed all relevant material and found no evidence of unreasonable or inappropriate decisions in ASIO's consideration of the application.

There are valid reasons why the intelligence agencies do not provide feedback to external applicants, ensuring that the agencies are protected from individuals seeking to gain access for the purpose of compromising Australia's security. IGIS's role is not to review the merits of agencies' employment decisions, but where questions arise such as these about discriminatory practices, IGIS will examine relevant aspects of agency records to consider the propriety of agency decision-making.

ALLEGATIONS OF INAPPROPRIATE COOPERATION WITH FOREIGN OFFICIALS

An individual contacted IGIS for assistance when a relative overseas was allegedly kidnapped by foreign officials and taken to an embassy. It was alleged that the relative's Australian passport was confiscated at the request of ASIO and another Australian agency for a terrorism-related reason, and that ASIO had put the relative at risk of torture by the foreign officials.

IGIS sought advice from ASIO on its role, if any, in this matter. IGIS was satisfied that ASIO had not acted in either an illegal or inappropriate manner. IGIS provided information to the complainant about the consular assistance being given to the complainant's relative, as well as about relevant protocols on ASIO's information exchange with foreign officials.

Further information about ASIO's exchange of information with foreign officials is on page 19 of this report.

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 IGIS human rights and discrimination matters relating to an act or practice of the intelligence and security agencies.

In 2016-17 the AHRC referred one case to the IGIS. As this matter had recently been the subject of IGIS investigation and IGIS had written to the complainant on that occasion, the IGIS wrote to the individual concerned to advise no further action was required.

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 relating to 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: *Corporate Plan 2016-2010*

QUANTITATIVE PERFORMANCE MEASURES

Figure 2.8: Timeliness of response to public interest disclosures

NUMBER OF PUBLIC INTEREST DISCLOSURES AND TIMELINESS OF RESPONSE TARGET: 90% ACKNOWLEDGED WITHIN 5 BUSINESS DAYS		
Total number of PID	Acknowledged within 5 business days	Average number of business days for acknowledgement
11	75%	6

Figure 2.9: Public interest disclosures by agency and source

COMPLAINTS BY AGENCY AND SOURCE – PUBLIC INTEREST DISCLOSURES			
Agency	Number of public interest disclosures*	From public	From intelligence agency employee or ex-employee**
ASIO	2	0	2
ASIS	2	0	2
ASD	5	1	4
AGO	1	0	1
DIO	2	1	1
ONA	1	0	1

*One disclosure concerned more than one agency (ASD, AGO and DIO) and did not meet the threshold for allocation

**Two anonymous disclosures were presumed to have been made by an intelligence agency employee or ex-employee



A former ASD contractor claimed that his security clearance was delayed after he made an internal complaint. The claim was considered to be a public interest disclosure and was referred by the IGIS to ASD to conduct an investigation into the claims.

ASD's investigation found no evidence of wrong conduct, finding that the discloser had contributed to the delay by failing to attend several appointments for an obligatory psychological assessment. ASD informed the IGIS of its finding and provided a copy of its investigation report. The agency also sent a copy of the report to the discloser, as required by section 51(4) of the *Public Interest Disclosure Act 2013*.

The discloser immediately contacted IGIS to dispute the agency's finding, saying he had only been told of one appointment for psychological assessment, which he attended. In response, IGIS asked the agency to re-examine the evidence. In conducting its second investigation, ASD discovered that typographical errors had existed in the discloser's contact details until an observant staff member noticed discrepancies and successfully made contact with the discloser to offer an appointment. Previous appointments for psychological assessment had been sent to an incorrect email address and were never received by the discloser.

ASD met with IGIS to discuss the circumstances of the case and propose options for resolving the issues identified through its investigation. ASD and IGIS developed an agreed course of action to address the identified issues. ASD sent a written apology to the discloser and explained the errors that had occurred in the first investigation. The agency also advised the discloser that he remained eligible for future work with ASD.

The discloser expressed appreciation for IGIS involvement in ensuring his concerns were properly considered, and was satisfied with ASD's explanation that the delay was due to error rather than a reprisal for his internal complaint.

IGIS'S HANDLING OF PUBLIC INTEREST DISCLOSURES

Key IGIS responsibilities under the PID scheme include:

- 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 eleven public interest disclosures handled during the reporting period, almost three times the number received in each of the two preceding reporting periods.

Most of the eleven public interest disclosures raised allegations of maladministration covering a range of issues, including staff recruitment and termination, allowances, the conduct of security clearances, and conduct relating to the withdrawal of security clearances. One disclosure related to conduct endangering health, namely systemic bullying, and another to the contravention of a law of the Commonwealth.

OVERSEEING THE OPERATION OF THE PID SCHEME IN THE INTELLIGENCE AGENCIES

In accordance with s 44(1A)(b) of the PID Act, the intelligence agencies are required to inform IGIS when a public interest disclosure is allocated for investigation by an intelligence agency, and meet other reporting obligations.

IGIS was informed of nine PIDs received by the intelligence agencies in the reporting period. Five of these were from ASD, and four from ASIO.

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



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: timeliness of advice provided to parliamentary committees and similar bodies

Target: written submissions provided by the date requested or agreed

Source: *Corporate Plan 2016-20*

All advice was provided by the agreed dates.

During the reporting period the IGIS appeared at five parliamentary committee hearings, and contributed to an independent review.

DISCUSSION

SENATE ESTIMATES HEARINGS

The Inspector-General appeared before the Senate Standing Committee on Finance and Public Administration on 17 October 2016 for Supplementary Budget Estimates, on 27 February 2017 during the 2016-17 Additional Estimates hearings and on 22 May 2017 for Budget Estimates.

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

The Inspector-General participated in two inquiries conducted by the Parliamentary Joint Committee on Intelligence and Security during 2016-17:

- Criminal Code Amendment (High Risk Terrorist Offenders) Bill 2016
- Review of ASIO's questioning and detention powers.

2017 INDEPENDENT INTELLIGENCE REVIEW

In November 2016 the Government announced an independent review of the Australian Intelligence Community. The Inspector-General contributed to the review by meeting with the review team on several occasions and making a submissions.





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) sets out various 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 IGIS. There are equivalent provisions in the *Archives Act 1983* for the AAT. The IGIS 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

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

Target: evidence provided by the date requested or agreed

Source: Portfolio Budget Statements 2016-17, p.234; *Corporate Plan 2016-20*

There were no quantitative performance measures identified in the *IGIS Corporate Plan 2016-20* that were directly applicable to the evidence we provided to the AAT and the Information Commissioner.

During the reporting period the Inspector-General was called on once by the Information Commissioner to give evidence in an FOI matter, and responded to one request carried over from the previous year. The IGIS was notified by the AAT of one new case where the IGIS may be requested to give evidence.

DISCUSSION

In the new case referred to the Inspector-General by the Information Commissioner, the IGIS decided after taking into account her functions under the IGIS Act that the matter fell outside of her area of expertise and, on that basis, declined to give evidence. In another case which was carried over from the previous year, the former Inspector-General provided evidence on one aspect of the claim being made by the Commonwealth.

Although the Inspector-General was notified by the AAT of one new case where the IGIS may be requested to give evidence, at the end of the reporting period the IGIS had not been called to give evidence in that case.

The number of cases referred to the IGIS 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 with the aim of increasing their awareness of their compliance responsibilities as well as increasing their understanding of the role of this office. In addition to discussions with agency heads and senior staff we have given presentations to new and current staff explaining the approach of this office to compliance issues illustrating this with reference to some of the more common problems we encounter. Our office also has a regular program of presentations to the broader intelligence community, and public groups with an interest in national security 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”; section 4(d), *Inspector-General of Intelligence and Security Act 1986*.

PERFORMANCE SUMMARY

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

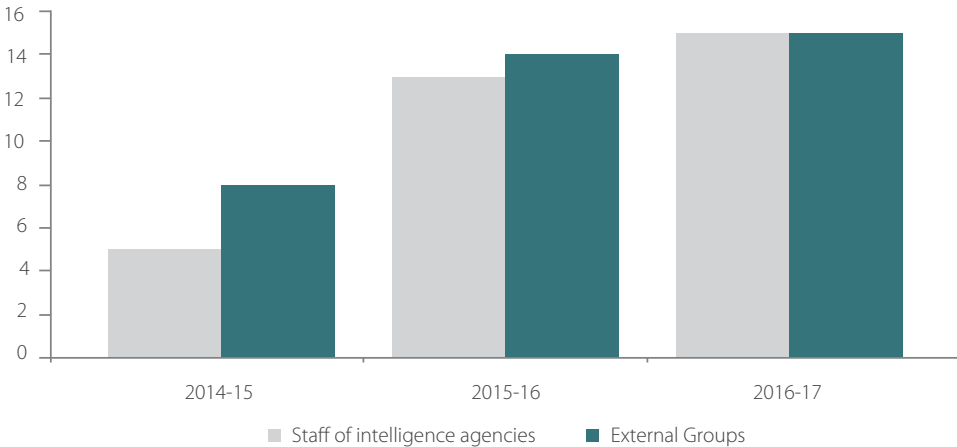
Raising awareness of the role and functions of the office outside the Australian intelligence agencies in order to increase public awareness of the scrutiny applied to the agencies.

Performance criteria: completion of at least nine outreach activities per year

Target: frequency of presentations and outreach. Meet all feasible requests.

Source: Portfolio Budget Statements, p.235; *Corporate Plan 2016-20*

Figure 2.10: Number of presentations by year and audience



PRESENTATIONS AND AGENCY ENGAGEMENT

In the reporting period, the office delivered 30 presentations, of which 15 were to members of the intelligence agencies, including in regional offices and other sites outside of Canberra; and 15 were to external groups. Over the last two reporting periods the office has increased the number of presentations as part of a deliberate strategy to extend our outreach.

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. 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 and explore any particular challenges they encounter. These may vary depending on the particular locations and operations at their post. These discussions enhance our understanding of each intelligence agency's operational environment and also provide a forum to resolve issues informally without the need for extended or time consuming correspondence.

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. We would like to express appreciation to our regular points of contact within each agency for assisting our work during the 2016-17 reporting period.

ENGAGEMENT WITH THE PUBLIC

In the reporting period, there were 15 presentations to groups external to the intelligence agencies. Presentations by the Inspector-General included a public lecture at the Australian Strategic Policy Institute, and presentations to the Australian National Security College, law firms and government departments. The Inspector-General and Deputy Inspector-General also provided guest lectures at the Australian National University.

It is intended to continue this program of presentations in the coming year.



ACTIVITY 8 LIAISING WITH OTHER ACCOUNTABILITY OR INTEGRITY AGENCIES

ABOUT LIAISING WITH OTHER ACCOUNTABILITY OR INTEGRITY AGENCIES

We frequently liaise with other accountability and integrity agencies, both in Australia and overseas. This liaison provides opportunities for us to discuss matters of mutual interest, learn from each other's practices and 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 Commonwealth Ombudsman and the Australian Human Rights Commission

Target: regular interactions as required

Source: *Corporate Plan 2016-20*

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 human rights and discrimination matters relating to an act or practice of the intelligence and security agencies to the IGIS. In the reporting period, our engagement with the AHRC included exchanges relating to complaint-handling practices.

Specific matters referred to the IGIS by the AHRC as complaints are discussed in detail in this report under Activity 3.

COMMONWEALTH OMBUDSMAN

The work of our 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 jurisdictions of each office. During 2016-17, we continued to hold regular face to face meetings at the Deputy IGIS/Deputy Ombudsman level. The purpose of these meetings was to ensure the coordination of our investigative activities, to reduce duplication of effort, and also to discuss issues of mutual interest including any legislative changes affecting integrity and oversight bodies.

The most frequent area of overlap between our respective offices continues to be in handling immigration and visa-related security assessment complaints. Where appropriate, our staff either refer matters directly to the OCO or advise the visa applicant that they may lodge a complaint with the OCO where the matter does not come within IGIS's jurisdiction. This includes, for example, cases 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 Immigration, for example, in cases where there has been prolonged delay by Immigration in processing certain visa applications.

This office also liaised closely with the OCO during 2016-17 on the management of the Commonwealth's Public Interest Disclosure Scheme. While the Commonwealth Ombudsman 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 is discussed at Activity 4 of this report.

INTERNATIONAL ENGAGEMENT

During the reporting period, the Inspector-General and/or Deputy Inspector-General met with officials from New Zealand, Canada and Japan on matters relating to intelligence and security. The office has also been engaged in discussions with international integrity agencies and the Five Eyes Intelligence Oversight and Security Review Council on matters of mutual interest.

SECTION THREE

MANAGEMENT AND ACCOUNTABILITY





PART 3.1

CORPORATE GOVERNANCE

The office has structures and processes in place to implement the principles and objectives of corporate governance.

ORGANISATIONAL STRUCTURE

The Inspector-General is supported by a Deputy, who has responsibility for legal and parliamentary matters, as well as finance and office management. In addition, a small number of Executive Level 2 officers share responsibility for the inspection programs, complaint-handling and projects.

Senior positions occupied during 2016–17 were as follows:

Inspector-General of Intelligence and Security (Statutory officer)

The Honourable Margaret Stone, appointed 24 August 2015

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

Mr Jake Blight

During the reporting period Mr Jake Blight acted as the Inspector-General pursuant to the Prime Minister's instrument of appointment.

Acting Assistant Inspector-General of Intelligence and Security

Ms Annette Willing

From 01 July 2016 – 10 February 2017, Ms Annette Willing acted as the Assistant Inspector-General of Intelligence and Security, under a non-Average Staffing Level affecting agreement.

During the reporting period Ms Willing acted as the Inspector-General pursuant to the Prime Minister's instrument of appointment.

SENIOR MANAGEMENT COMMITTEES

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

The functions of this committee are detailed under 'Internal Audit and Risk Management' on page 54.

CORPORATE AND OPERATIONAL PLANNING

OIGIS'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 s. 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 of 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 2017, we were fully compliant with all 36 mandatory requirements.

ETHICAL STANDARDS AND FRAUD CONTROL

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

The OIGIS has established and maintains appropriate systems of risk oversight, management and internal controls in accordance with section 16 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and the *Commonwealth Risk Management Policy*.

The Risk Management Plan includes controls 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. The Audit Committee is established and structured in accordance with section 45 of the PGPA Act and the PGPA Rules. It meets on a periodic basis to consider matters including risk management, internal control, financial reporting, compliance requirements, performance reporting and governance arrangements.

The office completes the Australian Institute of Criminology's annual *Fraud against the Commonwealth* survey. The 2015-16 response was submitted on 26 August 2016.

EMPLOYMENT OF SES OFFICERS

The office has one SES position filled by Mr Jake Blight. The terms and conditions of Mr Blight's employment, including salary, are set out in a Section 24(1) determination and are based broadly on SES remuneration within the Department of the Prime Minister and Cabinet.



EMPLOYMENT OF PERSONS FOR A PARTICULAR INQUIRY

Section 35(2AA) of the IGIS Act requires that the IGIS report on the employment under s. 32(3) of any person to perform functions and exercise powers for the purposes of a particular inquiry, and any delegation under s. 32AA to such a person. No person was employed under s. 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 (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 OIGIS interaction with parliamentary committees are available in the *Inspector-General's Review* on page vii.

DECISIONS BY THE JUDICIARY, TRIBUNALS OR THE INFORMATION COMMISSIONER

No judicial decisions or decisions of administrative tribunals or of the Information Commissioner made in 2016-17 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 2017, the office had 15 ongoing APS employees located in the Australian Capital Territory (not including the Inspector-General). Four 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 2017 (employment level and status)

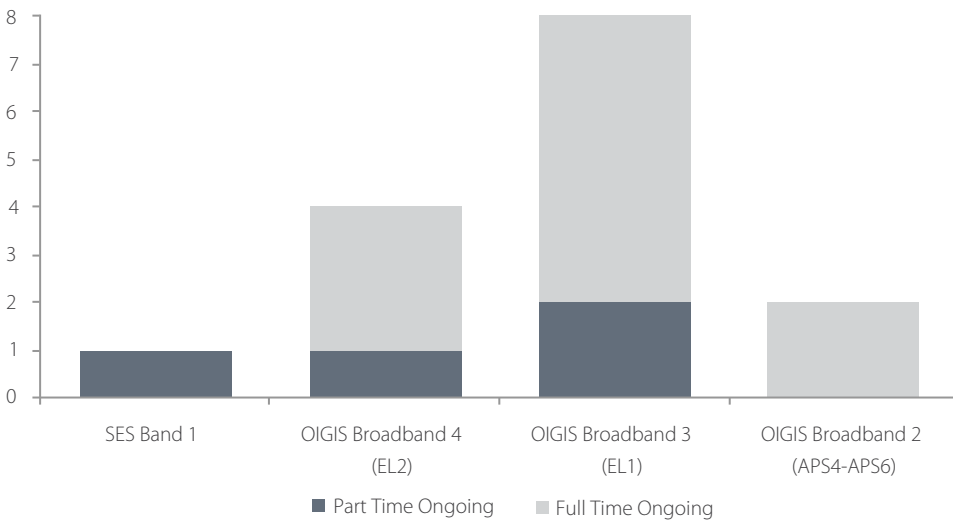
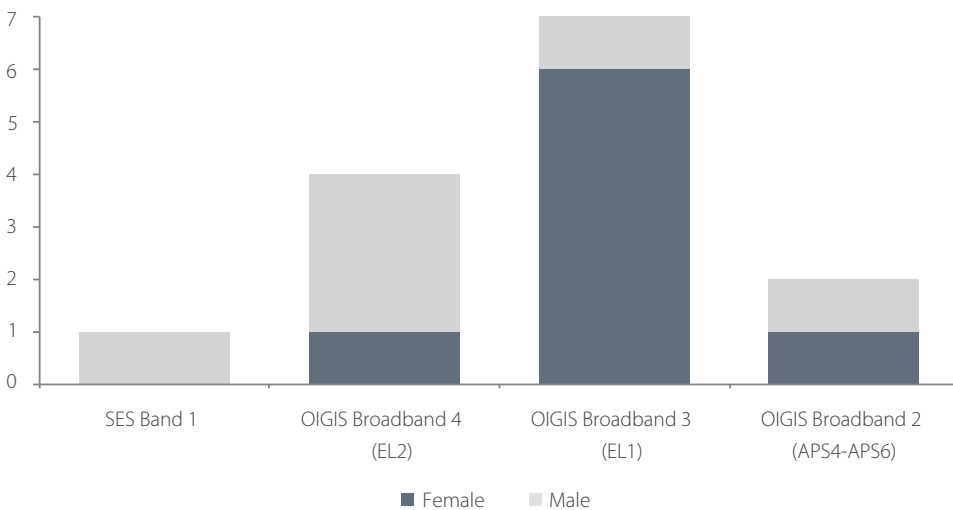


Figure 3.2: Gender Balance as at 30 June 2017 (by employment level)



Internal audit and risk management

The membership and functions of the Audit Committee are structured according to the PGPA Act. At 30 June 2017 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 (OIGIS). 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's 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.

EMPLOYMENT FRAMEWORKS

At 06 February 2017, all non-SES staff were employed under OIGIS Enterprise Agreement 2016-2019. One SES staff member was employed under a section 24(1) determination.

The salary range available to APS employees in OIGIS throughout 2016-17 is provided at Annex 5.2.

The only notable non-salary benefit for OIGIS 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 \$1093 per annum until 06 February 2017, when on commencement of the OIGIS Enterprise Agreement 2016-2019 it became \$1125.

TRAINING AND STAFF DEVELOPMENT

We continued the internal training program introduced in early 2012. The program of short training sessions, run once a fortnight, ensures that staff develop and maintain specialised knowledge and skills, and supplements on the job training. Topics covered in 2016–17 included:

- recent changes to legislation
- Parliamentary committees
- the Independent Reviewer of Adverse Security Assessments
- issue motivated groups
- the law of armed conflict
- performance management
- security awareness.

Staff were also provided with regular opportunities throughout 2016–17 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

OIGIS does not have a performance pay scheme.



PART 3.3

OTHER INFORMATION

PURCHASING

The agency 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/.

OIGIS 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

Total actual expenditure on consultancy contracts for 2016-17 was \$21 325.55 (GST inclusive). This represents six consultancy contracts for a range of services, including financial planning for staff members, and meeting national security accreditation requirements. This compares to no consultancies in 2015-16.

ANAO ACCESS CLAUSES

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

EXEMPT CONTRACTS

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

INFORMATION PUBLICATION SCHEME

Agencies subject to the Freedom of Information Act 1982 (FOI Act) are required to publish information to the public as part of the Information Publication Scheme (IPS). This requirement is in Part II of the FOI Act and has replaced the former requirement to publish a section 8 statement in an annual report. Each agency must display on its website a plan showing what information it publishes in accordance with the IPS requirements. As an exempt agency under the FOI Act, the scheme does not apply to OIGIS. Indexed file lists were published on OIGIS's website in the reporting period in accordance with the Senate Continuing Order No 10 (Harradine Order).

FREEDOM OF INFORMATION

This office is an exempt agency for the purposes of the *Freedom of Information Act 1982*.

DISABILITY REPORTING MECHANISM

Since 1994, Commonwealth departments and agencies have reported on their performance as 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 ten year national policy framework to improve the lives of people with disability, promote participation and create a more inclusive society. A high level two-yearly 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 2014, and can be found at www.dss.gov.au.



SECTION FOUR

FINANCIAL MANAGEMENT





PART 4.1

FINANCIAL SUMMARY

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

The office received an unqualified audit report from the Australian National Audit Office for its 2016-17 financial statements. A summary of our financial performance follows.

The office operated within available resources in 2016-17 and ended the year with a surplus of \$299 290.

Appropriation funding levels in 2016-17 remained steady with a slight increase reflecting changes in economic parameters. 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 budget variance related to employee expenses (\$267 000 underspend). This variance was largely due to delays in the lengthy security clearance process associated with recruitment. These delays also impacted on supplier expenses with security clearance fees \$36,000 below budget.

Net equity increased from \$2 831 350 in 2015-16 to \$3 161 158 in 2016-17. Movements in equity included a \$299 290 increase in retained surplus and a \$5,518 upward movement in the asset revaluation reserve. Contributed Equity also increased from \$503 126 in 2015-16 to \$528 126 in 2016-17. Movements in contributed equity included capital funding of \$25 000.

The following tables show:

Figure 4.1 – Agency Resource Statement and Resource for Outcomes 2016-17

Figure 4.2 – Expenses and Resources for Outcome 1.

OIGIS has one outcome and one program.

ENTITY RESOURCE STATEMENT AND RESOURCES FOR OUTCOMES 2016-17

Figure 4.1: Entity resource statement 2016-17

	ACTUAL AVAILABLE APPROPRIATION FOR 2016-17 \$'000 (A)	PAYMENTS MADE 2016-17 \$'000 (B)	BALANCE REMAINING 2016-17 \$'000 (A)-(B)
Ordinary Annual Services			
Departmental Appropriation			
Prior year departmental appropriation	3 468	2 706	762
Departmental appropriation	3 143	-	3 143
S74 Relevant Agency	121	-	121
Receipts			
Total	6 732	2 706	4 026
Administered expenses			
Total	-	-	-
Total ordinary annual services A	6 732	2 706	4 026
Other services			
Departmental non-operating	-	-	-
Total	-	-	-
Total other services B	-	-	-
Total available annual appropriations			
Special appropriations	-	-	-
Total special appropriations C	-	-	-
Special accounts	-	-	-
Total special accounts D	-	-	-
Total resourcing A + B + C + D	6 732	2 706	4 026
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	6 732	2 706	4 026

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 2016-17 \$'000	ACTUAL EXPENSES 2016-17 \$'000	VARIATION 2016-17 \$'000
	(A)	(B)	(A)-(B)

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

Departmental expenses

Departmental appropriation ¹	3 118	3 122	(4)
Special appropriations	-	-	-
Special Accounts	-	-	-
Expenses not requiring appropriation in the Budget year	140	172	(32)
Total for Program 1.1	3 258	3 294	(36)

Outcome 1 Totals by appropriation type

Departmental expenses

Departmental appropriation ¹	3 118	3 122	(4)
Special appropriations	-	-	-
Special Accounts	-	-	-
Expenses not requiring appropriation in the Budget year	140	172	(32)
Total expenses for Outcome 1	3 258	3 294	(36)

	Budget 2016-17	Actual 2016-17	
Average Staffing Level (number)	17	14	3

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 2016-17 included:

- A \$242 592 increase in employee expenses arising largely due to the impact of redundancy payments but also due to the effect of a pay increase which took effect from early 2017.
- A \$102 757 increase in supplier expenses. Increases in expenditure included \$5 213 in staff training expenses, \$44 981 in overseas travel expenses, \$19 448 in consultant expenses and a \$26 000 increase in resources received free of charge for office lease expenses.
- A \$11 694 increase in Property, Plant and Equipment following the purchase of office equipment and the effect of an increase in the fair values of assets following an independent valuation conducted by B & A Valuers at 30 June 2017.
- A \$263 226 increase in Other Payables largely due to outstanding redundancy payments and reimbursements to home agencies for seconded staff.
- A \$22 155 decrease in Employee Provisions due to staff turnover and the changing profile of the staff.

Figure 4.3: Trends in finance

		2016-17 OUTCOME 1 \$	2015-16 OUTCOME 1 \$	CHANGE FROM PREVIOUS YEAR
Revenue from Government		3 118 000	3 050 000	+2%
Other Income		157 705	128 625	+22%
Total income		3 275 705	3 178 625	
Employee expenses		2 590 442	2 347 850	+10%
Supplier expenses		365 906	263 149	+39%
Other expenses		20 067	15 062	+33%
Total expenses		2 976 415	2 626 061	
Operating result		299 290	552 564	
Financial assets	A	4 030 721	3 479 682	+15%
Non-financial assets	B	89 400	77 706	+15%
Liabilities	C	958 199	726 038	+31%
Net assets = A + B - C		3 161 158	2 831 350	



PART 4.2

FINANCIAL STATEMENTS



INDEPENDENT AUDITOR'S REPORT

To the Prime Minister

Opinion

In my opinion, the financial statements of the Office of the Inspector-General of Intelligence and Security for the year ended 30 June 2017:

- (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 2017 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 2017 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, comprising a Summary of Significant Accounting Policies and other explanatory information.

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* to the extent that they are not in conflict with the *Auditor-General Act 1997* (the Code). 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, disclosing matters related to going concern as applicable and using the going concern basis of accounting unless the Inspector-General of Intelligence and Security either intends to liquidate the entity or to cease operations, or has no realistic alternative but to do so.

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

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

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



Kristian Gage

Executive Director

Delegate of the Auditor-General

Canberra

20 September 2017

STATEMENT BY THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2017 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.



Mr Jake Blight
Acting Inspector-General of
Intelligence and Security

20 September 2017



OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY
STATEMENT OF COMPREHENSIVE INCOME
for the year ended 30 June 2017

	Notes	2017 \$	2016 \$	Original Budget \$
NET COST OF SERVICES				
Expenses				
Employee benefits	2A	2 590 442	2 347 850	2 857 000
Suppliers	2B	365 906	263 149	388 000
Depreciation	5	19 562	15 062	13 000
Write-down and impairment of asset		505	-	-
Total expenses		<u>2 976 415</u>	<u>2 626 061</u>	<u>3 258 000</u>
Own-Source Income				
Own-source revenue				
Other revenue	3A	157 705	128 625	-
Total own-source revenue		<u>157 705</u>	<u>128 625</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>157 705</u>	<u>128 625</u>	<u>127 000</u>
Net cost of services		<u>2 818 710</u>	<u>2 497 436</u>	<u>3 131 000</u>
Revenue from Government		<u>3 118 000</u>	<u>3 050 000</u>	<u>3 118 000</u>
Surplus /(deficit) after income tax on continuing operations		<u>299 290</u>	<u>552 564</u>	<u>(13 000)</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>304 808</u>	<u>552 564</u>	<u>(13 000)</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 2017

	Notes	2017 \$	2016 \$	Original Budget \$
ASSETS				
Financial Assets				
Cash and cash equivalents		200 498	154 879	175 000
Trade and other receivables	4	3 830 223	3 324 803	3 023 000
Total financial assets		<u>4 030 721</u>	<u>3 479 682</u>	<u>3 198 000</u>
Non-Financial Assets				
Property, plant and equipment	5	89 400	77 706	121 000
Total non-financial assets		<u>89 400</u>	<u>77 706</u>	<u>121 000</u>
Total Assets		<u>4 120 121</u>	<u>3 557 388</u>	<u>3 319 000</u>
LIABILITIES				
Payables				
Suppliers	6A	13 198	21 344	-
Other payables	6B	370 703	107 477	149 000
Total payables		<u>383 901</u>	<u>128 821</u>	<u>149 000</u>
Provisions				
Employee provisions	7	575 062	597 217	866 000
Total provisions		<u>575 062</u>	<u>597 217</u>	<u>866 000</u>
Total Liabilities		<u>958 963</u>	<u>726 038</u>	<u>1 015 000</u>
Net Assets		<u>3 161 158</u>	<u>2 831 350</u>	<u>2 304 000</u>
EQUITY				
Contributed equity		528 126	503 126	528 000
Reserves		21 623	16 105	16 000
Retained surplus		2 611 409	2 312 119	1 760 000
Total Equity		<u>3 161 158</u>	<u>2 831 350</u>	<u>2 304 000</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 2017

	2017 \$	2016 \$	Original Budget \$
CONTRIBUTED EQUITY			
Opening balance as at 1 July	503 126	478 126	503 000
Transactions with Owners			
Contributions by Owners			
Departmental Capital Budget	25 000	25 000	25 000
Total Transactions with Owners	25 000	25 000	25 000
Closing balance as at 30 June	528 126	503 126	528 000
RETAINED EARNINGS			
Opening balance as at 1 July			
Balance carried forward from previous period	2 312 119	1 759 555	1 773 000
Comprehensive Income			
Surplus/deficit for the period	299 290	552 564	(13 000)
Total comprehensive income	299 290	552 564	(13 000)
Closing balance as at 30 June	2 611 409	2 312 119	1 760 000
ASSET REVALUATION RESERVE			
Opening balance as at 1 July			
Balance carried forward from previous period	16 105	16 105	16 000
Comprehensive Income			
Other Comprehensive Income	5 518	-	-
Total comprehensive income	5 518	-	-
Closing balance as at 30 June	21 623	16 105	16 000
TOTAL EQUITY			
Opening balance			
Balance carried forward from previous period	2 831 350	2 253 786	2 292 000
Comprehensive Income			
Surplus/deficit for the period	299 290	552 564	(13 000)
Other comprehensive income	5 518	-	-
Total comprehensive income	304 808	552 564	(13 000)
Transactions with Owners			
Contributions by Owners			
Departmental Capital Budget	25 000	25 000	25 000
Total Transactions with Owners	25 000	25 000	25 000
Closing balance as at 30 June	3 161 158	2 831 350	2 304 000

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 2017

	Notes	2017 \$	2016 \$	Original Budget \$
OPERATING ACTIVITIES				
Cash received				
Appropriations		2,743 480	2 867 103	2 975 000
Net GST received		7 600	14 329	-
Other cash received		113 705	187 214	-
Total cash received		2 864 785	3 068 646	2 975 000
Cash used				
Employees		(2 412 936)	(2 279 195)	(2 831 000)
Suppliers		(291 283)	(641 163)	(118 000)
Section 74 receipts transferred to OPA		(113 705)	(185 044)	-
Total cash used		(2 817 924)	(3 105 402)	(2 949 000)
Net cash from/(used by) operating activities		46 861	(36 756)	26 000
INVESTING ACTIVITIES				
Cash used				
Purchase of property, plant and equipment		(26 242)	(49 094)	(51 000)
Total cash used		(26 242)	(49 094)	(51 000)
Net cash from/(used by) investing activities		(26 242)	(49 094)	(25 000)
FINANCING ACTIVITIES				
Cash received				
Contributed equity		25 000	65 915	25 000
Total cash received		25 000	65 915	25 000
Net cash from financing activities		25 000	65 915	25 000
Net increase/(decrease) in cash held		45 619	(19 935)	-
Cash and cash equivalents at the beginning of the reporting period		154 879	174 814	175 000
Cash and cash equivalents at the end of the reporting period		200 498	154 879	175 000

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

Major Budget Variances for 2017

The following table provides high level commentary of major variances between budgeted information for the OIGIS published in the 2016-17 Portfolio Budget Statements (PBS) and the 2016-17 final outcome as presented in accordance with Australian Accounting Standards for the OIGIS. Adjustments to the original PBS budget during the year included a reallocation between employee benefits and supplier expenses. 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)
Other Revenue – approximately \$157,000 above budget which was offset by Gains – Resources Received Free of Charge which was \$127,000 below budget following a reclassification. The increase related to a change in the assessed value of resources received free of charge from DPM&C for office space. The matching expense also increased so overall no result on the retained surplus.	Impacted: Statement of Comprehensive Income: Other Revenue Supplier expenses
Employee Benefits – \$267,000 underspent on original budget mainly due to recruitment delays associated with the lengthy security clearance process. Other Payables – approximately \$220,000 above budget. The most significant variance relates to an accrued redundancy payment not anticipated at original budget.	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 – \$22,000 underspent compared to the original budget and \$135,000 underspent compared to the revised budget. The most significant variances related to delays in the security clearance process and the delayed implementation of Portfolio wide shared service arrangements. 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 \$25,000 below budget due to changes in the scheduled replacement of existing assets and the need to prioritise office fitout changes to accommodate IT infrastructure upgrades.	Impacted: Statement of Comprehensive Income: Depreciation Statement of Financial Position: Property, plant and equipment Appropriations receivable Cashflow Statement: Cash used - investing activities
Other Cash Received – \$113,000 above budget. The variance relates to leave liabilities transfers for new starters which are not budgeted for.	Impacted: Statement of Financial Position: Cash and cash equivalents Appropriations receivable Cashflow Statement: Cash received - operating activities

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) for reporting periods ending on or after 1 July 2015; and
- Australian Accounting Standards and Interpretations – Reduced Disclosure Requirements issued by the Australian Accounting Standards Board (AASB) that apply for the reporting period.

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

The financial statements are presented in Australian dollars and values are rounded to the nearest dollar.

1.2 Significant Accounting Judgments and Estimates

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

1.3 New Australian Accounting Standards

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

1.4 Taxation

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

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

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

1.5 Revenue from Government

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

1.6 Events after the Reporting Period

There was no subsequent event that had the potential to significantly affect the ongoing structure and financial activities of OIGIS.



NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2017

Note 2 – Expenses

	2017 \$	2016 \$
<u>Note 2A – Employee Benefits</u>		
Wages and salaries	1 897 944	1 547 700
Superannuation:		
Defined benefit plans	119 336	136 643
Defined contribution plans	210 021	173 166
Leave and other entitlements	195 960	490 341
Separations and redundancies	167 181	-
Total employee benefits	2 590 442	2 347 850

Accounting Policy

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

	2017 \$	2016 \$
<u>Note 2B – Suppliers</u>		
Goods and services supplied or rendered		
Consultants	19 448	-
ICT support	46 000	46 000
Legal expenses	5 702	-
Printing non publications	8 022	9 483
Resources received free of charge:		
Notional Rent Charge	128 000	102 000
Notional Audit Fees	21 000	18 000
Notional IT Support Costs	4 545	4 545
Stationery	9 158	13 932
Training	18 899	13 868
Travel	14 222	9 200
Overseas Travel	44 981	-
Security Vetting Expenses	6 380	10 482
Other	17 523	15 584
Total goods and services supplied or rendered	343 880	243 094
Other suppliers		
Motor Vehicle Lease – minimum lease payments	15 863	14 675
Workers compensation premiums	6 163	5 380
Total other supplier	22 026	20 055
Total supplier	365 906	263 149

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2017

Leasing Commitments

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

	2017 \$	2016 \$
Within 1 year	11 134	11 134
Between 1 to 5 years	1 856	12 990
Total operating lease commitments	12 990	24 124

Note 3 – Own-Source Revenue

	2017 \$	2016 \$
<u>Note 3A – Other Revenue</u>		
Employee FBT Contributions	3 880	3 966
Other	280	114
Resources Received Free of Charge:		
Department of the Prime Minister & Cabinet	128 000	102 000
Australian National Audit Office	21 000	18 000
Australian Signals Directorate	4 545	4 545
Total other own-source revenue	157 705	128 625

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 2016-17 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

	2017 \$	2016 \$
<u>Trade and other receivables</u>		
Appropriations receivable	3 827 406	3 314 181
GST receivable from the Australian Taxation Office	2 817	176
Other receivables	-	10 446
Total trade and other receivables (net)	3 830 223	3 324 803

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 2017

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 2017. 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 2016	
Gross book value	120 685
Accumulated depreciation and impairment	(42 979)
Total as at 1 July 2016	77 706
Additions	
by purchase	26 242
Depreciation expense	(19 562)
Disposals	-
Revaluations and impairments	5 014
Total as at 30 June 2017	89 400
Total as at 30 June 2017 represented by:	
Gross book value	89 400
Accumulated depreciation and impairment	-
Total as at 30 June 2017	89 400

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 2017 included \$61,400 Level 2 assets (including office equipment and furniture) and \$28,000 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 2017

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 2017. 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 (2016: 1 – 14 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

	2017 \$	2016 \$
6A - Suppliers		
Trade creditors and accruals	13 198	21 344
Total suppliers	13 198	21 344

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 2017

	2017 \$	2016 \$
6B - Other Payables		
Salaries and wages	16 681	5 142
Superannuation	2 211	873
Leave liability transfers payable	-	44 119
Salary reimbursements for seconded officers	47 564	53 582
Redundancy payment	301 740	-
Other	2 507	3 761
Total other payables	370 703	107 477

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

	2017 \$	2016 \$
<u>Employee Provisions</u>		
Leave	575 062	597 217
Total employee provisions	575 062	597 217

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 2017

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 and the Deputy Chief Executive. Key management personnel remuneration is reported in the table below:

	2017 \$	2016 \$
Short-term employee benefits:		
Salary	615 485	626 182
Annual leave ¹	-	2 983
Allowances	41 752	43 775
Total short-term employee benefits	657 237	672 940
Post-employment benefits:		
Superannuation	106 719	94 626
Total post-employment benefits	106 719	94 626
Other long-term employee benefits:		
Annual Leave	47 792	43 850
Long Service Leave	6 582	9 171
Total other long-term employee benefits	54 374	53 021
Total senior executive remuneration expenses	818 330	820 587

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 (2016: 4 individuals). The 2017 figure includes two of the officers for part of the year.

1 Annual Leave expected to be taken within 12 months.

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;

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2017

- the members of the Executive – key management personnel for the whole of government financial statements; and
- other Australian Government entities.

Transactions with Related Parties

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

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 \$128,000 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 2017 (2016: Nil).

Note 11 – Financial Instruments

	2017 \$	2016 \$
<u>Categories of Financial Instruments</u>		
Financial Assets		
Loans and Receivables		
Loans and receivables		
Cash and cash equivalents	200 498	154 879
Trade and other receivables	-	10 446
Total financial assets	<u>200 498</u>	<u>165 325</u>
Financial Liabilities		
At amortised cost		
Suppliers	13 198	21 344
Total financial liabilities	<u>13 198</u>	<u>21 344</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.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2017

Credit terms are net 30 days (2015–16: 30 days).

Financial Liabilities

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

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

Settlement is usually made net 30 days.

Note 12 – Appropriations

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

	2017 \$	2016 \$
Ordinary Annual Services		
Annual Appropriation	3 118 000	3 050 000
PGPA Act – Section 74 Receipts	113 705	185 044
Annual Departmental Capital Budget ¹	25 000	25 000
Total appropriation	3 256 705	3 260 044
Appropriation applied (current and prior years)	2 743 480	2 933 018
Variance²	513 225	327 026

- 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 to section 74 receipts and recruitment delays associated with security clearance requirements.

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

	2017 \$	2016 \$
Departmental		
Appropriation Act (No 1) 2013-14 – DCB	2 843	3 085
Appropriation Act (No 3) 2014-15	-	241 040
Appropriation Act (No 1) 2014-15 – DCB	-	26 000
Appropriation Act (No 1) 2015-16	541 858	3 018 055
Appropriation Act (No 1) 2015-16 – DCB	25 000	25 000
Appropriation Act (No 1) 2016-17	1 913 825	-
Supply Act 1 2016-17	1 317 879	-
Appropriation Act (No 1) 2016-17 – DCB	14 000	-
Supply Act 1 2016-17 – DCB	11 000	-
Cash	200 498	154 879
Total Departmental	4 026 903	3 468 059

SECTION FIVE

ANNEXURES



ANNEXURE 5.1

PERFORMANCE CRITERIA MAP

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.					
PBS 2016-17	Corporate Plan 2016-20 <i>Key Activities</i>	PBS 2016-17 <i>Key Performance criteria</i>	Corporate Plan 2016-20 <i>Key Performance Indicators</i>	Targets	Corporate Plan 2016-20 <i>Other Performance Measures</i>
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)		Timeliness of completion of inquiries			Number of inquiries conducted
		Level of acceptance by intelligence agencies of findings and recommendations of inquiries conducted		Duration of each inquiry completed	Duration of each inquiry completed
		Extent to which there has been change within the intelligence agencies as a result of activities of OIGIS		100% of inquiry recommendations implemented	
Undertaking comprehensive inspection and visit programs to monitor and review intelligence agencies' operational activity		Range of inspection work undertaken		Inspection of at least 75% of each agency's activity categories	
Providing effective and timely responses to complaints or referrals received from members of the public, Ministers or members of parliament		Timeliness of complaint resolution		90% acknowledged within five business days, and 85% of visa-related complaints resolved within two weeks	Number of complaints received and handled
					Number of 'contacts' that do not meet the criteria for complaints

Facilitating the investigation of public interest disclosures relating to intelligence agencies and undertaking other responsibilities under the PID Act	Timeliness of our response to public interest disclosures	90% of public interest disclosures acknowledged within 5 business days	Number of public interest disclosure matters handled
Providing information/advice to parliamentary committees and others on oversight issues relating to intelligence agency powers and functions	Timeliness of advice provided to parliamentary committees and similar bodies	Written submissions provided by the date requested or agreed	Number of appearances at hearings of parliamentary committees and similar bodies
Providing evidence to the AAT and the Information Commissioner as required under relevant legislation	Timeliness of evidence provided to the AAT and Information Commissioner	Evidence provided by the date requested or agreed	Number of instances where IGIS evidence is provided to the AAT or IC
Undertaking presentations to new and existing employees of intelligence agencies to ensure an awareness and understanding of their responsibilities and accountability	Frequency of presentations to staff in intelligence agencies	Completion of at least 9 outreach activities per year	Number of presentations and outreach activities
Raising awareness of the role and functions of the Office outside the Australian intelligence agencies to increase public awareness of the scrutiny applied to those agencies	Frequency of outreach activities delivered to audiences outside the intelligence community	Meet all feasible requests	Avail ourselves of all reasonable opportunities
Liaising with other accountability and integrity agencies on issues of mutual interest	Frequency of interactions with other accountability and integrity agencies, including Commonwealth Ombudsman and Australian Human Rights Commission	Regular interactions as required	





ANNEXURE 5.2

OIGIS SALARY SCALE

OIGIS BAND	APS LEVEL	SALARY RANGE 1 JULY 2016 – 30 JUNE 2017 (\$)
OIGIS Band 4	EL2	112,564 – 137,986
OIGIS Band 3	EL1	96,710 – 111,044
OIGIS Band 2	APS 6	80,063 - 92,672
	APS 5	70,155 - 78,384
	APS 4	63,021 - 70,626
OIGIS Band 1	APS 3	56,680 - 62,869
	APS 2	49,543 - 56,745
	APS 1	45,138 - 49,806



ANNEXURE 5.3

OTHER MANDATORY INFORMATION

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

WORK HEALTH AND SAFETY

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

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 IGIS 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 *Work Health and Safety Act 2011* (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*.

OIGIS 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 OIGIS 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 IGIS 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 per cent of the office's photocopying, facsimile reports and document printing in 2016–17
- printers are configured to print double-sided by default
- all unclassified office paper and cardboard waste is recycled
- empty toner cartridges are recycled, except where security considerations apply.



ANNEXURE 5.4

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	iii
17AD(h)	Aids to access			
17AJ(a)	Prelim	Table of contents	Mandatory	iv-v
17AJ(b)	Annex	Alphabetical index	Mandatory	98
17AJ(c)	Annex	Glossary of abbreviations and acronyms	Mandatory	97
17AJ(d)	Annex	List of requirements	Mandatory	89
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	vii
17AD(b)	Overview of the entity			
17AE(1)(a)(i)	Section 1	A description of the role and functions of the entity	Mandatory	2
17AE(1)(a)(ii)	Section 3	A description of the organisational structure of the entity	Mandatory	53
17AE(1)(a)(iii)	Section 1	A description of the outcomes and programs administered by the entity	Mandatory	3
17AE(1)(a)(iv)	Section 1	A description of the purposes of the entity as included in corporate plan	Mandatory	3



PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
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	7
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	60
17AF(1)(b)	Section 4	A table summarising the total resources and total payments of the entity	Mandatory	61
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	63
17AD(d)	Management and Accountability			
	<i>Corporate Governance</i>			
17AG(2)(a)	Section 3	Information on compliance with section 10 (fraud systems)	Mandatory	51



PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
17AG(2)(b)(i)	Prelim	A certification by accountable authority that fraud risk assessments and fraud control plans have been prepared	Mandatory	iii
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	iii
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	iii
17AG(2)(c)	Section 3	An outline of structures and processes in place for the entity to implement principles and objectives of corporate governance	Mandatory	51
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	52
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	52
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

PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
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	55
17AG(4)(b)	Section 3	Statistics on the entity's APS employees on an ongoing and non-ongoing basis; including the following: 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	53
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	54
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	54
17AG(4)(c)(ii)	Annex	The salary ranges available for APS employees by classification level	Mandatory	86
17AG(4)(c)(iii)	Section 3	A description of non-salary benefits provided to employees	Mandatory	54
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

PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
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)	N/A	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)		An assessment of entity performance against the <i>Commonwealth Procurement Rules</i>	Mandatory	56
<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; 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	56
17AG(7)(b)	Section 3	A statement that "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]"	Mandatory	56



PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
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	56
17AG(7)(d)	Section 3	A statement that "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"	Mandatory	56
<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
<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



PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
<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	56
17AG(10)(b)	Section 3	An outline of the ways in which the procurement practices of the entity support small and medium enterprises	Mandatory	56
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	64
17AD(f)	Other Mandatory Information			
17AH(1)(a)(i)	N/A	If the entity conducted advertising campaigns, a statement that “During [reporting period], the [name of entity] conducted the following advertising campaigns: [name of advertising campaigns undertaken]. Further information on those advertising campaigns is available at [address of entity’s website] and in the reports on Australian Government advertising prepared by the Department of Finance. Those reports are available on the Department of Finance’s website.”	If applicable, Mandatory	N/A
17AH(1)(a)(ii)	Annex	If the entity did not conduct advertising campaigns, a statement to that effect	If applicable, Mandatory	87

PGPA RULE REFERENCE	PART OF REPORT	DESCRIPTION	REQUIREMENT	PAGE
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	57
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	56
17AH(1)(e)	N/A	Correction of material errors in previous annual report	If applicable, Mandatory	N/A
17AH(2)	Annex	Information required by other legislation	Mandatory	87



ANNEXURE 5.5

GLOSSARY OF ABBREVIATIONS

AAT	Administrative Appeals Tribunal
AGO	Australian Geospatial-intelligence Organisation
AHRC	Australian Human Rights Commission
AIC	Australian intelligence community
ASD	Australian Signals Directorate
ASIC	Aviation security identification card
AML/CTF Act	<i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i>
APS	Australian Public Service
ASIO	Australian Security Intelligence Organisation
ASIO Act	<i>Australian Security Intelligence Organisation Act 1979</i>
ASIS	Australian Secret Intelligence Service
AUSTRAC	Australian Transaction Reports and Analysis Centre
DFAT	Department of Foreign Affairs and Trade
DIO	Defence Intelligence Organisation
FIC	Foreign intelligence collection
FOI	Freedom of information
FOI Act	<i>Freedom of Information Act 1982</i>
ICCPR	International Covenant on Civil and Political Rights
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
OIGIS	Office of the Inspector-General of Intelligence and Security
ONA	Office of National Assessments
ONA Act	<i>Office of National Assessments Act 1977</i>
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>
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PM&C	Department of the Prime Minister and Cabinet
SES	Senior Executive Service
TIA Act	<i>Telecommunications (Interception and Access) Act 1979</i>
WHS Act	<i>Work Health and Safety Act 2011</i>

INDEX

2017 Independent Intelligence Review, vii, viii, 43

A

abbreviations, 99

Acting Assistant Inspector-General of Intelligence and Security, 50

Activity performance *see under* performance

address and contact details, *inside front cover*

Administrative Appeals Tribunal, 3, 44

administrative tribunal decisions (external scrutiny), 52

advertising and market research, 89

agency capability reviews, 52

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

analytic independence (DIO), 11, 32

analytic independence (ONA), 11, 32

analytic tradecraft, 15

ANAO *see* Australian National Audit Office

annual performance statement, 8

annual report availability, *inside front cover*

Anti-Money Laundering and Counter Terrorism Financing Act 2006, 33

Archives Act 1983, 3

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, 50

assumed identities, 33

Attorney-General, 4, 19

Attorney-General's Guidelines under ASIO Act, 21

Audit Committee, 50, 51, 54

Auditor-General *see* Australian National Audit Office

audits

 ANAO report on financial statements, 52

 internal audit, 54

AusTender, 56

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

Australian Citizenship Act 2007, 21

Australian citizenship, cessation of, 21 *see also* Australian persons

Australian Criminal Intelligence Commission, viii, 18

Australian Federal Police, viii, 18

Australian Geospatial-Intelligence Organisation (AGO)

- AUSTRAC information access and use, 34
- complaints, 36
- Director's approvals and reports, 31
- inspections of, 30–2
- intelligence on Australian persons, 31
- Ministerial authorisations, 31
- privacy rules compliance, viii, 31
- public interest disclosures, 40
- role and functions, 5

Australian Human Rights Commission, 39, 47

Australian Information Commissioner, 3, 44, 52

Australian Intelligence Community *see* intelligence agencies

Australian National Audit Office, 2

- access clauses in contracts, 56
- audit report, 52

Australian persons

- definition in ISA, viii
- intelligence collection on, 23, 24, 25–6, 28, 29, 31, 32
- presumption of nationality, 23, 26
- risk to, 19
- see also* privacy rules compliance

Australian Secret Intelligence Service (ASIS)

- assumed identities, 33
- AUSTRAC information access and use, 33–4
- complaints, 36, 37, 39
- cooperation with foreign liaisons, 24
- inspections of, 14, 24–7
- intelligence on Australian persons, 24, 25–6
- Ministerial authorisations, 24–5
- presumption of nationality, 26
- privacy rules compliance, viii, 26
- public interest disclosures, 40
- review of operational files, 26
- role and functions, 4
- weapons use and issues, 27



Australian Security Intelligence Organisation (ASIO)

- analytic tradecraft, 15
- assumed identities, 33
- Attorney-General's Guidelines, 21
- AUSTRAC information access and use, 34
- complaints, 36, 37, 38, 39
- foreign liaisons information exchange, 19, 39
- human source management, 15
- information exchange, 18, 19
- inspections of, 14–22
- investigative activities, 15
- journalist information warrants, 17
- Ministerial submissions, 19, 20
- online investigative activities, 21
- protection of complainant information, 22
- public interest disclosures, 40, 42
- questioning and detention warrants, 17
- role and functions, 4, 14
- security assessments, 19, 20
- Special Intelligence Operations, 18
- surveillance devices, 21
- taxation information access, 19
- telecommunications data and interception warrants, 16–18, 22
- use of force, 17
- warrants, 16–17

Australian Security Intelligence Organisation Act 1979, 4, 13

- Attorney-General's Guidelines, 21
- breaches of, 16, 20
- foreign liaison, 19, 39

Australian Signals Directorate (ASD), vii

- AUSTRAC information access and use, 34
- complaints, 36, 37
- compliance incident reports, 29–30
- cyber activities, 30
- inquiries relating to, vii, 12
- inspections of, 27–30
- intelligence on Australian persons, 28
- Ministerial authorisations, 28
- presumption of nationality, 29

- privacy rules compliance, viii, 29
- public interest disclosures, 40, 41, 42
- role and functions, 5
- telecommunications interception, 28

Australian Transaction Reports and Analysis Centre (AUSTRAC), viii, 32, 33–4

Australians *see* Australian persons

B

Blight, Jake, 50, 51

C

citizenship, cessation of, 21 *see also* Australian persons

citizenship-related complaints, 36, 37

coercive powers, 9

Commonwealth Disability Strategy, 57

Commonwealth Electoral Act 1918 reporting requirements, 87

Commonwealth Indigenous Procurement Policy, 56

Commonwealth Ombudsman, 37, 42, 47–8, 52

Commonwealth Procurement Rules, 56

Commonwealth Risk Management Policy, 51

community, OIGIS engagement with, vii, 45–6

complaints handling

- ‘contacts’ versus ‘complaints’, 35
- employment-related delay complaints, 38
- IGIS function and powers, vii, 2, 35
- non-visa related, 36, 37–8
- other contacts with the office, 38
- performance summary, 35–6
- protecting complainant information, 22
- recruitment complaints, 38, 39
- statistics, 36
- timeliness, 36, 37
- visa security assessment related, 36, 37
- see also* inquiries

consultants, 56

contact details, *inside front cover*

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

contracts, 56

- corporate and operational planning, 50–1, 54
 - corporate plan, 3, 13
 - risk management plan, 51, 54
- corporate governance, 50–2
- Crimes Act 1914*, 33
- cross-agency inspections, 33–4 *see also* inspections
- cyber activities (ASD), 30

D

- Defence Imagery and Geospatial Organisation (DIGO) *see* Australian Geospatial-Intelligence Organisation (AGO)
- Defence intelligence agencies, 5
- Defence Intelligence Organisation (DIO)
 - AUSTRAC information access and use, 32, 34
 - complaints, 36, 37
 - inquiries relating to, vii, 11, 32
 - inspections of, 32
 - privacy guidelines compliance, 32
 - public interest disclosures, 40
 - role and functions, 5
- Defence Signals Directorate (DSD) *see* Australian Signals Directorate (ASD)
- Department of Defence, 5
 - First Principles Review*, 32
 - see also* Minister for Defence
- Department of Immigration and Border Protection, viii, 18, 37
- Department of the Prime Minister and Cabinet, 51, 87–88
- Deputy Inspector-General of Intelligence and Security, 50, 51
- detention warrants *see* questioning and detention warrants
- DIO *see* Defence Intelligence Organisation (DIO)
- disability reporting, 57
- dual citizenship, 21

E

- ecologically sustainable development, 87–88
- emergency authorisations, 24–5, 28
- employment frameworks, 54

enterprise agreements, 54
entity resource statement and resources for outcome, 61–2
environmental performance, 87–88
ethical standards, 51
exchange of information
 between Australian agencies, 18
 with foreign liaisons, 19, 24, 39
exempt contracts, 56
expert evidence, 3

F

financial intelligence information, 33–4
financial performance summary, 60–3
financial statements, 52, 64–83
firearms *see* weapons use and issues
Five Eyes countries Intelligence Oversight and Review Council, vii, 48
force, use of, 16, 17
foreign liaisons, 19, 24, 39
fraud control, iii, 51
Freedom of information Act 1982, 3
 exempt documents, 44
 OIGIS as exempt agency, 56, 57
functions *see* roles and functions

G

general public, OIGIS engagement with, vii, 45–6
geospatial intelligence agency *see* Australian Geospatial-Intelligence Organisation (AGO)
glossary, 99
government agencies, liaison with, 47–8
Guidelines to Protect the Privacy of Australian Persons, 32

H

human resources management, 53–5 *see also* staff
human rights and discrimination matters, 39 *see also* Australian Human Rights Commission
human source operations, 4, 15, 26



- identities, assumed, 33
- imagery intelligence *see* Australian Geospatial-Intelligence Organisation (AGO)
- Independent Intelligence Review 2017*, vii, viii, 43
- Indigenous businesses, 56
- Information Commissioner *see* Australian Information Commissioner
- Information Publication Scheme, 56
- information security authority *see* Australian Signals Directorate (ASD)
- inquiries, vii
 - acceptance of recommendations by agencies, 12
 - employment of persons for a particular inquiry, 52
 - IGIS function and powers, 2
 - performance discussion, 9–13
 - statistics, 10
 - timeliness, 11
- inquiries by parliamentary committees *see* parliamentary committees
- inspections, vii–viii
 - AGO activities, 14, 30–2
 - ASD activities, 14, 27–30
 - ASIO activities, 14–22
 - ASIS activities, 14, 24–7
 - AUSTRAC access and use, 33–4
 - cross-agency inspections, 33–4
 - DIO activities, 14, 32
 - IGIS function and powers, 2, 13
 - ONA activities, 14, 32
 - performance summary, 13–14
 - see also names of agencies*
- Inspector-General of Intelligence and Security
 - jurisdiction, viii
 - powers, 9
 - presentations, 46
 - purpose, 3
 - review of year, vii–viii
 - role and functions, 2, 9, 13, 33, 35, 41
 - statutory officer, 50
- Inspector-General of Intelligence and Security Act 1986*, iii, vi, 2, 8
 - objects of the Act, 3

- section 8(1)(d) or 8(3)(c) inquiries, 11
 - section 8(2) inquiries, 12
 - subsection 32(3) employment, 52
- intelligence agencies, 4–5
 - AUSTRAC information access and use, 33–4
 - complaints, 35–8
 - cross-agency inspections, 33–4 *see also* inspections
 - IGIS engagement with, 45–6
 - IGIS jurisdiction, vii, viii, 2
 - limits on functions, 22
 - Ministerial authorisations, 2
 - privacy rules, viii, 23, 26, 29, 31, 32
 - public interest disclosures, 40–2
 - recruitment complaints, 38, 39
 - see also names of agencies*
- Intelligence Services Act 2001*, 13
 - ‘Australian person’ determination, viii
 - breaches of, 24, 31
 - limits on intelligence agencies’ functions, 22
 - privacy rules, 23 *see also* privacy rules compliance
 - section 13B notices, 25–6
 - training, 31, 32
- internal audit, 54
- international engagement, vii, 48
- Internet home page, *inside front cover*

J

- journalist information warrants, 17
- judicial decisions, 52
- jurisdiction, viii

L

- legal advice, incorrect, 12, 30
- legislative framework (purposes), 3, 13
- letter of transmittal, iii
- liaising with other accountability or integrity agencies, 47–8



M

- market research, 87
- memoranda of understanding
 - ASIO/AUSTRAC, 34
 - IGIS/ATO, 19
 - IGIS/AUSTRAC, 33
 - IGIS/Ombudsman, 47
- metadata collection, 17
- Minister for Defence, 5, 28, 29, 31
- Minister for Foreign Affairs, 4, 24
- ministerial and other authorisations to collect intelligence, 22, 24–5, 28, 31
- Ministerial submissions
 - ASD, 28
 - ASIO, 19, 20
 - ASIS, 24, 25

N

- National Disability Strategy, 57
- nationality, presumption of, 23, 26, 29
- non-salary benefits, 54
- notifiable incidents (WHS), 87

O

- Office of National Assessments Act 1977*, 13
- Office of National Assessments (ONA)
 - AUSTRAC information access and use, 34
 - complaints, 36
 - inquiries relating to, vii, 11, 32
 - inspections of, 32
 - privacy guidelines compliance, 32
 - public interest disclosures, 40
 - role and functions, 4–5
- Office of the Inspector-General of Intelligence and Security, 2, 3 *see also* Inspector-General of Intelligence and Security
- oleoresin capsicum spray (pepper spray), 27
- Ombudsman, 37, 42, 47–8, 52
- ONA *see* Office of National Assessments (ONA)
- online investigative activities, 21

- operational files (ASIS), review of, 26
- operational planning (OIGIS), 50–1, 54
- organisational profile, 53
- organisational structure, 50
- outcome and program, 3
- outreach program *see* presentations and outreach

P

- parliamentary committees

- IGIS submissions and appearances, 17, 43
 - scrutiny of IGIS, 52

- Parliamentary Joint Committee on Intelligence and Security, vii, viii, 2, 17, 21, 43
- pepper spray (oleoresin capsicum spray), 27

- performance

- annual performance statement, 8
 - financial performance summary, 60–3
 - performance criteria map, 84–5
 - performance summaries, 9–10, 13–14, 35–6, 40, 43, 44, 45, 47
 - results at a glance, 8
 - results discussion:
 - Activity 1, Inquiries, 9–12
 - Activity 2, Inspections, 13–34
 - Activity 3, Responding to complaints, 35–9
 - Activity 4, Public Interest Disclosures, 40–2
 - Activity 5, Advice to parliamentary committees and others, 43
 - Activity 6, Evidence to the AAT and the Australian Information Commissioner, 44
 - Activity 7, Engagement with the intelligence agencies and the public, 45–6
 - Activity 8, Liaising with other accountability or integrity agencies, 47–8

- performance pay, 55

- personal security *see* protective security

- plans and planning (OIGIS), 50–1, 54

- corporate plan, 3, 13
 - risk management plan, 51, 54

- Portfolio Budget Statements, 3, 13

- portfolio relationship, 2

- presentations and outreach, 45–6

- presumption of nationality, 23, 26, 29

- Prime Minister, 2, 5



privacy rules, 23, 31, 32
 privacy rules compliance, viii, 23, 26, 29, 31, 32
 procurement, 56
 protective security, 51
Public Governance, Performance and Accountability Act 2013, iii, vi, 8, 51
Public Interest Disclosure Act 2013, 3, 40, 41
 Public Interest Disclosure matters, vii, 35, 40–2, 48
Public Service Act 1999, section 24(1) determinations, 51, 54
 purchasing, 56
 purpose, 3

Q

questioning and detention warrants, 17

R

record keeping, 15, 18, 19, 26, 27, 33–4
 recruitment complaints, 38, 39
 remuneration

- non-salary benefits, 54
- performance pay, 55
- salary scale, 86
- SES, 51

 resources for outcome, 61–2
 risk management, 51
 Risk Management Plan, 51, 54
 roles and functions

- IGIS, 2, 9, 13, 33, 35, 41
- intelligence agencies, 4–5

Rules to Protect the Privacy of Australians, 29, 31

S

salary scale, 86
 section 24(1) determinations, 51, 54
 security (OIGIS), 51
 security assessments by ASIO, 19

- complaints, 37, 38

 security clearances (OIGIS staff), 54

Senate Estimates committees, vii, 43
 Senate Standing Committee on Finance and Public Administration, 43
 Senior Executive Service (SES) officers, 51
 senior management committees, 50
 signals intelligence *see* Australian Signals Directorate (ASD)
 small business participation in procurement, 56
 social media, 21
 Special Intelligence Operations, 18
 staff
 average staffing level, 62
 employment arrangements, 51, 52, 54
 gender balance, 53
 non-salary benefits, 54
 numbers and profile, 53
 salary scale, 86
 training and development, 55
 Stone, Hon Margaret, 2, 50 *see also* Inspector-General of Intelligence and Security
 study assistance scheme, 55
 submissions by IGIS to inquiries and reviews, 17, 43
 submissions to Ministers *see* Ministerial submissions
 surveillance devices, 21

T

Taxation Administration Act 1953 (TAA), 19
 taxation information, 19
Telecommunications (Interception and Access) Act 1979 (TIA Act)
 ASD compliance, 12, 29–30
 ASIO compliance, 16
 breaches of, 12, 16, 29–30
 telecommunications data, 18
 telecommunications interception, 12, 16, 29–30
 timeliness
 complaints handling, 36, 37
 inquiries, 11
 training and development (OIGIS), 55



U

use of force, 16, 17

V

visa security assessment processes, 19
complaints, 36, 37

W

warrants (ASIO), 16–17
weapons use and issues (ASIS), 27
website address, *inside front cover*
whistleblower protection scheme *see* Public Interest Disclosure matters
Willing, Annette, 50
work health and safety (OIGIS), 87

