



# **Annual Report**

2015–2016

# 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  
Fax: (02) 6271 5696

## General inquiries

Phone: (02) 6271 5692  
Fax: (02) 6271 5696

## Non-English speakers

If you speak a language other than English and need help please call the Translating and Interpreting Service on 131 450 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](http://www.igis.gov.au)

Annual report:  
[www.igis.gov.au/annual\\_report/index.cfm](http://www.igis.gov.au/annual_report/index.cfm)

ISSN: 1030-4657

© Commonwealth of Australia 2016



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](http://www.creativecommons.org).

Design and typesetting by Spectrum Graphics [www.sg.com.au](http://www.sg.com.au)

Printed by Impress Printers



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 2015 to 30 June 2016.

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 those components of the report which relate to them will not prejudice security, the defence of Australia, Australia's relations with other countries, law enforcement operations or the privacy of individuals. The report is therefore suitable to be laid before each House of Parliament.

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

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

Yours sincerely

Margaret Stone  
Inspector-General  
23 September 2016

# Contents

## i

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

## 2 Part 1

### Overview

The role of the Inspector-General of Intelligence and Security	2
About the Australian intelligence agencies	3

## 6 Part 2

### Performance summary

Annual performance statement	6
Introductory statement	6
Entity purpose	6
Results	7
Analysis of performance against the entity purpose	9
Summary of IGIS financial performance and resources for outcomes	10

---

## 12 Part 3

### Performance discussion

Activity 1: Conducting inquiries	12
Activity 2: Undertaking inspections	14
Activity 3: Responding to complaints	35
Activity 4: Public Interest Disclosures	40
Activity 5: Advice to parliamentary committees and others	41
Activity 6: Evidence to the AAT and the Australian Information Commissioner	42
Activity 7: Presentations and outreach	43
Activity 8: Liaising with other accountability or integrity agencies	44

## 46 Part 4

### Management and accountability

Corporate governance	46
Management of human resources	48
Other information	49

## 52 Part 5

### Financial statements

Financial statements (with ANAO report and Inspector-General's statement)	53
---	----

## 73 Part 6

### Annexures

Annex A: Entity resource statement and resources for outcomes 2015–16	74
Annex B: Salary ranges for APS employees in OIGIS in 2015–16	76
Annex C: List of annual report requirements as set out in Schedule 2 to the PGPA Rules	77
Annex D: Glossary of abbreviations	84
Index	85

# About this report

This is the Inspector-General of Intelligence and Security (IGIS)'s annual report for the period from 1 July 2015 to 30 June 2016.

This report has been prepared according to 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 financial results, and discusses the outlook for the year ahead.

**Part One** provides an overview of the Inspector-General of Intelligence and Security, including the role and functions of the office, our published outcomes and programme 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.

**Part Two** provides a summary of the office's performance during the reporting period. This includes an Annual Performance Statement, which summarises our performance against the indicators identified in our corporate plan, as well as a report on the financial performance of the office during the reporting period.

**Part Three** contains a more comprehensive discussion of the office's performance across the key activities that we undertook during the year. This includes both quantitative and qualitative discussion. Part Three also incorporates the requirements under section 35 of the IGIS Act to include certain additional information in the annual report, including the Inspector-General's comments on inspections conducted under section 9A of the IGIS Act.

**Part Four** contains information about the management and accountability of the office during 2015–16, including its organisational structure, corporate governance, management of human resources and other relevant information.

**Part Five** contains the office's audited financial statements.

**Part Six** contains the annexes to this report. The annexes contain a range of additional information about the office, including its entity resource statement, 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

My term as Inspector-General commenced in August 2015. I would like to acknowledge the work of my predecessor, Dr Vivienne Thom, and to congratulate her well deserved award as a Member of the Order of Australia. Dr Thom carried out her work as Inspector-General with integrity and professionalism, and I have her to thank for the efficiently run office and highly committed staff that I have inherited. I look forward to continuing to build on these foundations over the years ahead.

After significant legislative change during the previous reporting period, 2015–16 has been a time of consolidation in our inspection work. The national security legislative reforms enacted over the past two years substantially increased the powers of the intelligence agencies and our oversight arrangements. The changes required a revision of our work programme and existing inspection methodology to focus on the use of the new powers and higher risk activities.

The office continued to perform strongly during the reporting period, with new inspections being developed and carried out in addition to a comprehensive regime of existing inspections being maintained. We also continued to handle a large number of complaints, and one inquiry was finalised during the early part of the reporting period. I did not consider that any new matters arising from inspections or complaints to the office warranted investigation by means of a formal inquiry, and there were no ministerial references for inquiry.

Since my appointment, I expanded the outreach activities of the office. In particular, this has involved an increasing emphasis on engagement with 'thought leaders' in the Australian community, including through presentations at various forums and meetings with the judiciary and academics. My aim is to raise awareness of the role of the Inspector-General and to enhance public confidence in the extensive and powerful oversight of this office.

In the previous reporting period, the Government announced that the office would be exempt from the efficiency dividend from 2015–16. This exemption and additional funding received in recent years allowed for the recruitment of additional staff to help the office continue its comprehensive and effective oversight programme. Despite a range of recruitment and selection processes during the reporting period, staff turnover and lengthy security clearance processes before new staff can be appointed have challenged our attempts to increase staffing levels. On the positive side, we do now have a dedicated corporate officer to undertake tasks such as finance and human resource management, and this has relieved investigative staff of these duties. We also participated with other agencies in a short-term exchange of secondees which provided valuable experience for all those involved.

While the activities of the office will continue to be challenged by resource and recruitment constraints, in the year ahead we will maintain an approach to inspections that gives priority to the highest risk activities. I am also considering possible inquiries for the coming year. Supplementing our core work, I intend to continue to expand our outreach activities and engage with our stakeholders on matters of mutual interest.

# PART

## 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, succeeding Dr Vivienne Thom.

The Office of the Inspector-General of Intelligence and Security (OIGIS) is within the Prime Minister's portfolio but is not part of the Department of the Prime Minister and Cabinet. It has 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. Earlier identification of such issues may avoid 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 staff of an intelligence agency, about the activities of an intelligence agency.

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 programme structure

As explained in the Portfolio Budget Statements (PBS), "Government outcomes are the intended results, impacts or consequences of actions by the Government on the Australian community". That being so, the office has only one outcome, which is expressed in the PBS as the provision of independent assurance for the Prime Minister, senior ministers and Parliament as to whether Australia's intelligence and security agencies act



legally and with propriety by inspecting, inquiring into and reporting on their activities.

The 'Office of the Inspector-General of Intelligence and Security' is the only programme identified in the PBS as contributing to this outcome.

There were no changes to either the outcome or the programme during the reporting period.

## Purposes

Consistent with the above, the *OIGIS Corporate Plan 2015–19* 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:
  - the compliance with the law by, and the propriety of particular activities of, Australian intelligence agencies; and
  - the effectiveness and appropriateness of the procedures of those agencies relating to the legality and propriety of their activities; and
  - certain other aspects of the activities and procedures of certain of those agencies; and
- b) 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 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.

The Organisation'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 and the States and 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 warrant, 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 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 Australian Defence Force operations. AGO also directly assists 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 the information.

# PART 2

## Performance summary

### Annual performance statement

#### Introductory statement

I, Margaret Stone, as the accountable authority of the Office of the Inspector-General of Intelligence and Security, present the 2015–16 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**

#### Entity purpose

The purpose of the IGIS is 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.<sup>1</sup>

In performing this role, the IGIS, who is an independent statutory officer established by the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act), reviews the activities of the Australian intelligence agencies:

- Australian Security Intelligence Organisation (ASIO)
- Australian Secret Intelligence Service (ASIS)
- Australian Signals Directorate (ASD)
- Australian Geospatial-Intelligence Organisation (AGO)
- Defence Intelligence Organisation (DIO)
- Office of National Assessments (ONA).

<sup>1</sup> *IGIS Corporate Plan 2015–19*, p. 3.

The 2015–16 Portfolio Budget Statements provided a strategic direction statement with one planned outcome for the office, being:

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

The key strategies by which the office sought to achieve this outcome were:

- to continue and expand the entity's inspection activities, which involve proactively monitoring and reviewing the activities of the intelligence agencies
- where appropriate, to initiate 'own motion' inquiries and investigate complaints or referrals about the activities of the intelligence agencies
- at the request of the Prime Minister, to inquire into an intelligence and security matter relating to any Commonwealth agency.

## Results

### Performance criterion 1: The timeliness of completion of inquiries or complaint resolution

#### Criterion source:

*Corporate Plan 2015–19; Programme 1.1, 2015–16 Portfolio Budget Statements, p. 243.*

#### Result

One inquiry was concluded during 2015–16 with a duration of 157 days. This duration was considered to be reasonably proportionate to the level of complexity of the inquiry. The final report was provided to ASD in July 2015.

Of the complaints received during 2015–16, 95 per cent were acknowledged within five business days (Target: 90 per cent) and were investigated in a timely manner.

All four Public Interest Disclosure matters received in 2015–16 were acknowledged within five business days and were investigated in a timely manner.

### Performance criterion 2: The level of acceptance by intelligence agencies, complainants and ministers of findings and recommendations of inquiries conducted

#### Criterion source

*Corporate Plan 2015–19; Programme 1.1, 2015–16 Portfolio Budget Statements, p. 243.*

#### Result

The inquiry report included four (classified) recommendations, however it did not find any failure of ASD to comply with the law, nor did it reveal any systemic failures of governance or improper activity. As requested, ASD responded to the report in October 2015.

ASD accepted the principles underlying the recommendations and the Inspector-General is satisfied that ASD has appropriate ongoing arrangements in place in relation to the subject of the inquiry and was responsive to the recommendations.

### Performance criterion 3: The breadth and depth of inspection work undertaken

#### Criterion source

*Corporate Plan 2015–19; Programme 1.1, 2015–16 Portfolio Budget Statements, p. 243.*

#### Result

Inspections were a key area of focus during the reporting period. The office's existing programme of inspections was maintained and several new types of inspection and inspection projects were undertaken. Inspection activities were prioritised based on a risk management approach, within the resources available to the office.

**Performance criterion 4: The extent to which there has been change within the agencies as a result of activities of OIGIS**

**Criterion source**

Corporate Plan 2015–19; Programme 1.1, 2015–16 Portfolio Budget Statements, p. 243.

**Result**

- Routine reporting arrangements between ASD and the IGIS have been revised to ensure appropriate levels of ongoing oversight in relation to the subject of the inquiry.
- Detailed inspections are a key means by which the IGIS provides independent assurance that the Australian intelligence and security agencies are acting legally and with propriety. While the majority of inspections conducted in 2015–16 found no issues of concern, those that were found attracted further scrutiny. The office encouraged modification of agency practices in order to prevent reoccurrence.
- Our complaint investigation activities frequently provide opportunities to effect change in the intelligence agencies. In most cases, complaints can be resolved quite quickly and efficiently by IGIS staff speaking to the relevant agency or looking at their records.
- Similarly, our investigation of Public Interest Disclosure matters provides opportunities to effect change in the intelligence agencies where instances of impropriety or illegality are uncovered. No instances of wrongdoing on behalf of the intelligence agencies were uncovered by the IGIS's investigation of Public Interest Disclosures during 2015–16.
- Engagement with parliamentary committees and similar bodies provides opportunities for the Inspector-General to influence the development of the policies and legislation under which the intelligence agencies operate. During 2015–16, the IGIS participated in inquiries conducted by the Parliamentary Joint Committee on Intelligence and Security, reviewed evidence provided by ASIO to the coronial inquest into the Lindt Café siege, and contributed to the statutory review of the *Public Interest Disclosure Act 2013*. The Inspector-General also participated in a Senate estimates hearing.
- The IGIS's engagement and cooperation with the Administrative Appeals Tribunal and the Australian Information Commissioner also assists in enhancing oversight and promoting good practice in the agencies. During the reporting period, the IGIS responded to two requests from the Information Commissioner and was notified by the Administrative Appeals Tribunal of one new case where the IGIS may be requested to give evidence.
- The office continued to undertake presentations to new and existing staff of the intelligence agencies, with 13 such presentations delivered in 2015–16. By raising awareness of the accountability framework and promoting understanding of agency responsibilities, this ongoing contact helps to encourage a culture of lawfulness and propriety in the agencies.
- The office also expanded its outreach activities to external groups in 2015–16, particularly 'thought leaders' in the community such as judges, academics and public interest groups. The office delivered 14 such presentations during 2015–16. This outreach is intended to help raise the profile of the office and enhance public assurance in the oversight it provides.

- During 2015–16, staff from the office met regularly with the office of the Commonwealth Ombudsman, continued to liaise with the Australian Human Rights Commission, and held meetings with the New Zealand Inspector-General of Intelligence and Security and a representative of the Canadian Privy Council Office.
- Our cooperative relationship with other accountability and integrity agencies helps promote strong and seamless oversight across government, aiding the office in its role of providing independent assurance of the legality and propriety of the actions of the Australian intelligence agencies.

## Analysis of performance against the entity purpose

Our results show that the office continued to perform strongly in 2015–16 in support of its purpose of assisting Ministers in the oversight and review of the Australian intelligence agencies, assuring the Parliament and the public about the scrutiny of the operation of those agencies, and assisting in investigating intelligence and security matters.

A key area of focus during 2015–16 was the ongoing development of the office's inspection programme, with new inspections being carried out in addition to a comprehensive regime of existing inspections being maintained. Detailed inspections are a core means of ensuring legality and propriety of the agencies' activities. While the majority of inspections found no issues of concern, when issues were found they resulted in further scrutiny and we observed changes to agency practices in order to prevent reoccurrence. As with previous years, inspection activities were given priority on a risk management approach, within the resources available to us.

We also continued to handle many complaints during 2015–16, however there was an overall decrease in the number of complaints compared to previous years due to a decrease in the number of visa-related complaints. There was a slight increase in the number of other complaints and contacts with our office. There were also four Public Interest Disclosures handled by our office in 2015–16, the same number as the previous year. Although a majority of the complaints were resolved without identifying significant issues, there were a number which raised credible concerns which were also able to be resolved.

One inquiry was completed during the early part of the reporting period. No new matters arising from inspections or complaints were considered by the Inspector-General to warrant investigation by means of a formal inquiry, and there were also no matters referred to the IGIS by a minister for inquiry. A number of matters were resolved administratively during the reporting period and the Inspector-General is considering possible inquiries for commencement in the 2016–17 financial year.

During 2015–16, the Inspector-General also focused on expanding the outreach activities of the office. This involved presentations to staff of intelligence agencies as well as an increasing emphasis on engaging through forums and meetings with the broader Australian community. This external engagement is intended to increase public understanding of the role of the IGIS in overseeing and reviewing the actions of the intelligence and security agencies. We also continued our regular liaison with other accountability and integrity agencies, in particular the Office of the Commonwealth Ombudsman and the Australian Human Rights Commission.

## 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 2015–16 financial statements. A summary of our financial performance follows.

The office operated within available resources in 2015–16 and ended the year with a surplus of \$552 564.

Following a significant increase in appropriation funding in the previous year funding levels in 2015–16 remained steady with a slight increase reflecting changes in economic parameters.

In relation to expenditure, the most significant budget variance related to employee expenses (\$427 150 underspend). This variance was largely due to delays in the lengthy security clearance process associated with recruitment. Other underspends included demand driven expenses including \$30 000 for consultants, \$21 000 for legal expenses, \$13 000 for potential software licences and \$36 000 for security clearance fees.

Net equity increased from \$2 253 786 in 2014–15 to \$2 831 350 in 2015–16. Movements in equity included a \$552 564 increase in retained surplus. Contributed Equity also increased from \$478 126 in 2014–15 to \$503 126 in 2015–16. Movements in Contributed Equity included capital funding of \$25 000.

The following tables can be found in Part 6 Annex A:

Figure 5.1 – Entity Resource Statement 2015–16

Figure 5.2 – Expenses for Outcome 1.

IGIS has one outcome and one programme.

## Trends in Finance

Significant changes to the finances of the office during 2015–16 included:

- A \$159 407 increase in employee expenses arising from the additional staff recruited as a consequence of the receipt of additional funding in the previous year.
- A \$60 000 decrease in supplier expenses. Decreases in expenditure included \$17 000 in legal expenses, \$20 000 in staff training expenses, \$15 000 in travel expenses and \$11 000 in translation expenses.
- A \$50 000 increase in Property, Plant and Equipment following an upgrade to the office's secure IT system and the fit-out of the office with sit-to-stand desks.
- A \$21 000 decrease in Other Payables resulting from an increase in outstanding reimbursements to home agencies for seconded staff offset by a decrease in accrued salaries at the reporting date.
- A \$268 000 decrease in Employee Provisions because of staff turnover and the changing profile of the staff. The effect was magnified by the increased usage of secondment arrangements whereby leave liabilities are retained by the home agency.



		2015–16 OUTCOME 1 \$	2014–15 OUTCOME 1 \$	Change from previous year
Revenue from Government		3 050 000	3 003 000	+2%
Other Income		128 625	130 023	-1%
<b>TOTAL INCOME</b>		<b>3 178 625</b>	<b>3 133 023</b>	
Employee expenses		2 347 850	2 188 443	+7%
Supplier expenses		263 149	322 932	-18%
Other expenses		15 062	36 517	-59%
<b>TOTAL EXPENSES</b>		<b>2 626 061</b>	<b>2 547 892</b>	
<b>OPERATING RESULT</b>		<b>552 564</b>	<b>585 131</b>	
Financial assets	<b>A</b>	3 479 682	3 240 736	+7%
Non-financial assets	<b>B</b>	77 706	27 218	+185%
Liabilities	<b>C</b>	726 038	1 014 168	-28%
<b>NET ASSETS = A + B - C</b>		<b>2 831 350</b>	<b>2 253 786</b>	

# PART 3

## Performance discussion

Providing a complete picture of our performance requires qualitative discussion as well as quantitative analysis. In support of this, Part Three of the annual report provides a detailed discussion of our activities during 2015–16.

Part Three also complies with the requirements under section 35 of the IGIS Act to include certain additional information in the annual report, including the Inspector-General's comments on:

- any inquiry conducted by the Inspector-General in accordance with paragraph 8(1)(d) or 8(3)(c) of the Act
- any inspection conducted under section 9A of the Act
- the employment of any person under subsection 32(3) of the Act and any delegation under section 32AA that was in force
- the extent of compliance by ASIS, AGO and ASD with rules made under section 15 of the ISA.

The Performance discussion section is divided into eight sections. Each section discusses our performance in relation to one of the key activities identified in the *OIGIS Corporate Plan 2015–19*. These activities are:

1. 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)
2. undertaking comprehensive inspection programmes to monitor and review intelligence agencies' operational activity

3. providing effective and timely responses to complaints or referrals received from members of the public, ministers or members of parliament
4. facilitating the investigation of public interest disclosures and undertaking other responsibilities under the PID Act
5. providing advice to parliamentary committees and others on oversight issues relating to intelligence agency powers and functions
6. providing evidence to the Administrative Appeals Tribunal and the Australian Information Commissioner as required
7. undertaking presentations to new and existing employees of intelligence agencies to ensure an awareness and understanding of their responsibilities and accountability
8. liaising with other accountability or integrity agencies in Australia and overseas.

### Activity 1: Conducting inquiries

*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)*

#### Introduction

Under the IGIS Act, the IGIS can conduct an inquiry into a matter based on a complaint, of the IGIS's own motion, or in response to a ministerial

request. The Act establishes certain immunities and protections and provides for the use of strong coercive powers in such inquiries. These include the power to compel the production of information and documents, to enter premises occupied or used by a Commonwealth agency, to issue notices to persons to attend before the IGIS to answer questions relevant to the matter under inquiry, and for the IGIS to administer an oath or affirmation when taking evidence.

When coercive powers are used, the IGIS Act provides protections to people who have given the IGIS information. Those compelled to give information are protected 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.

Quantitative performance measures

The following metrics, identified in the *OIGIS Corporate Plan 2015–19*, were used to support the quantitative assessment of our performance in relation to this activity:

- number of inquiries conducted
- number of inquiry recommendations accepted and implemented.

One inquiry was finalised during the reporting period, although the majority of the work was carried out during the 2014–15 reporting period. The 157 day duration of this inquiry was considered to be reasonably proportionate to its level of complexity.

The same number of inquiries were finalised during 2014–15. The fact that no new inquiries were commenced in 2015–16 is mainly due to there being no major issue of concern arising during the period, a decision to prioritise the inspection of new functions carried out by agencies as a result of legislative change, there being no referrals received from a responsible minister and no substantiated complaint of sufficient complexity or seriousness to warrant an inquiry.

Discussion

2015 IGIS inquiry into an Australian Signals Directorate matter

In February 2015 an inquiry into an Australian Signals Directorate (ASD) matter was initiated by the then IGIS pursuant to s 8(2) of the IGIS Act. The final report was provided to ASD in July 2015. The report included four (classified) recommendations, however it did not find any failure of ASD to comply with the law, nor did it reveal any systemic failures of governance or improper activity. As requested ASD responded to the report in October 2015.

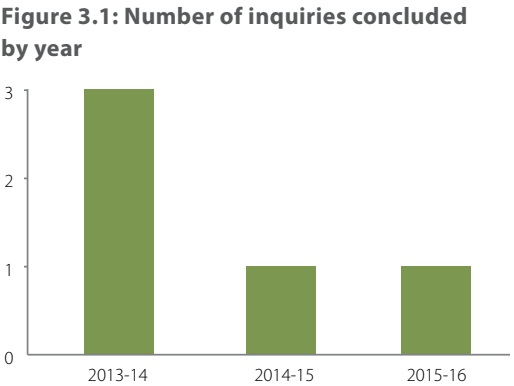


Figure 3.2: Summary of inquiries conducted during 2015–16

Agency	Source	Subject of inquiry	Date initiated	Date finalised	Duration (days)
ASD	IGIS	Inquiry into a matter relating to ASD	9 February 2015	15 July 2015	157

ASD accepted the principles underlying the recommendations and the Inspector-General was satisfied that ASD has appropriate ongoing arrangements in place in relation to the subject of the inquiry and was responsive to the recommendations. Routine reporting arrangements between ASD and the office have been revised to ensure appropriate levels of ongoing oversight in relation to the subject of the inquiry.

A full account of the inquiry is contained in the classified report which has been provided to the Director of ASD and the Minister for Defence 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.

#### **Inquiries conducted in accordance with paragraph 8(1)(d) or 8(3)(c) of the IGIS Act**

There were no inquiries conducted in accordance with paragraph 8(1)(d) or 8(3)(c) of the IGIS Act during the reporting period.<sup>2</sup>

<sup>2</sup> The Inspector-General is required under subsection 35(2) of the IGIS Act to include in the annual report comments on any inquiry conducted during the reporting period in accordance with the specific functions in paragraph 8(1)(d) or 8(3)(c) of the Act.

Paragraph 8(1)(d) provides that a function of the IGIS is:

where the responsible Minister has given a direction to ASIO on the question of whether

- (i) the collection of intelligence concerning a particular individual is, or is not, justified by reason of its relevance to security; or
- (ii) the communication of intelligence concerning a particular individual would be for a purpose relevant to security;

to inquire into whether that collection is justified on that ground or whether that communication would be for that purpose, as the case may be.

Paragraph 8(3)(c) provides that it is a function of the IGIS to, at the request of the responsible Minister or of the Inspector-General's own motion, inquire into any matter in relation to the statutory independence of ONA.

#### **Employment of persons under section 32(3) of the IGIS Act**

In 2015–16 there were no persons employed under subsection 32(3) of the IGIS Act and no delegations in force under section 32AA of the Act.<sup>3</sup>

## **Activity 2: Undertaking inspections**

*Undertaking inspections and visit programmes to monitor and review intelligence agencies' operational activity*

### **Introduction**

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 our staff directly accessing electronic records and reviewing hardcopy documentation.

Inspections concentrate on the potential impact of intelligence collection on the privacy of Australians. As such, inspections largely focus on the activities of ASIO, ASIS, AGO and ASD. This is because each of these agencies 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 there is no indication of their independence being compromised.

<sup>3</sup> The Inspector-General is required under subsection 35(2AA) of the IGIS Act to include in the annual report comments on the employment of any person under subsection 32(3) and any delegation in force under section 32AA during the reporting period.

Subsection 32(3) allows the Inspector-General to, by written agreement, employ a person to assist the Inspector-General to perform functions and exercise powers for the purposes of a particular inquiry, specified in the agreement.

Section 32AA enables the Inspector-General to delegate her inquiry and reporting powers to such a person for the purposes of the particular inquiry.

Inspections focus on whether each agency is acting in accordance with its statutory functions, any guidance provided by the responsible minister, and the agency's own internal policies and procedures. Inspection may comprise a combination of routine inspections (for example ASIO investigative cases and warrants) as well as inspection projects that target specific issues.

## Quantitative performance measures

There were no quantitative performance measures applicable to our inspections work identified in the *OIGIS Corporate Plan 2015–19*.

The qualitative discussion below addresses the breadth, depth and impact of our inspection work in support of an assessment against the key performance indicators. The discussion additionally incorporates the Inspector-General's comments on inspections carried out under section 9A of the IGIS Act and the Inspector-General's comments on the extent of compliance by ASIS, AGO and ASD with the privacy rules made under section 15 of the *Intelligence Services Act 2001*.<sup>4</sup>

## Inspection of ASIO activities

During 2015–16, we conducted a broad range of inspections at ASIO, including:

- regular inspections of investigative cases
- new inspections focused on analytical tradecraft and other areas
- human source management
- ASIO warrants
- Special Intelligence Operations
- access to telecommunications data
- exchange of information with Australian Government agencies
- ministerial submissions

- exchange of information with foreign liaisons
- security assessments, the consequences of which may include decisions by Government to cancel or refuse visas, passports or citizenship applications and in some cases may trigger consideration of removal of welfare payments
- a number of specific inspection projects.

We also examined ASIO's access to sensitive financial information under the *Anti-Money Laundering and Counter Terrorism Financing Act 2006*. The results of these inspections are set out later in this report.

The *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) empowers ASIO to obtain, correlate and evaluate intelligence information relevant to security. ASIO's activities are governed by the ASIO Act as well as the Attorney-General's Guidelines and internal policies and procedures. The Guidelines require that any means used by ASIO to obtain information must be proportionate to the gravity of the threat and the probability of its occurrence. They also require that inquiries and investigations into individuals or groups should be undertaken using as little intrusion into individual privacy as is possible consistent with the performance of ASIO's functions. The Guidelines are available on the ASIO website at [www.asio.gov.au](http://www.asio.gov.au).

We commenced new areas of inspection during 2015–16 in order to ensure that there was no gap in our oversight of certain types of inquiry and investigations.

In one case, the trial inspection demonstrated that this separate inspection programme was not required. The inquiries and investigations activities conducted by this ASIO division were already included in other routine IGIS inspection activities.

<sup>4</sup> The Inspector-General's comments on these matters are required under subsection 35(2A) of the IGIS Act to be included in the annual report.

Other new and existing areas of inspection are discussed below.

### Regular inspection of investigative cases

We continued to review a sample of ASIO investigative cases during the reporting period in order to examine:

- the justification and objectives provided for the investigation
- whether the investigative activities that were undertaken or proposed were appropriate
- whether investigations were subject to formal approval and periodic review
- the application of the principle of proportionality according to the gravity of the threat and the probability of its occurrence and with as little intrusion into individual privacy as is consistent with the performance of ASIO's functions.

Sample selection focuses on those cases utilising more intrusive investigative methods – for example, cases with warrants approved by the Attorney-General, access to sensitive financial information or prospective data authorisations.

During 2015–16, ASIO reviewed and revised a significant proportion of its internal policies and procedures. We paid particular attention to changes where authorisation and delegations levels have been lowered. While no issues of concern were identified by the devolution of authority for approval, we note that it is sometimes desirable for more sensitive matters to be considered and approved at above the minimum level required.

Another ongoing focus of inspections has been ASIO's investigative activities in relation to people under 18 years of age. With an increasing number of young people who are of interest to ASIO, ASIO's policies have evolved with experience. We will continue to focus on this area in our inspections.

We continue to work with ASIO to ensure that the inspection process can provide direct meaningful feedback to ASIO investigative staff in a timely manner with a view to improving processes overall.

### ASIO analytical tradecraft

We initiated a new inspection during the reporting period to look specifically at ASIO analytical tradecraft. In early 2014, ASIO invited the former Director-General of ONA, Mr Allan Gyngell AO, to conduct a comprehensive review into the state of analytical tradecraft and practices supporting the assessment function in ASIO. In June 2015, ASIO advised us that it had implemented a range of policies in accordance with Mr Gyngell's recommendations. We undertook a new inspection to examine compliance with these new policies. The inspection did not identify any issues of concern and we were satisfied with ASIO's policy and training. We will continue this new inspection in the next reporting period.

### Human source management

This inspection activity focuses on ensuring that the management of ASIO human source operations is both legal and proper. While the detailed results of these inspections are sensitive and cannot be disclosed in a public report, no significant concerns were identified in the inspections undertaken during the reporting period.

### ASIO Warrants

ASIO can intercept telecommunications and use other intrusive powers following the issue of warrants by the Attorney-General. Authority for telecommunications interception is provided in the *Telecommunications (Interception and Access) Act 1979* (TIA Act). The ASIO Act provides the authority for other powers, including searches, computer access and surveillance devices.

During 2015–16, inspections of ASIO warrants were undertaken quarterly, as well as in the course of our regular inspections of investigative cases. The separate warrants inspections began in 2014–15 in response to legislative changes made to the warrant provisions in the ASIO Act as part of the *National Security Legislation Amendment Act (No. 1) 2014*. These amendments included a new identified person warrant, a new surveillance device warrant that replaced the separate listening and tracking device warrants, and a number of amendments to the computer access warrants and search warrants. Additionally we inspected a sample of ASIO foreign intelligence collection warrants on a quarterly basis.

We reviewed a significant proportion of warrants obtained by ASIO in 2015–16. Our inspection programme did not identify any errors in ASIO's execution of warrant powers that constituted a breach of either the ASIO Act or the TIA Act. A small number of administrative errors, including typographical errors, were identified. These errors did not affect the legality or propriety of the warrant.

ASIO continued to self-report proactively in relation to breaches or errors in the execution of warrant powers. ASIO reported nine breaches, two of the ASIO Act and seven of the TIA Act. Given the volume of intercept activity, this number of breaches does not indicate a systemic problem. The breaches reported include:

- two breaches that occurred when data continued to be collected after the warrants were revoked by the Attorney-General. In one case, data was collected for 15 days after the revocation. In the other case, a service was not disconnected until six days after the Attorney-General revoked the warrant. In both cases, ASIO deleted the data permanently from its systems. The Inspector-General was satisfied that both breaches arose from human error and did not evidence any systemic practice. The relevant areas have reviewed their internal procedures for dealing with warrant revocations and implemented changes to reduce the likelihood of future occurrences.

- breaches of the TIA Act that occurred where a carrier was advised seven days after internal approval to remove two services. The TIA Act requires a carrier to be notified immediately, with confirmation in writing to be given as soon as practicable. ASIO instructed the service provider to delete any data that was collected. ASIO has established more stringent procedures and advice for staff to ensure a similar error does not occur in the future.
- a breach of the TIA Act that occurred when an incorrect service was intercepted by ASIO due to an incorrect phone number being provided by ASIO. The error was discovered nearly one month after interception began. ASIO purged the collected data from ASIO's systems and provided the correct number. ASIO re-examined its processes for error checking and reaffirmed the need for appropriate checking procedures to ensure a similar error does not occur in the future.
- ASIO advised of an over-collect issue where, for a period of eighteen months, it received an unknown amount of non-target session-related data intermixed with its warranted intercepts. The cause of the over-collect was unknown, but ASIO's initial investigation indicated it was due to a carrier error. In December 2015 ASIO advised it would delete from its systems all of the data collected by the carrier in the relevant period to ensure all non-target data was deleted.

As noted in previous annual reports, the IGIS continues to maintain a close interest in ASIO's use of B-party warrants. B-party warrants provide that ASIO may intercept a telecommunications service that is likely to be used by another person not of security interest to communicate with a person of security interest. B-party warrants can only be used for a maximum of three months, compared to six months for other interception warrants. The IGIS is satisfied that ASIO's use of B-party warrants has been consistent with the provisions in the TIA Act that restrict the availability of B-party warrants, and no outstanding issues remain at this time.

**Identified person warrants** were a key focus of our warrant inspection activity, as they are still a relatively new type of warrant. They differ from other ASIO warrants in that they give conditional approval for ASIO to use one or more special powers against an identified person. The ASIO Act provides that a written authorisation (signed by the Attorney-General or Director-General) is required before ASIO can actually do that which was conditionally approved under the warrant. To date, the majority of the identified person warrants inspected have had the authorisations signed by the Director-General rather than the Attorney-General. We understand this to be the preference of the current Attorney-General.

ASIO advised us of two breaches of the ASIO Act that occurred in its execution of identified person warrants. One occurred in ASIO's first use of an identified person warrant, when an ASIO officer acted on oral rather than written approval to exercise the authority conferred by the warrant.

The second breach occurred after ASIO obtained the Attorney-General's conditional approval to access computers, conduct searches and use surveillance devices in a particular case. Due to an administrative oversight ASIO did not seek specific authorisation, either from the Attorney-General or the Director-General of Security, prior to accessing a computer.

Once the breach was detected, ASIO ceased its computer access activity and quarantined the data that was collected before seeking the necessary authorisation and recommencing access to the computer. ASIO advised the IGIS that it had quarantined and deleted the data from ASIO systems, and implemented additional measures to minimise the likelihood of such breaches recurring. We are satisfied that the access occurred in error and that the new measures to reduce breaches are adequate.

After the execution of a warrant, ASIO must report to the Attorney-General on the intelligence value of the warrant. Initially the reports to the Attorney-General on identified person warrants were narrowly focused on the overall value of the warrant, without specifically referring to which authorisations had been executed, or the intelligence value of those particular authorisations. For example, the warrant report may only have mentioned the intelligence gained from one authorisation, without mentioning if the other authorisation(s) were used and what intelligence (if any) was derived from them. We suggested that the warrant report could provide information on each authorisation, which would give the Attorney-General a better picture of how identified person warrants were being used and how they had assisted ASIO in the performance of its functions. ASIO agreed to this suggestion, and amended its policy to reflect this. We have since seen identified person warrant reports that report on each authorisation and provide a clearer picture to the Attorney-General of what was done under the warrant and the authorisations signed by the Director-General.

### Questioning and detention warrants

The office has procedures in place to oversee ASIO's use of questioning powers however no questioning, or questioning and detention warrants, were issued in the reporting period.

### Journalist information warrants

During the reporting period the Government introduced a journalist information warrant regime. This regime imposes additional constraints on ASIO's access to journalists' telecommunications

data. The TIA Act now requires that, where ASIO seeks the telecommunications data of journalists or their employers for the purpose of identifying a journalist's source, ASIO must first obtain a warrant from the Attorney-General.

We confirmed that ASIO has policies and procedures in place to address the new journalist information warrant requirements and provide staff training. These policies and procedures will be reviewed in the course of our regular inspections.



## Use of force

Warrants issued under the ASIO Act may authorise the use of force so long as it is necessary and reasonable to do the things specified in the warrant. This provision was amended during the last reporting period specifically to include a reference to using force against persons as well as against things. Under section 31A of the ASIO Act, when force is used in the execution of a warrant ASIO is required to notify the Inspector-General 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, we did not receive any notifications of the use of force against persons during the execution of ASIO warrants by either ASIO or law enforcement officers. We will monitor the timeliness of notification and reporting of any future use of force.

There has been very close consultation between our office and ASIO in relation to ASIO's updated training and policy guidance in this area and we have maintained strong interest in ASIO's development and implementation of training for its officers in the use of force. ASIO has addressed issues raised by our office. In the last reporting period, ASIO commenced a self-defence training programme. During this reporting period, ASIO has commenced additional training specifically for officers involved in the execution of warrants. No ASIO officer is authorised to use force in the execution of a warrant until after receiving appropriate training. We will continue to monitor the frequency and effectiveness of this training.

## Special Intelligence Operations

We commenced inspecting ASIO's use of this new power in 2014–15.<sup>5</sup> With experience, our inspection methodology continued to evolve during the reporting period.

The legislation requires that ASIO notify the IGIS as soon as practicable after the special intelligence

operation authority is granted. In one case the IGIS was notified 10 days after the authorisation was granted. We noted that this was not in accordance with the legislation. ASIO promptly implemented a new procedure, which is working well.

The legislation also requires ASIO to give the Attorney-General and the IGIS a written report on each Special Intelligence Operation.

We have reviewed the documentation relating to each Special Intelligence Operation approved, and in some cases have received additional briefings. We have not identified any issues of legality or propriety.

We will continue to pay close attention to ASIO's Special Intelligence Operations.

## Access to telecommunications data

The *Telecommunications (Interception and Access) Act 1979* (TIA Act) enables certain persons to authorise the collection of prospective and historical telecommunications data from telecommunications carriers or carriage service providers. The Director-General, Deputy Director-General and ASIO employees or affiliates at an SES Band 2 or higher level may provide the authorisation for prospective data. The Director-General, Deputy Director-General and ASIO employees or affiliates approved by the Director-General for that purpose, may provide an authorisation for historical data. Prospective data authorisations provide near real-time data (typically call associated data and network location data) for the period that an authorisation is in force. The threshold that ASIO is required to meet is that access to the data is in connection with the performance by ASIO of its functions. In addition, the Attorney-General's Guidelines state that investigative activities should intrude into personal privacy as little as possible, consistent with the performance of ASIO's functions. The Attorney-General's Guidelines also require that priority be given to less intrusive means, and that authorisation levels for more intrusive activities should be higher.

ASIO's access to prospective telecommunications data and historical telecommunications data is reviewed as part of our regular inspection of ASIO investigative cases, discussed above.

Prospective data authorisations reviewed were endorsed by an appropriate senior officer, and

<sup>5</sup> Special Intelligence Operations are authorised in accordance with the Australian Security Intelligence Organisation Act 1979 Part III, Division 4 ss35A-35R

demonstrated that ASIO has regard to the Attorney-General's Guidelines and is meeting the legislative requirement to make requests for data only in the performance of its functions.

In July 2015, ASIO advised us of an error that had occurred in a telecommunications provider's interception system which, contrary to the prospective data authorisation, resulted in ASIO receiving SMS content of multiple mobile phone services belonging to the provider. The problem occurred because the provider initiated a change to its systems without providing ASIO with any notice of these changes or any testing of the changes prior to their implementation. The error was discovered in less than two days. On discovery of the issue, ASIO undertook an audit of access logs and confirmed that no ASIO staff had accessed the unwarranted content. All the content was deleted from ASIO's systems, and the telecommunication provider rectified the situation by reinstating the previous system. ASIO undertook to investigate ways to buffer incorrect data of this type in the future.

### Preservation requests

No specific inspection activity occurred in the reporting period, but these requests may be reviewed as part of inquiry and investigation inspections. There were no issues of concern noted during the reporting period.

### ASIO exchange of information with Australian Government agencies

An area of focus for our office is ASIO's liaison with other government agencies, particularly where sensitive personal information is involved. During the reporting period we queried ASIO's procedure regarding requests for sensitive personal information from another Australian Government agency. While we did not have concerns with ASIO's limited use of the information, we did suggest that where the information is to be used in security intelligence investigations, ASIO should consider whether it is appropriate to require additional approval to access the information and the level at which, where required, the approval can be given. ASIO has advised it will change its procedure accordingly.

### Access to taxation information

Section 355-70 of Schedule 1 to the *Taxation Administration Act 1953* provides that a taxation officer authorised by the Commissioner of Taxation or delegate may disclose protected information to an authorised ASIO officer if the information is relevant to the performance of ASIO's functions.

This access to sensitive information is further governed by a memorandum of understanding between the Commissioner of Taxation and the Director-General of Security, the Attorney-General's Guidelines, and ASIO's internal guidelines and procedures.

ASIO rarely requests access to this type of information. We review all of ASIO's access to sensitive taxation information, including:

- ASIO requests for information to the ATO
- spontaneous disseminations from the ATO to ASIO
- disseminations of information from ASIO to a law enforcement agency.

In 2015–16, ASIO reported that no requests had been made to access ATO information. The ATO made two proactive disclosures to ASIO, which will be reviewed in August 2016.

During this reporting period, our staff also conducted a review of ASIO access to sensitive tax information carried over from the previous financial year. We did not identify any matters of concern.

### Ministerial submissions

Each quarter we review a range of briefing notes and submissions on operational matters made by ASIO to the Attorney-General. In addition to the other ASIO inspection activities, these reviews continue to be useful in supporting our oversight of legality and propriety issues relevant to high risk activities—for example, cooperation with new foreign agencies, and significant operations.

### **ASIO exchange of information with foreign liaison**

The ASIO Act provides the authority for ASIO to seek information from, and provide information to, authorities in other countries that is relevant to Australia's security or the security of the foreign country. ASIO may cooperate with foreign authorities approved by the Attorney-General. In general, the foreign authorities that are approved by the Attorney-General perform broadly similar functions to ASIO. In the course of our regular reviews of ASIO investigative cases we noted authorisation documentation and correspondence for such exchanges. We have noticed some inconsistency in relation to how records are kept regarding foreign liaison. We have come across varying practices throughout the Organisation in our inspections. We will continue to monitor how records on foreign liaison activity are kept as part of our inspection activities.

### **Security assessments (which can lead to cancellation or refusal of visas or passports and in some cases may trigger consideration of removal of welfare payments)**

We continued to review a sample of cases where ASIO had recommended passport suspension, cancellation or refusal, or visa (emergency or regular) cancellations. We also reviewed cases where, in consequence of a security assessment for passport purposes, the Government may consider cancelling a person's entitlement to welfare payments. We continue to pay particularly close attention to any passport suspensions that do not proceed to a cancellation. In those cases, we may look in greater depth at the intelligence case supporting ASIO's advice to assess whether the advice was reasonable based on what was known to ASIO at the time.

In last year's annual report we noted that we had conducted an inspection project focusing on whether ASIO's advice concerning the (then) passport cancellation and refusal powers was consistent with the relevant legislation. At the time, section 14 of the *Australian Passports Act 2005* (Passports Act) made a distinction between advice provided by ASIO and advice provided by the Director-General of Security, depending on

whether the request concerned circumstances relating to a foreign country or concerned prejudice to Australia's security. The review found that ASIO's advice to the Minister appeared not to make the distinction in relevant cases. ASIO agreed to review its ministerial submission templates for passport cancellation and refusal to reflect the legislative basis for recommendations under the Passports Act.

We note that the Passports Act and the accompanying Australian Passports Determination have since been amended. The competent authority in both circumstances (whether the request concerns a foreign country or prejudice to the security of Australia) is now either the Director-General of Security or a Deputy Director-General of Security. This removes any uncertainty with regard to the identification of the competent authority in individual cases. ASIO's templates reflect this and we are satisfied this issue has now been resolved.

### **ASIO inspection projects**

#### **ASIO's record retention and destruction project**

The IGIS annual report for 2014–15 reported on a project we initiated to investigate the data destruction practices of ASIO, with a specific focus on material obtained under warrants.

At that time, we made a number of observations arising from this project in relation to ASIO's electronic and paper-based file keeping practices.

The findings of this project are informing the IGIS's input to the review of the Attorney-General's Guidelines being undertaken by ASIO and the Attorney-General's Department – the review was ongoing at the end of the reporting period. The Government initiated this review in response to a recommendation of the Parliamentary Joint Committee on Intelligence and Security as part of its review of the *National Security Legislation Amendment Bill (No. 1) 2014*. In accordance with that recommendation, the Attorney-General's Guidelines issued under section 8A of the ASIO Act are being reviewed, including examining requirements to govern ASIO's management and destruction of information obtained on persons who are not relevant, or no longer relevant, to security matters.

### Use of information holdings within ASIO

In mid-2015, we initiated an inspection project to review ASIO's implementation and auditing of the policy introduced in June 2014 concerning staff use of ASIO's information holdings. The policy emphasises that information holdings within ASIO are only for official purposes and not for matters which may be relevant to their personal circumstances; staff with personal security concerns should raise this with the relevant areas within ASIO, for checks to be undertaken if appropriate. The policy was implemented following concerns raised by the former IGIS in 2013–14 about the purposes for which ASIO staff were accessing ASIO information holdings.

In the course of the inspection project, ASIO provided us with details of guidance material and training provided to staff on the new policy and the audits conducted to determine compliance. ASIO also identified three instances of non-compliance with the policy. While these instances did not raise any serious or systemic concerns, we felt that they did highlight the need for ASIO to continue its efforts to ensure that staff were aware of their responsibilities. This is particularly important for staff who were familiar with the previous policy. ASIO advised that they are considering other ways to remind staff of their security obligations. We have also asked ASIO to provide us with periodic updates on the results of audits and any instances of non-compliance with the policy, so that we can continue to monitor this issue.

### ASIO Telecommunications Interception System

During the reporting period, our staff reviewed a number of warranted and non-warranted telecommunications activities as part of an inspection project.

The services subject to the inspection were identified during regular inspections as being of potential compliance risk. These matters included collection of non-subject data or where there was an interval between the expiry of one instrument and the authorisation of the next. In the course of this inspection we identified one compliance issue where data had been retained unnecessarily.

In February 2016, ASIO advised our office of an 'overcollection' of telecommunications data under a warrant.

Mobile phone data was collected for 12 days from a mobile phone that was not being used by ASIO's person of interest. In the course of requesting the warrant, ASIO had undertaken the appropriate checks prior to interception that indicated the service belonged to the person of interest. There was no information to indicate the individual actually using the service was linked to the person of interest. ASIO advised the IGIS that it ceased intercepting the product and deleted all of the product collected from ASIO systems, however during an inspection of ASIO's telecommunications interception system it was discovered that the data had not been deleted, although it had been quarantined awaiting deletion. ASIO has advised that the error was due to a vendor system setting. ASIO have since confirmed that the data has now been fully deleted. While we are satisfied that this incident involved a simple oversight, it is important that the advice provided to this office is accurate.

### Warrants 'whole of life' project

In April 2015, the previous IGIS initiated an inspection project reviewing four sets of warrants where consecutive warrants have been issued over time. The purpose of the project was to review the underlying intelligence case for each warrant and to consider whether the intelligence case put to the Attorney-General each time the warrant was raised was accurate and balanced. Based on the sample of warrants examined, the review concluded that ASIO generally managed the warrant renewal process with appropriate consideration of its obligations under the ASIO Act and the TIA Act and consistently with ASIO's internal policies and procedures. In particular, the inspection team noted improvements in source documentation between the 2011 and 2014 warrants. The project did observe some draft warrant documentation which lacked references to source documents. The project also noted that ASIO publishing practices and guidelines were not consistently applied by staff in preparation of warrant documentation.

As a result of the project findings, we recommended that ASIO teams responsible for preparing warrant documentation should consider implementing a more formal quality assurance

process and extend the principles of ASIO's new Analytical Tradecraft policies, released in May 2015, to warrant documents. This will provide greater assurance that the Attorney-General is provided with sound analysis characterised by current, objective, clear, easily located and comprehensive information. ASIO advised that, following the receipt of the report, ASIO staff were reminded of ASIO internal procedures regarding referencing and retention of draft documentation.

### Lawyers at interview

During the reporting period, we conducted an inspection project to follow up on an inquiry the previous IGIS had carried out in 2013. The inquiry concerned the attendance of legal representatives at ASIO interviews, and related matters.

The 2013 inquiry examined concerns raised by the Refugee Advisory and Casework Service (RACS), which alleged inconsistent and arbitrary practices by ASIO in relation to the attendance of legal representatives at security assessment interviews. The inquiry also considered related issues that arose during the course of the inquiry in respect of ASIO's broader policies and practices for the conduct of voluntary interviews (that is, those which are not conducted under the authority of a questioning warrant or a questioning and detention warrant).

The final report was presented to the Attorney-General in January 2014 and made five recommendations. ASIO agreed to recommendations 1-4 of the report and agreed in part to recommendation 5. In August 2014, ASIO provided advice to the IGIS regarding its implementation of these recommendations.

This inspection project reviewed ASIO's implementation of the inquiry's recommendations, and found that ASIO has implemented the changes recommended in the inquiry. We note that ASIO's policies are now clearer, especially in relation to the presence of third parties at interviews and the voluntariness of the interviews.

We are satisfied ASIO has successfully implemented the recommendations made in the IGIS inquiry.

## Inspection of agencies subject to the *Intelligence Services Act 2001*

### Limits on intelligence agencies' functions

The functions of the agencies governed by the *Intelligence Services Act 2001* (the ISA) are set out in sections 6, 6B and 7 of the ISA. For example, for ASIS, its main functions are to obtain, in accordance with the Government's requirements, intelligence about the capabilities, intentions or activities of people or organisations outside Australia; and to communicate, in accordance with the Government's requirements, such intelligence. 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.

### 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 us 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 ASIS, ASD and AGO are to presume that a person located in Australia is an Australian person, and that a person who is located out of Australia is not an Australian person, unless there is evidence to the contrary.

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 was already in possession of evidence that indicated that a person was an Australian person that should have been considered in the initial assessment, or another Australian agency might have possessed that information. In this case the presumption of nationality would be rebutted and if intelligence information had already been communicated about the Australian person there may have been a breach of the privacy rules. There may also be a breach of the ministerial authorisation rules if intelligence collection actually was undertaken.

If the agency made a reasonable assessment of the nationality status of that person, based on all the information that was available at the time, there is no breach of the privacy rules.

Where a presumption of nationality is later rebutted, ASIS, ASD and AGO must advise the IGIS of this and the measures taken to protect the privacy of the Australian concerned.

### Inspection of ASIS activities

During 2015–16, we conducted a broad range of inspections of ASIS activities, including examination of:

- operational files
- ministerial authorisations to produce intelligence on Australian persons
- emergency ministerial authorisations
- ASIS's compliance with the privacy rules
- authorisations relating to the use of weapons.



We also examined ASIS's access to sensitive financial information under the *Anti-Money Laundering and Counter Terrorism Financing Act 2006*. The results of these inspections are set out later in this report.

### Review of operational files

Members of our staff visited ASIS several times each month during 2015–16 to review ASIS's operational case files. ASIS activities involve the use of human sources and ASIS officers are deployed in many countries to support a wide range of activities including counter-terrorism, efforts against people smuggling and support to military operations. These activities are often high-risk and sensitive. During the reporting period, we reviewed files relating to ASIS's operational activities in a diverse range of countries where ASIS has a presence.

These inspections provide a deep insight into the operational environment in which field staff operate, the extent to which staff in ASIS headquarters evaluate risk and guide sensitive activities, and often, an indication of the health of inter-agency relations.

While the sensitive nature of ASIS's operational activities means that we cannot describe in detail the nature and range of issues arising from these inspections in a public report, we can confirm that these reviews are thorough and rigorous.

The insertion of section 13B into the ISA during the previous reporting period allows ASIS to produce intelligence on an Australian person, or a class of Australian persons, in support of ASIO's performance of its functions, without first obtaining authorisation from the Minister for Foreign Affairs. For this power to be enlivened ASIO needs to give ASIS 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. We continued to monitor closely the use of these powers throughout 2015–16, primarily through our regular operational file inspections.

### Ministerial authorisations to produce intelligence on Australian persons

The majority of ASIS ministerial submissions reviewed were of a high standard.

ASIS self-reported that in September 2015, at the request of ASIO, it had passed intelligence information on Australian persons to a foreign liaison without applying the appropriate privacy rules. The information passed included a request for information beyond the current holdings of the foreign liaison on the two Australian persons, without obtaining the appropriate authority to do so. Although we were assured that no intelligence was produced, this activity did not comply with the requirements in sections 8(1)(a)(i) or 13B(1) of the ISA to obtain an appropriate authority to undertake an activity, or series of activities, for the specific purpose, or purposes which include the specific purpose, of producing intelligence on an Australian person.

Under section 10A(2) 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 section 9, 9A or 9B. In November 2015, ASIS advised us of two occasions when it did not advise the Minister within the required three-month timeframe. In both instances, assessments provided by ASIO to ASIS indicated that the individual Australians were deceased, and consequently the grounds for the ministerial authorisation ceased as the person was no longer an Australian person for the purpose of the Act. ASIS also wrote to the Minister for Foreign Affairs and this office providing further details of the matter and the steps taken to mitigate the risk of this reoccurring.

During 2015–16, there were two instances where ASIS sought a renewal of an existing ministerial authorisation that was not signed within the required period for renewal. In each case the renewal was signed the day after the authorisation ceased to have effect, which meant that in practice there was no 'gap' in authorisation.

As a result of queries we raised in a previous reporting period, ASIS advised that it had investigated two historical cases where it had collected intelligence on Australian persons without appropriate authorisation and therefore was not compliant with section 8 of the ISA.

One of those cases involved an agent seeking information from a contact, an Australian person, about the activities of various associates. Although the information collected directly related to non-Australian persons, the information inadvertently also related to the Australian contact.

The other matter related to activities that occurred between 2007 and 2011. Although the sensitive nature of these activities means we cannot detail the nature and range of issues, we are confident that the policies, guidance and training that ASIS has developed since this case, in consultation with this office, are appropriate mitigation strategies to reduce the likelihood of future failures of this kind.

### Emergency ministerial authorisations

No issues were identified with ASIS's use of emergency ministerial authorisations during the reporting period.

Only one emergency ministerial authorisation was issued by the Minister during the reporting period. ASIS notified us promptly in accordance with the formal reporting requirements set out in the ISA.

During 2015–16 ASIS did not use the provision that allows an agency head to give an authorisation in an emergency when the Minister is not available.

### Compliance with privacy rules

During our regular inspection activities we pay close attention to ASIS's distribution of intelligence about Australian persons.

ASIS continued to modify its guidelines and training on producing intelligence on Australian persons, incorporating strategies to mitigate against the risk of unintentionally reporting on Australian persons.

Throughout 2015–16, there were a number of occasions identified where the privacy rules were not applied to reporting on an Australian person

or company due to either human or technical error. In some of these cases, information had been communicated to a foreign liaison without the application of the privacy rules and without approval under ASIS internal policy. Although we identified some of these occasions during routine operational file inspections, most issues were self-reported by ASIS as a result of raised awareness of the issue amongst ASIS staff following increased compliance training.

ASIS reported five occasions in 2015–16 where the 'presumption of nationality' was rebutted; that is, information that an individual was actually an Australian person came to light and the privacy rules were retrospectively applied to reporting. In these instances there was no breach of the rules as the presumption of nationality was reasonable at the time it was applied and the information suggesting the person was Australian was not available at that time.

ASIS advised that during the reporting period there were five cases where, at the request of ASIO, it had passed intelligence information on Australian persons from ASIO to a foreign liaison without applying the appropriate privacy rules. In each instance we were satisfied that ASIS had implemented appropriate remediation measures.

### 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 for 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 2015–16 and we were satisfied that the need for a limited number of ASIS staff to have access to weapons for self-defence in order to perform their duties was genuine.

We conducted an inspection of ASIS weapons and self-defence training records in April 2016. The inspection found that ASIS's governance



and recordkeeping on this matter continued to be effective, with no breaches of the ISA or non-compliance with the ASIS internal weapons guidelines noted during the reporting period.

## Inspection of ASD activities

During 2015–16, we conducted a broad range of inspections at ASD, including examination of:

- ministerial authorisations to produce intelligence on Australian persons
- cancellations and non-renewals of ministerial authorisations
- selected ministerial authorisations for in-depth inspection
- ASD's compliance with the privacy rules
- compliance incident reports.

We also examined ASD's access to sensitive financial information under the *Anti-Money Laundering and Counter Terrorism Financing Act 2006*. The results of these inspections are reported separately later in this report.

### Ministerial authorisations

During 2015–16, we continued to inspect the large majority of ASD's ministerial authorisations to produce intelligence on an Australian person.

In the previous reporting period, we noted that a number of ministerial authorisations that were identified for renewal lapsed for a period of time before being renewed. Legally, intelligence collection activities had to be suspended until a new authorisation was obtained. In the cases reviewed toward the end of the last reporting period, it appeared that this issue was caused by the delay in finalising the submission to the Minister while awaiting information from another agency.

We continued to monitor this issue in 2015–16. While we noted a similar number of occurrences, we are satisfied that ASD, who also administers the ministerial authorisation process for AGO, has appropriate policies and procedures in place to manage the ministerial authorisation renewal process. Requests for the information and documents required in support of the ministerial

authorisation process are made in a timely manner and factor in reasonable time frames for response. We have noted an improvement in the information provided to the Minister in these circumstances, in line with the feedback we provided.

### Ministerial authorisations – cancellations and non-renewals

A ministerial authorisation may be cancelled by the Minister as a result of a change of circumstances or it may expire at the end of the authorisation period. In either case, there is a requirement for agencies to report to the Minister within three months on activities conducted in accordance with the authorisation.

During the 2015–16 reporting period, we identified an issue in relation to the detail provided to the Minister in post activity reporting for both ASD and AGO. We are satisfied that in each case this was an isolated occurrence and was not indicative of any systemic problem. This matter is also reflected in our reporting below in relation to AGO.

### Ministerial authorisations – in-depth inspections

During the reporting period, we commenced a new process of in-depth reviews on a small sample of ministerial authorisations. These in-depth reviews looked at the internal procedures of ASD teams for developing and reviewing the submissions which are ultimately presented to the Minister, the detail of the supporting intelligence, and the accuracy of this information as presented to the Minister.

In one of the matters reviewed, we noted that one aspect of the reporting relied upon in a submission to the Minister was significantly older than the remainder of the reporting without making this distinction clear to the Minister. We considered that this was not material to the decision made by the Minister in this instance. Nevertheless, to ensure that the Minister is provided with a clear and accurate understanding of the situation described, we recommended that any significant difference in the currency of the information relied on should be brought to the attention of the Minister. ASD has accepted this recommendation.

Another in-depth review identified that a key preliminary decision was not made in accordance with the normal procedure. This decision was reviewed and we were satisfied that, despite the departure from normal procedures, the decision was made in a manner consistent with ASD's obligations under the ISA and the intention of internal policies. The preliminary decision making process in another matter highlighted varied interpretations, at the working level, of how to assess whether or not ASD had a purpose to produce intelligence on an individual.

Noting the issues highlighted by these reviews, we commenced a regular inspection of ASD's preliminary decision making processes in relation to ministerial authorisations. These inspections have not identified any issues of concern.

### **ASD compliance with privacy rules**

In accordance with its obligations, ASD continued to report to the IGIS cases where a presumption that a person was not Australian had later been found to be inappropriate, and the measures taken to protect the privacy of the Australian person involved.

In all cases where a presumption that a person was not Australian was made and rebutted at a later date, we considered that the application of the presumption was reasonable based on the information available to ASD at the time. The actions taken by ASD, including actions to ensure that other intelligence agencies were informed that the subject was an Australian person, were appropriate and consistent with the privacy rules. We made one recommendation to ASD in relation to the detail contained in its reporting of rebuttals of presumptions of nationality. This recommendation was accepted and implemented during the reporting period.

### **Compliance incident reports**

There were a small number of compliance incident investigations ongoing at the time the previous IGIS annual report was prepared. These matters were finalised in this reporting period and have been incorporated in to this report.

In April 2015, ASD advised the IGIS that it had failed to report activities conducted in accordance

with a ministerial authorisation within the three month reporting timeframe stipulated by the ISA. An internal review was conducted and a report provided to the IGIS in October 2015. The circumstances of the incident were unique, highly sensitive, and while a formal report was not provided within the required timeframe, ASD had informally engaged with the Minister and the Minister's office in relation to the authorised activity. A formal report to the Minister was provided a short time later. A similar breach of the same ISA requirement occurred in March 2016, again in relation to a highly sensitive matter. While we are satisfied that the circumstances of each of these incidents were unique, we are pleased that ASD is revising its internal procedures in relation to the management of highly sensitive authorisations to reduce the likelihood of any further breaches of this requirement.

In February 2016, ASD advised that on three occasions it had conducted activities with the purpose of producing intelligence in relation to an Australian person without prior authorisation from the Minister for Defence and therefore in breach of the ISA.

On one occasion, a failure to take into account all of the information available resulted in the conduct of an unauthorised activity. This error in ASD's preliminary processes was identified internally and reported to our office.

The second incident involved the continuation of an activity beyond the expiry of the ministerial authorisation. ASD had taken steps to cease its activities in advance of the expiry of the authorisation, however, because of a failure in internal processes, one aspect of its activities continued for an additional four days. ASD advised that internal guidance and procedures will be updated to address these failures in process. We will continue to monitor the implementation of the recommendations arising from these incidents.

The third matter was identified by an internal audit, which detected an historical breach of the ISA. This incident occurred between 2010 and 2014 as a result of a failure by ASD to follow appropriate record keeping practices, an issue that we previously reviewed and reported on in more detail in the 2013–14 Annual Report. We are

pleased that ASD has continued with a proactive process of internal review and continues to report legacy issues to us where they are identified. We are satisfied with the additional technical safeguards implemented by ASD in conjunction with compliance guidance and training for staff in relation to this type of record keeping.

In May 2015, ASD became aware that individuals who were not authorised under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) had conducted a testing activity. ASD's internal investigation of this breach was not finalised until early in this reporting period. The investigation determined that the personnel involved in the activity were aware of the legislative requirements and had assumed that the required authorisation was in place. In response to this breach ASD decided that a dedicated officer would be appointed within the areas that conduct testing activities to oversee compliance with legislative and policy requirements. These appointments are being made and we are regularly involved with the training of appointees. ASD has also updated its internal guidance to reflect the lessons learnt. We are satisfied with the management of this incident and the actions taken to prevent reoccurrence.

Where the Attorney-General gives a testing authority under the TIA Act, ASD is required to provide a report on activities conducted under the authority within three months of expiration. In May 2015, ASD identified that a report had been prepared within the required timeframe, but because of a series of administrative errors, the report was not submitted until two months after the reporting deadline had passed. ASD highlighted the breach of the TIA Act reporting requirements to the Attorney-General when the report was submitted. ASD conducted an internal review of this matter and provided a report to us in August 2015. We are satisfied with the improvements made to ASD's internal administrative arrangements in response to this incident and have observed that all subsequent reports for this reporting period have been submitted within the required timeframe.

ASD also advised us that, in September 2015, it had collected intelligence in breach of the TIA Act. The

breach was identified internally and immediate action was taken in response. The breach was the subject of an internal investigation, which we reviewed. The internal investigation determined that an analytical oversight was the cause of the breach. We agree with this assessment and are satisfied that there were no underlying systemic issues that contributed to the incident. We are satisfied that ASD has taken appropriate steps, including updates to internal training, to prevent a similar oversight in the future.

## Inspection of AGO activities

During 2015–16, we conducted a broad range of inspections at AGO, including examination of:

- Director's approvals of intelligence collection activities in relation to Australian territory
- ministerial authorisations to produce intelligence on Australian persons
- cancellations and non-renewals of ministerial authorisations
- AGO's compliance with the privacy rules.

During the reporting period, the Inspector-General conducted a visit to AGO's Bendigo facility and met with staff to discuss the capabilities and the scope of ongoing work to be conducted from Bendigo.

We also examined AGO's access to sensitive financial information under the *Anti-Money Laundering and Counter Terrorism Financing Act 2006*. The results of these inspections are set out later in this report.

## Director's approvals and post activity reporting

The Minister for Defence requires the Director of AGO personally to approve AGO intelligence collection activities undertaken in relation to Australian territory. The Director of AGO provides a report on these authorisations to the Minister for Defence quarterly. Additionally, a post activity compliance report is provided to the Director of AGO in relation to each approval. Our staff reviewed a significant sample of the post activity compliance reports provided to the Director of AGO during the reporting period.

The approval provided by the Director is often subject to conditions. During 2015–16, we identified two issues in relation to compliance with the conditions imposed by the Director. An administrative oversight in the drafting of one approval resulted in the imposition of a condition that was inconsistent with the intent of the Director's approval. In another matter, the post activity compliance report did not specifically refer to compliance with the conditions imposed. A review of a sample of the activities conducted under the approval confirmed that the conditions had been met. AGO have accepted the recommendations our office made regarding its administrative processes in relation to conditions imposed on an approval by the Director and we are satisfied that AGO's subsequent actions are appropriate to address this issue.

### Ministerial authorisations

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 2015–16, we inspected the large majority of AGO's ministerial authorisations.

Late in the 2014–15 reporting period, AGO advised us that a draft intelligence report had been developed on the basis of information voluntarily provided by an Australian person prior to the Minister giving an authorisation. The internal review of this matter was concluded in July 2015 and reported to us. It was identified that appropriate internal policies and procedures were in place but had not been followed. We noted that AGO staff identified the issue on the same day the draft report was developed. We consider that the remedial actions taken were appropriate in the circumstances.

Our office made one recommendation in relation to this matter which was accepted by AGO.

### Ministerial authorisations – cancellations and non-renewals

A ministerial authorisation may expire at the conclusion of the authorisation period or be cancelled by the Minister as a result of a change of circumstances. In either case, there is a

requirement for agencies to report to the Minister within three months on activities conducted in accordance with the authorisation.

During the 2015–2016 reporting period, we identified an issue in relation to the detail provided to the Minister in post activity reporting for an authorisation for both AGO and ASD. We are satisfied that this was an isolated occurrence and not indicative of any systemic issues. This matter is also reflected in our reporting in relation to ASD above.

### AGO compliance with privacy rules

The Minister for Defence makes written rules designed to ensure the privacy of Australian persons or entities where intelligence has been collected about them. These rules regulate the communication and retention of intelligence information in relation to Australian persons and entities.

During the reporting period, AGO identified a historical breach of these rules, promptly notified us and conducted an internal review. In satisfying ourselves that the remedial action taken by AGO in relation to this matter was appropriate, we considered the developments in AGO internal policies and training since the breach occurred, as well as the specific response to this incident.

While working on a task in support of another intelligence agency during the 2015–16 reporting period, AGO revised nationality assessments for companies but did not advise their partner agency. We commend AGO's diligence in continuing to reassess issues of nationality as new information becomes available, but it is important that, where appropriate, this information is shared between agencies to ensure that there is a consistent approach to compliance and the protection of the privacy of Australian persons. AGO have accepted our recommendations on this issue.

### Inspection of DIO activities

As has been the practice of this office over a number of years, during the reporting period we continued to exercise a 'light touch' inspection regime with respect to DIO. Our rationale for this

is that, as DIO is an assessment agency (that is, it does not directly collect intelligence information), its activities are far less likely to intrude into the personal affairs of Australian persons than the activities of intelligence collection agencies.

During 2015–16, we conducted inspections examining:

- DIO's compliance with its privacy guidelines
- a range of sensitive assessments published by DIO which are distributed to key decision makers
- special briefings.

We also examined DIO's access to sensitive financial information under the *Anti-Money Laundering and Counter Terrorism Financing Act 2006*. The results of these inspections are reported separately later in this report.

### Compliance with privacy guidelines

We aim to review the compliance of DIO with its privacy guidelines at least twice a year. In 2015–16 we undertook two such inspection visits to review relevant DIO records.

These inspections revealed that DIO is generally compliant with the requirements of its privacy guidelines and that the agency continues to take its privacy responsibilities seriously.

To the extent that non-compliance issues were identified, these tended to be relatively minor and administrative in nature and there was no evidence that intelligence was passed in breach of the guidelines.

In addition to our bi-annual inspection visits, DIO will, as circumstances demand in individual cases, seek a waiver from the Inspector-General to vary the way in which it records instances where the DIO privacy guidelines have been invoked to justify the disclosure of intelligence information about an Australian person.

These requests are typically made when it is anticipated that the information in question is likely to be time critical, and passage of that information to intended recipients should not be delayed while usual processes are followed. The IGIS granted four such waivers during the reporting period. Relevant records were kept

and reviewed in each instance, and no issues of concern were identified.

### Other inspection activities

As an assessment agency, DIO produces a range of products that contain its assessments of various topical and enduring issues. The IGIS monitors this output, with a view to informing our periodic reviews of the analytical integrity of DIO's products.

The Inspector-General is not empowered to receive complaints about DIO, however, if made aware of matters that would reach our office's complaint threshold, the Inspector-General has the capacity either to make administrative inquiries of DIO, or where appropriate, to initiate an 'own motion' inquiry.

The Inspector-General became aware of a complaint that was aired in the media in the second half of the reporting period. The complaint alleged that during a training event a number of years earlier, several DIO military personnel had been involved in conduct raising issues of concern. The matter was investigated by this office however the IGIS concluded that there was insufficient basis to justify an inquiry.

### Inspection of ONA activities

We also exercised a 'light touch' inspection regime with respect to ONA during the reporting period. We did so because ONA is an assessment agency and its activities are consequently less likely to intrude upon the personal affairs of Australian persons than those of the intelligence collection agencies.

During 2015–16, we conducted inspections examining:

- ONA's compliance with its privacy guidelines
- a wide range of sensitive assessments published by ONA which are distributed to key decision makers
- special briefings.

We also examined ONA's access to sensitive financial information under the *Anti-Money Laundering and Counter Terrorism Financing Act 2006*. The results of these inspections are reported separately later in this report.

### Compliance with privacy guidelines

We intend to review the compliance of ONA with its privacy guidelines by reviewing its relevant records at least twice a year. In 2015–16, we undertook two such inspections.

The first of these inspections identified a number of interpretative and administrative errors. While this was concerning to us, it should be noted that none of these errors led to intelligence information about an Australian person being disseminated without there being an appropriate underlying basis for doing so.

As a consequence of this first inspection activity, ONA instituted a number of process changes to its business rules for the completion of privacy guidelines compliance sheets. ONA also put in place a centrally located quality assessor to ensure that the guidelines are properly interpreted and applied.

More rigorous justifications are now provided in those instances where it is necessary to refer to Australian persons in ONA products and communications. Following these changes, our second inspection of the year found no errors of any consequence.

In addition to these changes, the Director-General of ONA has initiated a review of ONA's existing privacy related guidance and is developing a revised training package to be delivered to relevant staff. We commend the positive and responsible response of the Director-General of ONA to our earlier inspection concerns.

### Other inspection activities

ONA produces a wide range of products that contain its assessments of various topical and enduring issues. The IGIS monitors this output, with a view to informing our periodic reviews of the political independence of the assessments contained in ONA's products.

### Cross-agency inspections

During the reporting period, we 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 carrying out their functions. The legislation protects authorised officers from civil and criminal liability where they use an assumed identity in circumstances that would otherwise be considered unlawful. Similarly, the legislation protects the Commonwealth, State and Territory agencies responsible for providing 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. This includes the *Crimes Act 1914* section 15LG requirement that ASIO and ASIS each conduct six monthly audits of assumed identity records; and the section 15LE requirement that each agency is to provide the IGIS with an annual report containing information on the assumed identities created and used during the year. The Director-General of Security and the Director-General of ASIS provided us with reports covering the activities of their respective agencies for the 2014–15 reporting period. There was nothing in the reports to suggest that the agencies were not complying with their legislative responsibilities, or which otherwise caused concern.

### Cyber project

During the reporting period, we conducted an inspection project focused on a specific intelligence operation conducted jointly by a team of ASD and ASIS personnel. The project reviewed the operation from the identification of the intelligence requirement, through to the planning, approval and conduct of the operation. We were satisfied that the operation was conducted appropriately and in accordance with the law. The records of the operation showed that key decisions made throughout the conduct of the operation and the reasons for those decisions were soundly based.

A focus of our future activities will be revising our inspection activities in light of the increasing resources available to ASD under the 2016



Defence White Paper and Cyber Security Strategy. The allocation of our resources must be responsive to organisational and capability changes within the agencies.

### Foreign Intelligence Collection review

During the reporting period, we undertook a project to review a sample of completed Foreign Intelligence Collection (FIC) warrants (including warrants requested, executed and reported). This inspection project involved a whole of Australian Intelligence Community FIC warrant inspection. The project accessed information from ASIO, ASD, ASIS and ONA. We noted that some of the information provided to us by some of the agencies was out-dated or not comprehensive.

The project found that, overall, the FIC warrant process is managed well and there were no substantial issues of concern. The IGIS recommended the agencies involved ensure that comprehensive and up-to-date guidance is available for all staff involved in the FIC warrant process.

### Joint teams

We completed a project during 2015–16 to increase our understanding of governance arrangements for joint teams and joint positions involving one or more Australian intelligence agencies. Two joint teams were selected for the project. We were comfortable with the processes and systems in place for recording details of information exchanges, however, the project found that each joint team is quite different. For that reason it is difficult to reach any broad conclusions or draw comparisons between the governance arrangements without undertaking an extensive review of a range of joint teams. Resources permitting, this is a possible area for future projects or inspections.

### Work Health and Safety Project

During the reporting period, our office considered how ASIO and ASIS applied section 12C of the *Work Health and Safety Act 2011* (the WHS Act). This section enables these agencies, in the course of maintaining Australia's national security, to exempt themselves from certain reporting required by the

WHS Act. Our inspections extended to examining any records, reports, policies and guidelines relevant to the exemption.

Both ASIO and ASIS have written declarations outlining circumstances in which the exemption could be applied, focusing, among other things, on exempting reporting and post-incident investigations in order to protect national security material. Both declarations detail exemptions and modifications of certain other provisions within the WHS Act.

We found that both declarations and the accompanying policies and procedures were sound and appropriate.

### 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 within 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 our office are designated agencies for the purposes of the AML/CTF Act.

In 2012, the Inspector-General entered into a memorandum of understanding with AUSTRAC in relation to monitoring the intelligence agencies' access to, and use of, AUSTRAC information.

In overseeing the agencies' use of AUSTRAC information, we check that there is a demonstrated intelligence purpose pertinent to the agencies' functions, that access is appropriately limited, searches are focussed, and information passed to both Australian agencies and foreign intelligence counterparts is correctly authorised.

During 2015–16, in accordance with the memorandum of understanding, the IGIS reported to the responsible ministers on the outcome of compliance monitoring activities in each of the agencies concerning their access to, and use of, AUSTRAC information in the previous reporting period.

In 2015, we conducted an inspection project to examine how ONA, ASIS and ASIO, as part of their in-house vetting, obtained approval to access financial information from the co-holder of a jointly held account. Advice was also sought from the Australian Government Security Vetting Agency for comparison purposes. In summary, the project found that all agencies sought approval from a co-holder to access jointly held financial information.

### ASIO

We conducted regular inspections of ASIO's access to AUSTRAC material during 2015–16. In our previous report we noted our ongoing interaction with ASIO regarding two inconsistent internal policies relating to the setting of search limitations. This issue was subsequently resolved.

During our inspections we identified only a limited number of compliance issues. These issues included:

- typographical errors in ASIO's searches of an AUSTRAC database, such as misspelling a name
- AUSTRAC information provided to the requesting officer that exceeded the parameters of the request.

These issues were addressed appropriately by ASIO staff.

### ASIS

We conducted inspections of ASIS records in September 2015 and March 2016. The inspections found that ASIS's governance and recordkeeping on this matter continued to be effective, with no breaches of the ISA or non-compliance with the ASIS guidelines in relation to the use of AUSTRAC material noted during the reporting period.

### ASD

Our AUSTRAC inspection activities in relation to ASD during 2015–16 were facilitated by an annual compliance statement provided to our office by

ASD. Our inspection activities identified no issues of legality or propriety in relation to ASD's access to or use of AUSTRAC information. ASD has clear internal guidance in place for the management and use of AUSTRAC information, which were complied with during the reporting period.

### AGO

Our AUSTRAC inspection activities in relation to AGO during 2015–16 were facilitated by an annual compliance statement provided to our office by AGO. Our inspection activities identified no issues of legality or propriety in relation to AGO's access to or use of AUSTRAC information.

### DIO

Our AUSTRAC inspection activities in relation to DIO during 2015–16 were facilitated by a comprehensive internal review conducted by DIO. We noted one breach of the AUSTRAC-DIO memorandum of understanding during the reporting period in relation to the dissemination of information to an official within DIO who did not work within one of the designated analytic branches authorised to receive AUSTRAC data. We are satisfied that steps are being taken, through the implementation of internal guidance and the renegotiation of the memorandum of understanding with AUSTRAC, to reduce the chance of reoccurrence. We will continue to monitor the suitability of these measures through annual inspection activities.

### ONA

We identified no significant concerns with ONA's access to and use of AUSTRAC related data during the reporting period. Where issues of a compliance nature were identified, we were satisfied that steps were being taken, through the implementation of internal guidance, to reduce the chance of reoccurrence. We will continue to monitor the suitability of these measures through annual inspection activities.



# Activity 3: Responding to complaints

*Providing effective and timely responses to complaints or referrals received from members of the public, ministers or members of parliament*

## Introduction

Most of the communications our office receives are treated as ‘contacts’ or ‘complaints’.

We consider a matter to be a ‘contact’ where the issues raised are clearly not credible, where they are not intelligible, where they fall outside of the jurisdiction of the office, or where the communication is relevant to the office but is not a complaint (e.g. requests for information about the office or the Australian intelligence community).

We consider a matter to be a ‘complaint’ if it raises an initially credible allegation of illegality, impropriety or abuse of human rights, in relation to an action of an intelligence agency. Complaints can be made orally or in writing, however there is no obligation on the Inspector-General to pursue complaints that are not made in writing if this has been requested.

Each communication is assessed to determine whether it falls within the jurisdiction of the office and, if so, the most appropriate course of action. Where it is assessed that a communication is a complaint that justifies further action, it will be handled administratively in the first instance. All contacts and complaints are also assessed to determine whether they should be handled under the Public Interest Disclosure (PID) scheme.

In most cases, complaints and other matters can be resolved quite 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 reduces the procedural burden of an inquiry. Administrative resolution can allow for a timely response to be provided to the complainant. Information provided by agencies in this way can help the IGIS determine whether to conduct an inquiry for more serious or complex matters.

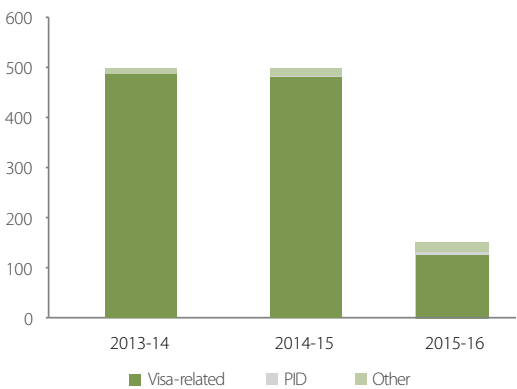
Irrespective of how a matter is handled, all persons contacting the office are advised of the actions taken, and the outcomes, to the maximum extent possible, consistent with the office’s overriding security obligations.

## Quantitative performance measures

The following metrics, identified in the *OIGIS Corporate Plan 2015–19*, were used to support the quantitative assessment of our performance in relation to this activity:

- number of complaints received and handled
- target percentage (90%) of complaints acknowledged within five business days, and 85% of visa-related complaints resolved within two weeks.

**Figure 3.3: Number of complaints by year and type**



**Figure 3.4: 2015–16 complaints (including PID) by agency and source**

Complaints by agency and source	ASIO	ASIS	ASD	AGO	DIO	ONA
Number of complaints	139	4	3	0	1	0
From public	137	3	0	0	1	0
From intelligence agency employee or ex-employee	2	1	3	0	0	0

**Figure 3.5: Performance against complaint acknowledgement and resolution targets**

Complaint type	Total number of complaints	Percentage acknowledged within 5 business days (Target: 90%)	Percentage of visa-related complaints resolved within two weeks (Target: 85%)
Visa-related	118	97%	72%
PID	4	100%	n/a
Other	25	88%	n/a
<b>TOTAL</b>	<b>147</b>	<b>95%</b>	<b>72%</b>

In the 2015–16 reporting period, the IGIS received 147 complaints that justified action. Of these, four were assessed as meeting the threshold to be handled under the PID scheme; 118 complaints were about delay with visa-related security referrals; and 25 raised other concerns about the activities of the Australian intelligence agencies.

This represents an overall decrease in complaints received by the office over the last three years. The decrease is solely attributable to the significant drop in complaints about delay in visa-related security assessments.

### Complaints about security referrals for visa applicants

In 2015–16 there was a significant drop in the number of visa security referral related complaints. In 2014–15, the office received 473 visa security referral related complaints. In 2015–16, the office received 118 such complaints, an average of 10 complaints per month. The drop in complaints is considered to be most likely as a result of changes in national security considerations and other factors for which this office is not responsible. The majority of complaints were in relation to visa security assessments (94 per cent).

As with previous years, the largest number of complaints made to the office came from individuals seeking skilled business or work visas (49 per cent). There was also a substantial number of complaints relating to family reunion visas (20 per cent) and protection or refugee visas (21 per cent). The office also received a small number of complaints relating to security assessments in relation to applications for Australian citizenship.

The main complaint about visa security referrals is delay. Most of the factors that lead

to delay are outside the control of the relevant intelligence agencies.

During the reporting period, we acknowledged 97 per cent of visa-related complaints within five working days, well above our performance indicator of 90 per cent.

We consider a complaint about delay in visa security assessments to be resolved once we have completed our administrative inquiries and responded to the complainant. On average, we resolved visa-related complaints within 12 days, however while the office aimed to resolve 85 per cent of visa-related complaints within two weeks, we were only able to resolve 72 per cent of visa-related complaints within this period. This was due to complex circumstances of some of the visa security assessments that were reviewed by our staff.

### Other complaints

We received 25 non visa-related complaints in the reporting period (excluding PID matters), marginally higher than the 23 we received in 2015–16. Nineteen complaints in this reporting period concerned ASIO, four related to ASIS, one to ASD and one to DIO.

The average time taken to acknowledge other complaints in the reporting period was 2.9 business days. We responded to 88 per cent of complaints within five business days, just outside our performance goal of 90 per cent. The three complaints that were acknowledged outside the five day performance measure exceeded the measure by a maximum of two days. Delay in the three cases was unavoidable, caused by the need to translate documents into English before responding (one complaint), and an intention to

provide an acknowledgement and substantive response in a single communication being hampered by unexpected delays in receiving external inputs (two complaints).

Of the 25 complaints received in the reporting period, twenty three were closed at the end of the reporting period, with an average of 37 days until a final response was sent.

### Other contacts with the office

We also received around 325 contacts from individuals seeking advice or expressing concern about matters affecting them that were assessed to be outside the jurisdiction of the office, or as lacking credibility. This compares with approximately 300 such contacts in 2014–15, and around 200 contacts in 2013–14.<sup>6</sup>

This continued increase in the number of contacts may be attributable to the increased focus on intelligence related matters in public discourse and in the media, greater awareness of the existence of this office, and public debate about the powers and surveillance capabilities that are available to the intelligence agencies.

When we are contacted in the above circumstances, we provide written or oral advice about the jurisdiction of the office and alternative avenues to pursue, 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, we take no further action unless substantially new and credible information is provided.

## Discussion

### Visa-related security referrals

ASIO provides Commonwealth agencies with security assessments relevant to their functions and responsibilities. A visa application to travel to, or remain in, Australia may be referred to ASIO with a request to provide a security assessment. We do not assess the merits of any particular

security assessment, nor do we request a change in the priority in which cases are processed, either in general or in particular. In contrast, however, where visa applicants have raised reasonable concerns that an error may have occurred, we examine ASIO's processes.

For approaches about visa-related security assessments, we consider the length of time ASIO has had to respond to a request for a security assessment before determining if the matter should be treated as a complaint or a contact. Specifically, we consider if the visa application was submitted more than 12 months earlier, or whether six months have passed since any previous enquiry about that application was made. Approaches about visa-related security assessments that do not meet these criteria are counted as 'contacts' (see above).

### Visa-related complaints

During 2015–16, we continued to focus on ASIO's handling of visa security assessments because of the significant impact this can have on individuals. We note, however, that delays in the processing of visas can arise from factors outside ASIO's control and not related to ASIO's handling of security assessments. We continued to access ASIO's systems directly as well as to increase liaison with other government stakeholders, including the Department of Immigration and Border Protection (Immigration) and the Office of the Commonwealth Ombudsman.

In one case, we received a complaint from a visa applicant whose case had been remitted to Immigration by the Refugee Review Tribunal. Following our inquiries, Immigration determined that an administrative oversight by its visa processing area had caused the delay in ASIO performing the visa-related security assessment. Immigration advised this office and ASIO of the oversight and took steps to rectify the situation.

While reviewing another complaint, our office found that the complainant's representative was no longer registered as a migration agent. The Office of Migration Agents Registration Authority (OMARA) had found that the complainant's representative was not a fit and proper person to give immigration assistance and accordingly cancelled the representative's registration. Our

<sup>6</sup> Individuals who contacted the office on multiple occasions are counted as a single 'contact' in these figures.

office liaised with Immigration's National Security Branch and OMARA, and subsequently advised the complainant of the agent's deregistration.

### Other complaints

All 25 'other' complaints received during the reporting period were investigated administratively, rather than by means of a formal inquiry.

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

- the execution of, or legal basis for, search warrants and related interactions with ASIO
- failure to provide a duty of care to an individual who previously assisted ASIO
- discrimination and harassment based on race
- inappropriate access to information
- security assessments for passports and employment
- delays in security checks for Aviation Security Identification Card (ASIC) and Maritime Security Identification Card (MSIC).

All complainants were given advice about the action we had taken in response to their complaints. This included details about our examination of agency records and consideration of agency briefings, and our degree of confidence in the legality and propriety of agency actions. Where appropriate, complainants were also invited to make further contact with us if their concerns persisted.

Three complainants received prompt, practical remedies as a result of their complaints to the IGIS. In the first case, the remedy included an apology from the agency concerned and improvements to agency systems. In the second, relating to an ASIO search warrant, ASIO attended the complainant's home and addressed the concerns personally. The third case was resolved when ASIO was able to finalise its security assessment after particularly urgent concerns were brought to its attention.

We do not contact complainants to ask about their level of satisfaction with our handling of their complaint. In 2015–16, few complainants contacted us after the finalisation of their complaint to express

either disappointment or satisfaction with the outcome.

On the other hand, people raising matters that were outside the jurisdiction of the office or lacked substance frequently expressed their frustration that we had not pursued their concerns.

In all cases, we provide advice about our role, and the role and functions of relevant Australian intelligence agencies. Where we do not directly address specific concerns, we provide details of suitable alternative avenues to pursue, if this is appropriate.

Further details of some of the complaints we investigated are contained in the case studies below. The complaints that were assessed as falling within the PID scheme are discussed in the following pages.

### 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 this reporting period the AHRC referred two cases to the IGIS. Broadly these cases alleged that:

- surveillance by ASIO was racially motivated, contrary to the complainant's human rights as set out under the United Nations *International Covenant on Civil and Political Rights* (ICCPR)
- surveillance by ASIO amounted to an inappropriate interference in the complainant's personal affairs, contrary to the ICCPR.

In the first of these referred matters, we did not find any evidence to support the complainant's claims.

In the second case, we explained the role and functions of ASIO, and the role of the IGIS in overseeing ASIO's functions (as the complainant seemed confused about these matters). The complainant was also invited to provide additional information in support of the claims. As the complainant did not reply, and there was insufficient cogent information contained in the initial complaint, the Inspector-General decided that further inquiry into the matter would be futile.

## Case study 1: Execution of an ASIO search warrant

An individual whose family home had been the subject of an overt ASIO entry and search warrant made a complaint alleging that her home had been left in a disordered state at the end of the search. The complainant also said ASIO had provided a copy of its seizure list that was too faint to read and it was impossible to identify the items ASIO had taken.

We raised the matter with ASIO. We also reviewed the relevant files, and noted that a video recording of the search had not been made because of faulty equipment.

As well as providing details to the IGIS about the execution of the search warrant, ASIO officers promptly visited the complainant's residence. The complainant refused the officers entry to the property and therefore they were not able to inspect it for the alleged damage. In the circumstances, ASIO offered, and the complainant accepted, a sum of cash sufficient to pay for professional carpet cleaning, as well as a legible copy of the seized goods list.

## Case study 2: ASIC/MSIC cases

During the reporting period, we maintained an interest in ASIO's processing of security assessments for Aviation Security Identification Cards (ASIC) and Maritime Security Identification Cards (MSIC).

As we reported last year, some cases can be subject to lengthy delays, and we sought further briefings on ASIO's management of these assessments. ASIO provided information about how cases are prioritised and allocated for assessment.

We received eight complaints about ASIO's handling of these cases. All related to significant delay. In the course of investigating one complaint we obtained further details of the person's personal circumstances which caused us concern. When ASIO was made aware of these circumstances, their response was prompt and the matter was resolved.

## Case study 3: Recruitment complaints

We received two complaints from persons formerly employed within the Australian intelligence community (AIC) who raised concerns about recruitment processes when they sought engagement within the AIC. Both complaints related to how AIC agencies took account of each applicant's employment and security-related history within the AIC in determining their suitability for further employment.

In the first case, the agency identified that its approach to the complainant's application for a return to employment, following his resignation some years earlier, was not given appropriate or fair consideration. The agency took steps to address these concerns, including by providing a written apology to the complainant. It also revised its processes to ensure fair and balanced consideration of relevant information in this and all future applications.

The second complaint related to information exchange between AIC agencies. As it also raised other matters, the complaint was treated as a Public Interest Disclosure. IGIS considered whether the agencies concerned had followed relevant security guidelines such as those set out in the Protective Security Policy Framework. The complaint remained open as at 30 June 2016.

## Activity 4: Public Interest Disclosures

*Facilitating the investigation of public interest disclosures and undertaking other responsibilities under the PID Act*

### Introduction

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 dealt with.

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.

### Quantitative performance measures

The following metrics, identified in the *IGIS Corporate Plan 2015–19*, were used to support the quantitative assessment of our performance in relation to this activity:

- number of public interest disclosure matters handled
- target percentage (90%) of complaints acknowledged within five business days.

These metrics have been reported on in the preceding section of this annual report (Activity 3), alongside the metrics for other types of complaints.

In summary, there were four Public Interest Disclosure matters handled during the reporting period, each of which was acknowledged within five business days.

### Discussion

In the reporting period four disclosures were made to the IGIS under the PID scheme.

One of these disclosures was made by an anonymous complainant who alleged that members of a small work unit in an Australian Intelligence Community (AIC) agency were secretly monitoring the internal communications of their workplace colleagues. They were said to be using information accessed as a source of gossip and potential influence.

Although the complaint was anonymous, it contained sufficient inside knowledge of the agency in question to suggest that it came from a current public official. The matter was construed as reaching the PID threshold and formally allocated to the Inspector-General for investigation.

The anonymous nature of the complaint and its lack of specificity (for example, with regard to the names of purported offenders and date ranges) made it difficult to investigate. Despite this, a number of forensic technical checks were undertaken to identify any inappropriate conduct or unusual patterns. None were found.

The second matter considered to be a disclosure was a complaint made by a serving AIC officer who had been suspended on full pay pending the formal withdrawal of the officer's security clearance and the termination of the officer's employment.

The discloser claimed that the 'review for cause' investigation which had led to the recommendation to withdraw the security clearance had been so flawed as to amount to a denial of procedural fairness, and that, for this reason, the decision should be overturned.

## Public Interest Disclosure

One PID (the third received by this office) revolved around claims by a former AIC agency employee that he should not have been permitted to attend specialist training in sensitive techniques relevant to his then employment, if he was already the subject of a 'review for cause' security investigation into his continued suitability to hold a security clearance. It was construed that the discloser had raised serious concerns of maladministration, and the matter was allocated to the IGIS for investigation.

Following investigation, the IGIS was satisfied that the complainant was not actually the subject of a formal 'review for cause' process prior to the commencement of the relevant training. Rather, the process was commenced one week after the course was concluded.

The IGIS found that while security related concerns had been raised about the complainant in the preceding weeks, the agency had sought to find a reasonable balance between maintaining appropriate and necessary security standards and treating the complainant in a fair and reasonable manner.

After reviewing relevant material, the IGIS identified no procedural flaws and decided that the decision of the agency head to withdraw the discloser's security clearance was not unreasonable in the circumstances.

The final internal disclosure made directly to the Inspector-General came from a former AIC agency officer who raised concerns about the manner in which a code of conduct investigation was carried out; alleged workplace bullying and harassment; and whether the agency concerned had inappropriately communicated personal information about the discloser to AIC and other agencies with a view to exclusion from future employment.

This matter was regarded as a PID on the basis that the disclosure pointed to potential maladministration and actions which, if proven, could give rise to disciplinary action. Although the matter was still open at the end of the reporting period, it was finalised very shortly afterwards. The IGIS found no evidence to support the claims made by the discloser.

The office was also very heavily involved in providing comments and input to the statutory review of the PID Act, which was conducted by Mr Philip Moss AM in the second half of the reporting period. This is discussed in more detail under Activity 5 in this report.

## Activity 5: Advice to parliamentary committees and others

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

### Introduction

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

### Quantitative performance measures

There were no quantitative performance measures identified in the *OIGIS Corporate Plan 2015–19* that were directly applicable to the advice we provided to parliamentary committees and similar bodies.

During the reporting period the IGIS appeared at two parliamentary committee hearings, provided two written submissions to a parliamentary committee, reviewed material presented to a coronial inquest and contributed to an independent statutory review of the *Public Interest Disclosure Act 2013*.



## Discussion

### Senate estimates hearings

The Inspector-General appeared before the Senate Standing Committee on Finance and Public Administration on 22 February 2016 during the 2015–16 Additional Estimates hearings.

### 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 2015–16:

- on 10 December 2015 the IGIS made a submission to the *Inquiry into the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015*
- on 20 January 2016 the IGIS made a submission to the *Review of Administration and Expenditure No. 14 (2014–15)* and appeared before the committee at a private hearing on 5 May 2016.

### Lindt Café siege coronial inquest

The Inspector-General has reviewed evidence put to the coronial inquest into the Lindt Café siege being presided over by the New South Wales State Coroner, Magistrate Michael Barnes. The purpose was to determine if there was a need for this office to investigate any aspect of the matters. No such need was identified.

### Statutory review of the Public Interest Disclosure Act 2013

The Government appointed the former Integrity Commissioner, Mr Philip Moss AM, to conduct a review of the *Public Interest Disclosure Act 2013* (PID Act) on 15 January 2016. This appointment was made in accordance with the requirement of section 82A of the PID Act, that a review of the operation of the PID Act be undertaken two years after it had commenced.

Mr Moss invited the Inspector-General to contribute to this review, as the IGIS is an investigative body for the purposes of the PID Act and is also responsible for overseeing the operation of the scheme in the Australian Intelligence Community (AIC).

The IGIS lodged a submission on 18 March 2016. A copy of the IGIS submission can be found on the IGIS website [www.igis.gov.au/public-statements/submissions](http://www.igis.gov.au/public-statements/submissions).

The submission reflected the thoughts of the Inspector-General on practical issues and concerns with the operation of the PID Act in its first two years of operation, as well as comments and input from AIC agencies.

The Inspector-General and relevant staff were also consulted by Mr Moss and his secretariat as they developed their final report.

## Activity 6: Evidence to the AAT and the Australian Information Commissioner

*Providing evidence to the Administrative Appeals Tribunal and the Australian Information Commissioner as required*

### Introduction

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 Australian 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.

### Quantitative performance measures

There were no quantitative performance measures identified in the OIGIS Corporate Plan 2015–19 that were directly applicable to the evidence we provided to the AAT and the Australian Information Commissioner.



During the reporting period the Inspector-General was called on twice by the Australian 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 one new case referred to the Inspector-General by the Australian Information Commissioner, the IGIS decided after taking into account the functions under the IGIS Act that the matter fell outside of her area of expertise and, on that basis, declined to give evidence. The other new request from the Australian Information Commissioner was outstanding at the end of the reporting period. 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 Australian Information Commissioner and the AAT is similar to previous reporting periods.

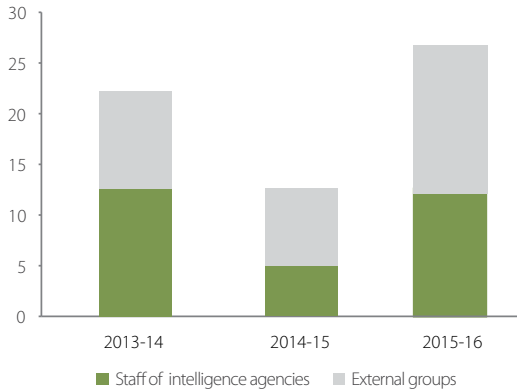
Activity 7: Presentations and outreach

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

Introduction

Each year, the office conducts a range of activities aimed at engaging with new and existing employees of intelligence agencies to help ensure awareness and understanding of their responsibilities and accountability. This engagement has included discussions with agency heads as well as presentations delivered to staff in the intelligence agencies, and other related agencies.

Figure 3.6: Number of presentations by year and audience



Quantitative performance measures

The following metric, identified in the *OIGIS Corporate Plan 2015–19*, was used to support the quantitative assessment of our performance in relation to this activity:

- number of outreach activities.

In the reporting period, we delivered a total of 27 presentations. Of these, 13 were to staff in the intelligence agencies, including in regional offices and other sites outside of Canberra; and 14 were to external groups. The number of presentations delivered has increased on previous years. This is indicative of a deliberate strategy to increase our outreach to external groups.

Discussion

Agency engagement

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. Agencies typically also use these discussions to brief the office on emerging risks or potential concerns and how they plan to respond to these challenges.

These discussions enhance awareness 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. The designation of these coordination points does not limit our capacity to speak with anyone else in the organisation when required, and indeed goes a long way to ensuring that our requirements are met in a full and prompt manner. We would like to express appreciation to our regular points of contact within each agency for assisting our work during the 2015–16 reporting period.

### Outreach

Presentations delivered to staff in the intelligence agencies, and other related agencies, 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 continued the practice of meeting with ASIS heads of station and other officers from intelligence agencies before they are posted to remind them of the functions of the office and explore any particular challenges they anticipate, depending on the particular locations and operations at their post.

In the reporting period, the Inspector-General was invited to address several leadership groups that were external to the intelligence agencies, including the Senior Executive Development Program of the Australian National Security College, the 2016 Conference on Designing Effective and Innovative Public Policy in a Complex Environment, and the Women Leaders in Public Sector Forum.

During February and March 2016, the Inspector-General addressed several legal and judicial groups, including both High Court Judges and Federal Court Judges, and the Law Council of Australia. These forums provide a valuable opportunity to increase awareness and understanding of the role of the office.

The Assistant Inspector-General, Mr Jake Blight, presented at the Australian National University as a guest lecturer.

Further presentations of a similar kind are planned in the coming year.

## Activity 8: Liaising with other accountability or integrity agencies

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

### Introduction

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.

### Quantitative performance measures

There were no quantitative performance measures identified in the *OIGIS Corporate Plan 2015–19* that were directly applicable to our liaison with other accountability or integrity agencies in Australia and overseas.

A summary of our interactions with such agencies is provided in the discussion below.

### Discussion

#### 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 June 2016, the Inspector-General met with Professor Gillian Triggs, President of the Australian Human Rights Commission, to discuss their respective roles and other issues of mutual interest. The Inspector-General also met with AHRC staff to discuss the role of our office in handling those matters referred to it.

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 guides how complaints that overlap the jurisdictions of each office are handled.

During 2015–16, we continued to hold face to face meetings every two months at the Assistant 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 relate to the handling of immigration and visa-related security assessment complaints. Where appropriate, our staff either refer matters directly to the OCO or recommend to the visa applicant that they may wish to 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 apparently been prolonged delay by Immigration in processing certain visa applications.

This office also liaised closely with OCO during 2015–16 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

In March 2016, the Inspector-General met with a member of the Canadian Privy Council Office, Mr David Vigneault, to discuss matters of mutual interest in the oversight of intelligence agencies.

In April 2016 New Zealand Inspector-General of Intelligence and Security, Ms Cheryl Gwyn, and a delegation from her office, met with the IGIS and staff to discuss ongoing inspection and oversight activities. Given the similarity in their respective governing legislation the two offices can learn much from each other in relation to the discharge of their responsibilities.

# PART 4

## Management and Accountability

### 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 an Assistant IGIS, 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 oversight of the inspection programme, complaint-handling, projects, risk management and fraud control.

Senior positions occupied during 2015–16 were as follows:

#### Inspector-General of Intelligence and Security (statutory officer)

Dr Vivienne Thom 01–18 July 2015

The Hon Margaret Stone from 24 August 2015

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

Mr Jake Blight

During the reporting period Mr Jake Blight was the Acting Inspector-General, for the period between the departure of the previous and arrival of the current Inspectors-General.

Ms Annette Willing filled the role of Assistant Inspector-General of Intelligence and Security during Mr Blight's absence on leave from October 2015 until the end of the reporting period.

#### Senior management committees

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

The functions of this committee are described in the 'Internal Audit and Risk Management' section of this chapter.

#### Corporate and operational planning

Our corporate and operational planning processes are straightforward, reflecting the small size and specialist function of the office.

The office addresses these matters through:

- an annual forward planning process to set strategic priorities
- weekly meetings between the IGIS and senior staff members, to review and document operational priorities
- monthly meetings between the IGIS and all office staff, during which internal guidelines, procedures and governance issues are discussed
- a forward plan for inspection activities in each intelligence agency, which is determined in consultation with the relevant agency head (in accordance with section 9A of the IGIS Act).

### Protective security

The Australian Government's Protective Security Policy Framework provides a structure for Australian government agencies to manage security risks proportionately and effectively, and provide the necessary protection 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 2016, we were fully compliant with 35 of the 36 mandatory requirements and partially compliant with one. A risk mitigation strategy is in place for the partially compliant requirement.

### Internal audit and risk management

The membership and functions of the Audit Committee are structured according to the PGPA Act. At 30 June 2016 the members were Mr Matthew King (Treasury) as Chair, Mr Trevor Kennedy (Attorney-General's Department) and Ms Annette Willing (OIGIS) as members. The Inspector-General attends the meetings as an observer.

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

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

The Committee reviews the Risk Management Plan annually based on its assessment of the office'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.

### Ethical standards and fraud control

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

We have established and maintained appropriate systems of risk oversight, management and internal controls in accordance with section 16 of the PGPA Act and the *Commonwealth Risk Management Policy*.

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

Regular monitoring of risks is undertaken, considered 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.

### 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.

During the reporting period, Ms Annette Willing filled the role of the Assistant Inspector-General of Intelligence and Security, under a non-Average Staffing Level affecting agreement.

### Employment of persons for a particular inquiry

Section 35(2AA) of the IGIS Act requires the Inspector-General to report on the employment under section 32(3) of any person to perform functions and exercise powers for the purposes of a particular inquiry, and any delegation under section 32AA to such a person. No such person was employed in the reporting period.

### 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 Inspector-General through team leaders and the Workplace Health and Safety Representative.

No notifiable incidents resulting from undertakings carried out by the office that would

require reporting under the *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.

### 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 our interaction with parliamentary committees are available in the *Performance* section of this report.

### Decisions by the judiciary, tribunals or the Australian Information Commissioner

No judicial decisions or decisions of administrative tribunals or of the Australian Information Commissioner made in 2015–16 had, or may have, a significant impact on the operations of the office.

## Management of Human Resources

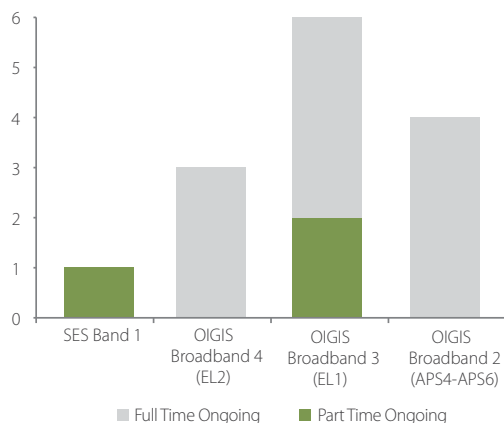
### Organisational profile

At 30 June 2016 the office had 14 ongoing APS employees (not including the Inspector-General), compared to 15 at 30 June 2015, located in the Australian Capital Territory. Three employees worked part-time.

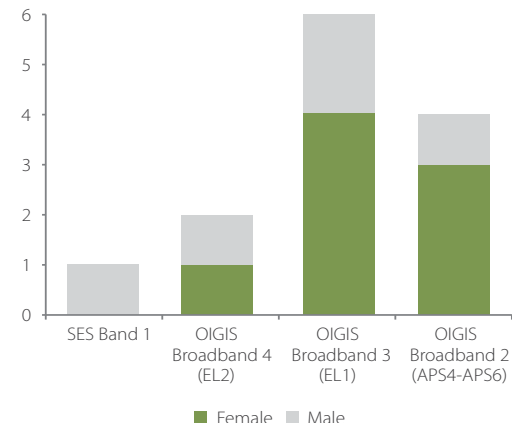
No employees identified as Indigenous.

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

**Figure 4.1: Organisational Profile as at 30 June 2016 (employment level and status)**



**Figure 4.2: Gender Balance as at 30 June 2016 (by employment level)**



### Employment frameworks

At 1 July 2015, all non-SES staff were employed under the OIGIS Enterprise Agreement 2011–2014. One SES staff member was employed under a section 24(1) determination.

Negotiations for the approval of a new OIGIS Enterprise Agreement are ongoing.

The salary range available to APS employees in the office throughout 2015–16 is provided at Annex B.

The only notable non-salary benefit for our non-SES staff is a taxable annual allowance in recognition of the requirement to undergo regular and intrusive security clearance processes necessary to maintain a Positive 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 as at 30 June 2016.

### Training and staff development

We continued the internal training programme introduced in early 2012, although not with the same frequency. The programme of short training sessions ensures that staff develop and maintain specialised knowledge and skills, and supplements on the job training.

Staff were also provided with regular opportunities throughout 2015–16 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

We do not have a performance pay scheme.

## 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/](http://www.finance.gov.au/procurement/statistics-on-commonwealth-purchasing-contracts/).

We are committed to the continued development and support of Indigenous businesses, under the Commonwealth Indigenous Procurement Policy.

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

### Consultants

During the reporting period the office did not employ the services of consultants.

### ANAO access clauses

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

### Exempt contracts

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

### Compliance with the finance law

No significant instances of non-compliance requiring a report to the responsible Minister in accordance with the PGPA Act have been recorded in the office for 2015–16.

### 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 this office. Indexed file lists were published on our 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 FOI Act.

### Advertising and market research

The following information is provided in accordance with the requirements of section 311A of the *Commonwealth Electoral Act 1918*.

The office did not incur any expenditure on advertising campaigns, market research, polling or direct mailing during the reporting period.

### Ecologically sustainable development and environmental performance

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

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

Due to the small size of the office, PM&C does not separately measure the utilities we use 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 2015–16
- 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.

### 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](http://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](http://www.dss.gov.au).

### **Correcting the Record**

In the IGIS Annual Report 2014–15, we reported the employment of one female SES Band 1 officer (p.44, Management of Human Resources, Gender Balance). This information was incorrect. In 2014–15, we had one male SES Band 1 officer.

# PART 5

## Financial statements



## INDEPENDENT AUDITOR'S REPORT

### To the Prime Minister

I have audited the accompanying annual financial statements of the Office of the Inspector-General of Intelligence and Security for the year ended 30 June 2016, which comprise a 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 including significant accounting policies and other explanatory information.

### Opinion

In my opinion, the financial statements of the Office of the Inspector-General of Intelligence and Security:

- (a) comply with Australian Accounting Standards 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 2016 and its financial performance and cash flows for the year then ended.

### Accountable Authority's Responsibility for the Financial Statements

The Inspector-General of Intelligence and Security of the Office of 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 and the rules made under that Act and 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.

### Auditor's Responsibility

My responsibility is to express an opinion on the financial statements based on my audit. I have conducted my audit in accordance with the Australian National Audit Office Auditing Standards, which incorporate the Australian Auditing Standards. These auditing standards require that I comply with relevant ethical requirements relating to audit engagements and plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgement, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements 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

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

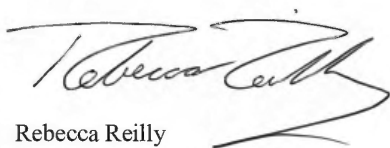
entity's internal control. An audit also includes evaluating the appropriateness of the accounting policies used and the reasonableness of accounting estimates made by the Accountable Authority of the entity, as well as evaluating the overall presentation of the financial statements.

I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my audit opinion.

***Independence***

In conducting my audit, I have followed the independence requirements of the Australian National Audit Office, which incorporate the requirements of the Australian accounting profession.

Australian National Audit Office

A handwritten signature in dark ink, appearing to read 'Rebecca Reilly', with a stylized flourish at the end.

Rebecca Reilly  
Executive Director

Delegate of the Auditor-General

Canberra  
22 September 2016

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

In my opinion, the attached financial statements for the year ended 30 June 2016 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.



Ms Annette Willing  
Acting Inspector-General of  
Intelligence and Security

22 September 2016

**OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY**  
**STATEMENT OF COMPREHENSIVE INCOME**  
*for the year ended 30 June 2016*

	Notes	2016 \$	2015 \$	Original Budget \$
<b>NET COST OF SERVICES</b>				
<b>Expenses</b>				
Employee benefits	2A	2 347 850	2 188 443	2 775 000
Suppliers	2B	263 149	322 932	393 000
Depreciation and amortisation		15 062	36 481	13 000
Loss on asset disposal		-	36	-
<b>Total Expenses</b>		<u>2 626 061</u>	<u>2 547 892</u>	<u>3 181 000</u>
<b>Own-Source Income</b>				
<b>Own-source revenue</b>				
Other revenue	3A	<u>26 625</u>	<u>28 023</u>	-
<b>Total own-source revenue</b>		<u>26 625</u>	<u>28 023</u>	-
<b>Gains</b>				
Resources Received Free of Charge	3B	<u>102 000</u>	<u>102 000</u>	<u>118 000</u>
<b>Total gains</b>		<u>102 000</u>	<u>102 000</u>	<u>118 000</u>
<b>Total own-source income</b>		<u>128 625</u>	<u>130 023</u>	<u>118 000</u>
<b>Net Cost of services</b>		<u>2 497 436</u>	<u>2 417 869</u>	<u>3 063 000</u>
Revenue from Government		<u>3 050 000</u>	<u>3 003 000</u>	<u>3 050 000</u>
<b>Surplus /(deficit) attributable to the Australian Government</b>		<u>552 564</u>	<u>585 131</u>	<u>(13 000)</u>
<b>OTHER COMPREHENSIVE INCOME</b>				
Items not subject to subsequent reclassification to net cost of services		-	-	-
<b>Total comprehensive income/(loss) attributable to the Australian Government</b>		<u>552 564</u>	<u>585 131</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 2016*

	Notes	2016 \$	2015 \$	Original Budget \$
<b>ASSETS</b>				
<b>Financial Assets</b>				
Cash and cash equivalents		154 879	174 814	206 000
Trade and other receivables	5	3 324 803	3 065 922	2 163 000
<b>Total financial assets</b>		<u>3 479 682</u>	<u>3 240 736</u>	<u>2 369 000</u>
<b>Non-Financial Assets</b>				
Property, plant and equipment	6	77 706	27 218	155 000
<b>Total non-financial assets</b>		<u>77 706</u>	<u>27 218</u>	<u>155 000</u>
<b>Total Assets</b>		<u>3 557 388</u>	<u>3 267 954</u>	<u>2 524 000</u>
<b>LIABILITIES</b>				
<b>Payables</b>				
Trade Creditors and Accruals	7	21 344	20 690	-
Other payables	7	107 477	128 131	115 000
<b>Total payables</b>		<u>128 821</u>	<u>148 821</u>	<u>115 000</u>
<b>Provisions</b>				
Employee provisions	8	597 217	865 347	730 000
<b>Total provisions</b>		<u>597 217</u>	<u>865 347</u>	<u>730 000</u>
<b>Total Liabilities</b>		<u>726 038</u>	<u>1 014 168</u>	<u>845 000</u>
<b>Net Assets</b>		<u>2 831 350</u>	<u>2 253 786</u>	<u>1 679 000</u>
<b>EQUITY</b>				
Contributed equity		503 126	478 126	514 000
Reserves		16 105	16 105	16 000
Retained surplus		2 312 119	1 759 555	1 149 000
<b>Total Equity</b>		<u>2 831 350</u>	<u>2 253 786</u>	<u>1 679 000</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 2016*

	2016 \$	2015 \$	Original Budget \$
<b>CONTRIBUTED EQUITY</b>			
<b>Opening balance as at 1 July</b>			
Balance carried forward from previous period	478 126	463 000	489 000
Other Comprehensive Income	-	-	-
<b>Total comprehensive income</b>	-	-	-
<b>Transactions with Owners</b>			
<b>Contributions by Owners</b>			
Appropriations Repealed <sup>1</sup>	-	(10 874)	-
Departmental Capital Budget	25 000	26 000	25 000
<b>Total Transactions with Owners</b>	25 000	15 126	25 000
<b>Closing balance as at 30 June</b>	503 126	478 126	514 000
<b>RETAINED EARNINGS</b>			
<b>Opening balance as at 1 July</b>			
Balance carried forward from previous period	1 759 555	1 174 424	1 162 000
<b>Comprehensive Income</b>			
Surplus/deficit for the period	552 564	585 131	(13 000)
<b>Total comprehensive income</b>	552 564	585 131	(13 000)
<b>Closing balance as at 30 June</b>	2 312 119	1 759 555	1 149 000
<b>ASSET REVALUATION RESERVE</b>			
<b>Opening balance as at 1 July</b>			
Balance carried forward from previous period	16 105	16 105	16 000
<b>Closing balance as at 30 June</b>	16 105	16 105	16 000
<b>TOTAL EQUITY</b>			
<b>Opening balance</b>			
Balance carried forward from previous period	2 253 786	1 653 529	1 667 000
<b>Comprehensive Income</b>			
Surplus/deficit for the period	552 564	585 131	(13 000)
<b>Total comprehensive income</b>	552 564	585 131	(13 000)
<b>Transactions with Owners</b>			
<b>Contributions by Owners</b>			
Appropriations Repealed <sup>1</sup>	-	(10 874)	-
Departmental Capital Budget	25 000	26 000	25 000
<b>Total Transactions with Owners</b>	25 000	15 126	25 000
<b>Closing balance as at 30 June</b>	2 831 350	2 253 786	1 679 000

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

Contributed Equity

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 2016*

	Notes	2016 \$	2015 \$	Budget \$
<b>OPERATING ACTIVITIES</b>				
<b>Cash received</b>				
Appropriations		2 867 103	2 371 063	3 170 000
Net GST received		14 329	8 598	-
Other cash received		187 214	116 499	2 000
<b>Total cash received</b>		<b>3 068 646</b>	2 496 160	3 172 000
<b>Cash used</b>				
Employees		(2 279 195)	(2 092 294)	(2 775 000)
Suppliers		(641 163)	(314 023)	(397 000)
Section 74 receipts transferred to OPA		(185 044)	(116 499)	-
<b>Total cash used</b>		<b>(3 105 402)</b>	(2 522 816)	(3 172 000)
<b>Net cash from/(used by) operating activities</b>	<b>13</b>	<b>(36 756)</b>	(26 656)	-
<b>INVESTING ACTIVITIES</b>				
<b>Cash used</b>				
Purchase of property, plant and equipment		(49 094)	(5 535)	(91 000)
<b>Total cash used</b>		<b>(49 094)</b>	(5 535)	(91 000)
<b>Net cash from/(used by) investing activities</b>		<b>(49 094)</b>	(5 535)	(91 000)
<b>FINANCING ACTIVITIES</b>				
<b>Cash received</b>				
Contributed equity		65 915	-	91 000
<b>Total cash received</b>		<b>65 915</b>	-	91 000
<b>Net cash from financing activities</b>		<b>65 915</b>	-	91 000
<b>Net increase/(decrease) in cash held</b>		<b>(19 935)</b>	(32 191)	-
Cash and cash equivalents at the beginning of the reporting period		174 814	207 005	206 000
<b>Cash and cash equivalents at the end of the reporting period</b>	<b>13</b>	<b>154 879</b>	174 814	206 000

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

## Departmental Major Budget Variances for 2016

The following table provides high level commentary of major variances between budgeted information for the OIGIS published in the Prime Minister and Cabinet's 2015-16 Portfolio Budget Statements (PBS) and the 2015-16 final outcome as presented in accordance with Australian Accounting Standards for the OIGIS. The Budget is not audited. Major variances are those deemed relevant to an analysis of OIGIS' performance and are not focused merely on numerical differences between the budget and actual amounts. Explanations of major variances are as follows:

Explanation of major variances	Affected line items (and statements)
Employee Benefits – \$427,150 underspent due mainly to recruitment delays associated with the lengthy security clearance process.	Impacted: Employee expenses Appropriations receivable Employee provisions Other payables Retained surplus Cashflow statement operating activities
Suppliers – \$129,851 underspent. The most significant variance was a \$36,000 underspend in security clearance fees due to delays in the recruitment process. Other variances included underspends in expenses typically driven by the number and scope of inquiry work, including \$30,000 for consultants and \$21,000 for legal expenses and less than expected costs associated with the purchase of software licences in the current year.	Impacted: Supplier expenses Appropriation receivable Suppliers payables Retained surplus Cashflow statement operating activities
Property, Plant and Equipment – capital expenditure was approximately \$55,000 below budget due to delays in the scheduled replacement of existing assets.	Impacted: Property, plant and equipment Depreciation and amortisation Appropriations receivable Cashflow statement financing activities
Other Cash Received – approximately \$185,214 above budget. The variance relates to salary reimbursements received for officers seconded to other agencies and leave liabilities transfers for new starters which are not budgeted for.	Impacted: Cash and cash equivalents Appropriations receivable Cashflow statement operating activities

## **Note 1 – Overview**

### **1.1 Objectives of the Office of the Inspector-General of Intelligence and Security**

The Office of the Inspector General of Intelligence and Security (OIGIS) is an Australian Government controlled not-for-profit entity. The objective of OIGIS is to meet the following outcome:

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.

OIGIS's activities contributing towards this program are classified as departmental. Departmental activities involve the use of assets, liabilities, income and expenses controlled or incurred by OIGIS in its own right.

The continued existence of the OIGIS in its present form and with its present programs is dependent on government policy and on continuing funding by Parliament for OIGIS's administration and programs.

### **1.2 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 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.

### **1.3 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.

#### **1.4 New Australian Accounting Standards**

##### Adoption of New Australian Accounting Standard Requirements

No accounting standard has been adopted earlier than the application date as stated in the standard.

New/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 the entity's financial statements.

##### Future Australian Accounting Standard Requirements

Amendments to AASB 124 *Related Party Disclosures* are effective for annual reporting periods beginning on or after 1 July 2016. The amendments include changes to the definition of related parties and will require OIGIS to assess the details of our related parties and include disclosures in future financial statements.

Other new new/revised standards, interpretations and amending standards that were issued prior to the sign-off date and applicable to future reporting periods are not expected to have a material impact on the entity's financial statements.

#### **1.5 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.

#### **1.6 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, except for certain amounts that relate to activities that are reciprocal in nature, in which case revenue is recognised only when it has been earned. Appropriations receivable are recognised at their nominal amounts.

#### **1.7 Events after the Reporting Period**

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

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for year ended 30 June 2016

**Note 2 – Expenses**

	2016 \$	2015 \$
<u>Note 2A – Employee Benefits</u>		
Wages and salaries	1 547 700	1 644 289
Superannuation:		
Defined benefit plans	136 643	223 658
Defined contribution plans	173 166	97 823
Leave and other entitlements	490 341	222 673
<b>Total employee benefits</b>	<b>2 347 850</b>	<b>2 188 443</b>

**Accounting Policy**

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

	2016 \$	2015 \$
<u>Note 2B – Suppliers</u>		
<b>Goods and services supplied or rendered</b>		
Consultants	-	-
ICT support	46 000	46 000
Legal expenses	-	17 104
Printing non publications	9 483	8 868
Resources received free of charge:		
Notional Rent Charge	102 000	102 000
Notional Audit Fees	18 000	18 000
Notional IT Support Costs	4 545	4 545
Stationery	13 932	9 758
Training	13 868	33 657
Travel	9 200	24 111
Translation Services	469	11 804
Other	25 597	32 945
<b>Total goods and services supplied or rendered</b>	<b>243 094</b>	<b>308 792</b>
<b>Other suppliers</b>		
Motor Vehicle Lease – minimum lease payments	14 675	9 380
Workers compensation premiums	5 380	4 760
<b>Total other supplier</b>	<b>20 055</b>	<b>14 140</b>
<b>Total supplier</b>	<b>263 149</b>	<b>322 932</b>

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for year ended 30 June 2016

Leasing Commitments

OIGIS in its capacity as lessee holds one motor vehicle operating lease. The lease has contracted monthly payments of \$927.87 (GST exclusive) and expires 20 August 2018.

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

	2016 \$	2015 \$
Within 1 year	11 134	10 396
Between 1 to 5 years	12 990	24 124
<b>Total operating lease commitments</b>	<b>24 124</b>	<b>34 520</b>

**Note 3 – Own-Source Income**

	2016 \$	2015 \$
Employee FBT Contributions	3 966	5 403
Other	114	75
Resources Received Free of Charge:		
Australian National Audit Office	18 000	18 000
Australian Signals Directorate	4 545	4 545
<b>Total other own-source revenue</b>	<b>26 625</b>	<b>28 023</b>

Note 3B – Other Gains

Resources Received Free of Charge:		
Department of the Prime Minister & Cabinet	102 000	102 000
<b>Total other gains</b>	<b>102 000</b>	<b>102 000</b>

Accounting Policy

Resources Received Free of Charge

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

The main resources received free of charge in 2015-16 are 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).

Contributions of assets at no cost of acquisition or for nominal considerations are recognised as gains at their fair value when the asset qualifies for recognition, unless received from another Government agency or authority as a consequence of a restructuring of administrative arrangements.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for year ended 30 June 2016

**Note 4 – Fair Value Measurement**

The following table provides an analysis of assets and liabilities that are measured at fair value. The different levels of the fair value hierarchy are defined below:

Level 1 – Quoted prices (unadjusted) in active markets for identical assets or liabilities that the entity can access at measurement date.

Level 2 – Inputs other than quoted prices included within Level 1 that are observable for the asset or liability, either directly or indirectly.

Level 3 – Unobservable inputs for the asset or liability.

**Note 4A – Fair Value Measurements**

	Fair value measurement at the end of the reporting period			For Levels 2 and 3 fair value measurements	
	2016	2015	Category (Level 1, 2 or 3)	Valuation Technique(s) <sup>1</sup>	Inputs used
<b>Non-Financial Assets</b>					
Property, plant and equipment					
Level 2 assets included office equipment and furniture	75 477	22 338	Level 2	Market comparables	Sale prices of comparable assets
Level 3 assets included computer equipment and office furniture	2 229	4 880	Level 3	Market comparables and depreciated replacement cost	Sale prices of comparable assets in limited market and quotes for replacement assets adjusted for life of asset

1. No change in valuation technique occurred during the period.

The OIGIS's assets are held for operational purposes and not held for the purposes of deriving a profit. The current use of all controlled assets is considered their highest and best use.

**Note 4B – Level 1 and Level 2 Transfers for Recurring Fair Value Measurements**

There were no transfers between levels during 2015-16.

OIGIS's policy is that transfers between levels are deemed to have occurred at the end of the reporting period.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for year ended 30 June 2016

**Note 5 – Financial Assets**

	2016 \$	2015 \$
<u>Trade and other receivables</u>		
Appropriations receivable	3 314 181	2 987 155
GST receivable from the Australian Taxation Office	176	1 752
Other receivables	10 446	77 015
<b>Total trade and other receivables (net)</b>	<b>3 324 803</b>	<b>3 065 922</b>

**Trade and Other Receivables (Gross) are aged as follows:**

Not overdue	3 324 803	3 065 922
-------------	-----------	-----------

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

**Accounting Policy**

Receivables for goods and services, which have 30 day terms, are recognised at the nominal amounts due less any 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.

**Note 6 – Non-Financial Assets**

Reconciliation of the Opening and Closing Balances of Property, Plant and Equipment for 2016

Item	Property, plant & equipment \$ 2016	Property, plant & equipment \$ 2015
<b>As at 1 July</b>		
Gross book value	63 635	63 735
Accumulated depreciation and impairment	(36 417)	-
<b>Total as at 1 July</b>	<b>27 218</b>	<b>63 735</b>
Additions		
by purchase	65 550	-
Depreciation expense	(15 062)	(36,481)
Disposals	-	(36)
<b>Total as at 30 June</b>	<b>77 706</b>	<b>27 218</b>
<b>Total as at 30 June represented by:</b>		
Gross book value	120 685	63 635
Accumulated depreciation and impairment	(42 979)	36 417
<b>Total as at 30 June</b>	<b>77 706</b>	<b>27 218</b>

**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.



NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for year ended 30 June 2016

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).

Revaluations

Fair values are determined by market selling price.

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. A full revaluation was conducted at 30 June 2014 by an independent valuer.

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 2014.

All assets were examined for indicators of impairment during the stocktake completed on 30 June 2016 and none were found.

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 – 14 years (2015: 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.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for year ended 30 June 2016

**Note 7 – Payables**

	2016 \$	2015 \$
<u>Trade Creditors and Accruals</u>		
Trade creditors and accruals	21 344	20 690
<b>Total suppliers</b>	<u>21 344</u>	<u>20 690</u>

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

**Accounting Policy**

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

	2016 \$	2015 \$
<u>Other Payables</u>		
Salaries and wages	5 142	67 338
Superannuation	873	10 572
Other	101 462	50 221
<b>Total other payables</b>	<u>107 477</u>	<u>128 131</u>

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

**Accounting Policy**

Superannuation

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

**Note 8 – Employee Provisions**

	2016 \$	2015 \$
<u>Employee Provisions</u>		
Leave	597 217	865 347
<b>Total employee provisions</b>	<u>597 217</u>	<u>865 347</u>
<b>Employee provisions are expected to be settled in:</b>		
No more than 12 months	93 584	145 538
More than 12 months	503 633	719 809
<b>Total employee provisions</b>	<u>597 217</u>	<u>865 347</u>

**Accounting Policy**

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

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for year ended 30 June 2016

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 FRR. The estimate of the present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

Superannuation

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

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

The PSSap is a defined contribution scheme.

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.

**Note 9 – Senior Management Personnel Remuneration**

	2016 \$	2015 \$
<b>Short-term employee benefits:</b>		
Salary	626 182	521 028
Annual leave <sup>1</sup>	2 983	29 772
Allowances	43 775	-
<b>Total short-term employee benefits</b>	<b>672 940</b>	<b>550 800</b>
<b>Post-employment benefits:</b>		
Superannuation	94 626	94 438
<b>Total post-employment benefits</b>	<b>94 626</b>	<b>94 438</b>
<b>Other long-term employee benefits:</b>		
Annual Leave	43 850	10 742
Long Service Leave	9 171	18 997
<b>Total other long-term employee benefits</b>	<b>53 021</b>	<b>29 739</b>
<b>Total senior executive remuneration expenses</b>	<b>820 587</b>	<b>674 977</b>

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for year ended 30 June 2016

### **Accounting Policy**

This note is prepared on an accrual basis. The total number of senior management personnel that are included in the above table are 4 individuals (2015: 3 individuals). The 2016 figure includes three of the officers for part of the year.

1 Annual Leave expected to be taken within 12 months.

### **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 in either 2014-15 or in 2015-16.

No contingent rentals exist.

### **Note 11 – Financial Instruments**

	2016 \$	2015 \$
<b><u>Note 11 – Categories of Financial Instruments</u></b>		
<b>Financial Assets</b>		
<b>Loans and Receivables</b>		
Loans and receivables		
Cash and cash equivalents	154 879	174 814
Trade receivables	10 446	77 015
<b>Total financial assets</b>	<u>165 325</u>	<u>251 829</u>
<b>Financial Liabilities</b>		
<b>At amortised cost</b>		
Trade creditors	21 344	20 690
<b>Total financial liabilities</b>	<u>21 344</u>	<u>20 690</u>

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

### **Financial Assets**

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

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

Credit terms are net 30 days (2014–15: 30 days).

### **Financial Liabilities**

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

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for year ended 30 June 2016

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.

Credit Risk

OIGIS has endorsed policies and procedures for debt management (including the provision of credit terms), to reduce the incidence of credit risk. In most instances debtors for OIGIS are other government entities and therefore represent minimal credit risk.

The carrying amount of financial assets, net of impairment losses, reported in the statement of financial position represents the Agencies maximum exposure to credit risk.

Liquidity Risk

OIGIS's financial liabilities only include payables. Any exposure to liquidity risk is based on the notion that OIGIS will encounter difficulty in meeting its obligations associated with financial liabilities. This is highly unlikely as OIGIS is appropriated funding from the Australian Government and manages its budgeted funds to ensure it has adequate funds to meet payments as they fall due. In addition, the entity has policies in place to ensure timely payments were made when due and has no past experience of default.

Market Risk

OIGIS holds only basic financial instruments that do not expose the agency to certain market risks, such as 'Currency risk' and 'Other price risk'.

**Note 12 – Appropriations**

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

	2016 \$	2015 \$
<b>Ordinary Annual Services</b>		
Annual Appropriation	3 050 000	3 003 000
PGPA Act – Section 74 Receipts	185 044	116 500
Annual Departmental Capital Budget <sup>1</sup>	25 000	26 000
<b>Total appropriation</b>	<b>3 260 044</b>	<b>3 145 500</b>
Appropriation applied (current and prior years)	2 933 018	2 371 063
<b>Variance<sup>2</sup></b>	<b>327 026</b>	<b>774 437</b>

- 1 Departmental Capital Budgets are appropriated through Appropriation Acts (No 1,3,5). They form part of ordinary annual services, and are not separately identified in the Appropriation Acts.
- 2 Variance between Total Appropriation and Appropriation Applied is due to section 74 receipts and recruitment delays associated with security clearance requirements.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for year ended 30 June 2016

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

	2016 \$	2015 \$
<b>Departmental</b>		
Appropriation Act (No 1) 2013-14 - DCB	3 085	69 000
Appropriation Act (No 1) 2014-15	-	2 225 969
Appropriation Act (No 3) 2014-15	241 040	840 000
Appropriation Act (No 1) 2014-15 -- DCB	26 000	26 000
Appropriation Act (No 1) 2015-16	3 172 934	-
Appropriation Act (No 1) 2015-16 -- DCB	25 000	-
<b>Total Departmental</b>	<b>3 468 059</b>	<b>3 160 969</b>

**Note 13 – Cash Flow Reconciliation**

	2016 \$	2015 \$
<b>Reconciliation of net cost of services to net cash from operating activities:</b>		
Net cost of services	(2 497 436)	(2 417 869)
Add revenue from Government	3 050 000	3 003 000
<b>Adjustments for non-cash items</b>		
Depreciation/amortisation	15 062	36 481
Loss on disposal of assets	-	36
<b>Movements in assets and liabilities</b>		
Increase/(Decrease) in provision of employee liabilities	(268 130)	134 959
Increase/(Decrease) in other payables	(20 655)	49 905
Increase/(Decrease) in supplier trade creditors	(15 801)	(12 575)
(Increase)/Decrease in appropriation receivables	(367 941)	(748 436)
(Increase)/Decrease in other assets	66 569	(70 558)
(Increase)/Decrease in other prepayments	-	-
(Increase)/Decrease in GST receivable	1 576	(1 599)
<b>Net cash from (used by) operating activities</b>	<b>(36 756)</b>	<b>(26 656)</b>

**Accounting Policy**

**Cash**

Cash and cash equivalents includes cash on hand and any deposits in bank accounts with an original maturity of 3 months or less that are readily convertible to known amounts of cash and subject to insignificant risk of changes in value. Cash is recognised at its nominal amount.

# PART 6

## Annexures

## Annex A:

### Entity resource statement and resources for outcomes 2015–16

Figure 5.1: Entity resource statement 2015–16

		Actual available appropriation for 2015–16 \$'000 (a)	Payments made 2015–16 \$'000 (b)	Balance remaining 2015–16 \$'000 (a) – (b)
<b>Ordinary Annual Services</b>				
<b>Departmental Appropriation</b>				
Prior year departmental appropriation		3 160	2 650	510
Departmental appropriation		3 075	319	2 756
S74 Relevant Agency Receipts		202	-	202
<b>Total</b>		<b>6 437</b>	<b>2 969</b>	<b>3 468</b>
<b>Administered expenses</b>				
<b>Total</b>		-	-	-
<b>Total ordinary annual services</b>	<b>A</b>	<b>6 437</b>	<b>2 969</b>	<b>3 468</b>
<b>Other services</b>				
Departmental non-operating		-	-	-
<b>Total</b>		-	-	-
<b>Total other services</b>	<b>B</b>	-	-	-
<b>Total available annual appropriations</b>		<b>6 437</b>	<b>2 969</b>	<b>3 468</b>
<b>Special appropriations</b>				
<b>Total special appropriations</b>	<b>C</b>	-	-	-
<b>Special accounts</b>				
<b>Total special accounts</b>	<b>D</b>	-	-	-
<b>Total resourcing A + B + C + D</b>		<b>6 437</b>	<b>2 969</b>	<b>3 468</b>
Less appropriations drawn from annual or special appropriations above and credited to special accounts and/or payments to corporate entities through annual appropriations		-	-	-
<b>Total net resourcing and payments for agency</b>		<b>6 437</b>	<b>2 969</b>	<b>3 468</b>



**Figure 5.2: 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 2015–16 \$'000 (a)	Actual expenses 2015–16 \$'000 (b)	Variation 2015–16 \$'000 (a) – (b)
<b>Programme 1.1: Office of the Inspector-General of Intelligence and Security</b>			
Departmental expenses			
Departmental appropriation <sup>7</sup>	3 050	3 054	(4)
Special appropriations	-	-	-
Special Accounts	-	-	-
Expenses not requiring appropriation in the Budget year	131	139	(8)
<b>Total for Program 1.1</b>	<b>3 181</b>	<b>3 193</b>	<b>(12)</b>
<b>Outcome 1 Totals by appropriation type</b>			
Departmental expenses			
Departmental appropriation <sup>1</sup>	3 050	3 054	(4)
Special appropriations	-	-	-
Special Accounts	-	-	-
Expenses not requiring appropriation in the Budget year	131	139	(8)
<b>Total expenses for Outcome 1</b>	<b>3 181</b>	<b>3 193</b>	<b>(12)</b>
	<b>Budget 2015–16</b>	<b>Actual 2015–16</b>	
<b>Average Staffing Level (number)</b>	<b>16</b>	<b>14</b>	<b>2</b>

<sup>7</sup> Departmental appropriation combines ordinary annual services (Appropriation Act Nos 1, 3 and 5) and retained revenue receipts under section 74 of the *Public Governance, Performance and Accountability Act 2013*.

# Annex B:

## OIGIS Salary Scale

OIGIS Band	APS Level	Salary Range 1 July 2015 – 30 June 2016 (\$)
OIGIS Band 4	EL2	112,564 - 133,967
OIGIS Band 3	EL1	96,710 - 107,810
OIGIS Band 2	APS 6	80,063 - 89,973
	APS 5	70,155 - 76,101
	APS 4	63,021 - 68,569
OIGIS Band 1	APS 3	56,680 - 61,038
	APS 2	49,543 - 55,092
	APS 1	45,138 - 48,355

## Annex C:

### Requirements for annual reports

PGPA Rule Reference	Part of Report	Description	Requirement	Page
<b>17AD(g)</b>	<b>Letter of transmittal</b>			
17AI		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 PGPA Act and any enabling legislation that specified additional requirements in relation to the annual report.	Mandatory	i
<b>17AD(h)</b>	<b>Aids to access</b>			
17AJ(a)		Table of contents	Mandatory	ii–iii
17AJ(b)		Alphabetical index	Mandatory	85
17AJ(c)		Glossary of abbreviations and acronyms	Mandatory	84
17AJ(d)		List of requirements	Mandatory	77–83
17AJ(e)		Details of contact officer	Mandatory	inside front cover
17AJ(f)		Entity's website address	Mandatory	inside front cover
17AJ(g)		Electronic address of report	Mandatory	inside front cover
<b>17AD(a)</b>	<b>Review by accountable authority</b>			
17AD(a)		A review by the accountable authority of the entity	Mandatory	v
<b>17AD(b)</b>	<b>Overview of the entity</b>			
17AE(1)(a)(i)		A description of the role and functions of the entity	Mandatory	2–3, 6–7
17AE(1)(a)(ii)		A description of the organisational structure of the entity	Mandatory	46
17AE(1)(a)(iii)		A description of the outcomes and programmes administered by the entity	Mandatory	2–3
17AE(1)(a)(iv)		A description of the purposes of the entity as included in corporate plan	Mandatory	3, 6–7
17AE(1)(b)		An outline of the structure of the portfolio of the entity	Portfolio departments, Mandatory	N/A

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AE(2)		Where the outcomes and programmes administered by the entity differ from any Portfolio Budget Statement, Portfolio Additional Estimates Statement or other portfolio estimates statement that was prepared for the entity for the period, include details of variation and reasons for change	If applicable, Mandatory	N/A
<b>17AD(c)</b>	<b>Report on the Performance of the entity</b>			
	<b>Annual performance statements</b>			
17AD(c)(i); 16F		Annual performance statement in accordance with paragraph 39(1)(b) of the Act and section 16F of the Rule	Mandatory	6
17AD(c) (ii)	<b>Report on Financial Performance</b>			
17AF(1)(a)		A discussion and analysis of the entity's financial performance	Mandatory	10–11
17AF(1)(b)		A table summarising the total resources and total payments of the entity	Mandatory	74–75
17AF(2)		If there may be significant changes in the financial results during or after the previous or current reporting period, information on those changes, including: the cause of any operating loss of the entity; how the entity has responded to the loss and the actions that have been taken in relation to the loss; and any matter or circumstances that it can reasonably be anticipated will have a significant impact on the entity's future operation or financial results	If applicable, Mandatory	N/A
<b>17AD(d)</b>	<b>Management and Accountability</b>			
	<b>Corporate Governance</b>			
17AG(2)(a)		Information on compliance with section 10 (fraud systems)	Mandatory	i, 47–48
17AG(2)(b)(i)		A certification by accountable authority that fraud risk assessments and fraud control plans have been prepared	Mandatory	i
17AG(2)(b)(ii)		A certification by accountable authority that appropriate mechanisms for preventing, detecting incidents of, investigating or otherwise dealing with, and recording or reporting fraud that meet the specific needs of the entity are in place	Mandatory	i

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(2)(b)(iii)		A certification by accountable authority that all reasonable measures have been taken to deal appropriately with fraud relating to the entity	Mandatory	i
17AG(2)(c)		An outline of structures and processes in place for the entity to implement principles and objectives of corporate governance	Mandatory	46–48
17AG(2)(d) – (e)		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
<b>External Scrutiny</b>				
17AG(3)		Information on the most significant developments in external scrutiny and the entity's response to the scrutiny	Mandatory	48
17AG(3)(a)		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	N/A
17AG(3)(b)		Information on any reports on operations of the entity by the Auditor-General (other than report under section 43 of the Act), a Parliamentary Committee, or the Commonwealth Ombudsman	If applicable, Mandatory	N/A
17AG(3)(c)		Information on any capability reviews on the entity that were released during the period	If applicable, Mandatory	N/A
<b>Management of Human Resources</b>				
17AG(4)(a)		An assessment of the entity's effectiveness in managing and developing employees to achieve entity objectives	Mandatory	48–49

PGPA Rule Reference	Part of Report	Description	Requirement	Page
17AG(4)(b)		<p>Statistics on the entity's APS employees on an ongoing and non-ongoing basis; including the following:</p> <ul style="list-style-type: none"> <li>• statistics on staffing classification level</li> <li>• statistics on full-time employees</li> <li>• statistics on part-time employees</li> <li>• statistics on gender</li> <li>• statistics on staff location</li> <li>• statistics on employees who identify as Indigenous</li> </ul>	Mandatory	49
17AG(4)(c)		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	49
17AG(4)(c)(i)		Information on the number of SES and non-SES employees covered by agreements etc identified in paragraph 17AG(4)(c)	Mandatory	49
17AG(4)(c )(ii)		The salary ranges available for APS employees by classification level	Mandatory	76
17AG(4)(c )(iii)		A description of non-salary benefits provided to employees	Mandatory	49
17AG(4)(d)(i)		Information on the number of employees at each classification level who received performance pay	If applicable, Mandatory	49
17AG(4)(d)(ii)		Information on aggregate amounts of performance pay at each classification level	If applicable, Mandatory	N/A
17AG(4)(d)(iii)		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)		Information on aggregate amount of performance payments	If applicable, Mandatory	N/A

PGPA Rule Reference	Part of Report	Description	Requirement	Page
<b>Assets Management</b>				
17AG(5)		An assessment of effectiveness of assets management where asset management is a significant part of the entity's activities	If applicable, Mandatory	N/A
<b>Purchasing</b>				
17AG(6)		An assessment of entity performance against the <i>Commonwealth Procurement Rules</i>	Mandatory	49
<b>Consultants</b>				
17AG(7)(a)		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	50
17AG(7)(b)		A statement that " <i>During [reporting period], [specified number] new consultancy contracts were entered into involving total actual expenditure of \$[specified million]. In addition, [specified number] ongoing consultancy contracts were active during the period, involving total actual expenditure of \$[specified million]</i> "	Mandatory	50
17AG(7)(c )		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	50
17AG(7)(d)		A statement that " <i>Annual reports contain information about actual expenditure on contracts for consultancies. Information on the value of contracts and consultancies is available on the AusTender website</i> "	Mandatory	50

PGPA Rule Reference	Part of Report	Description	Requirement	Page
<b>Australian National Audit Office Access Clauses</b>				
17AG(8)		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
<b>Exempt contracts</b>				
17AG(9)		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
<b>Small business</b>				
17AG(10)(a)		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	49
17AG(10)(b)		An outline of the ways in which the procurement practices of the entity support small and medium enterprises	Mandatory	49
17AG(10)(c)		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



PGPA Rule Reference	Part of Report	Description	Requirement	Page
<b>Financial Statements</b>				
17AD(e)		Inclusion of the annual financial statements in accordance with subsection 43(4) of the Act	Mandatory	52–72
<b>17AD(f)</b>	<b>Other Mandatory Information</b>			
17AH(1)(a)(i)		If the entity conducted advertising campaigns, a statement that <i>“During [reporting period], the [name of entity] conducted the following advertising campaigns: [name of advertising campaigns undertaken]. Further information on those advertising campaigns is available at [address of entity’s website] and in the reports on Australian Government advertising prepared by the Department of Finance. Those reports are available on the Department of Finance’s website.”</i>	If applicable, Mandatory	N/A
17AH(1)(a)(ii)		If the entity did not conduct advertising campaigns, a statement to that effect	If applicable, Mandatory	50
17AH(1)(b)		A statement that <i>“Information on grants awarded by [name of entity] during [reporting period] is available at [address of entity’s website].”</i>	If applicable, Mandatory	N/A
17AH(1)(c )		Outline of mechanisms of disability reporting, including reference to website for further information	Mandatory	50–51
17AH(1)(d)		Website reference to where the entity’s Information Publication Scheme statement pursuant to Part II of FOI Act can be found	Mandatory	N/A
17AH(1)(e)		Correction of material errors in previous annual report	If applicable, Mandatory	51
17AH(2)		Information required by other legislation	Mandatory	50

## Annex D: Glossary of abbreviations

<b>AAT</b>	Administrative Appeals Tribunal
<b>AGO</b>	Australian Geospatial-Intelligence Organisation
<b>AHRC</b>	Australian Human Rights Commission
<b>AIC</b>	Australian Intelligence Community
<b>ASD</b>	Australian Signals Directorate
<b>ASIC</b>	Aviation Security Identification Card
<b>AML/CTF Act</b>	<i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i>
<b>APS</b>	Australian Public Service
<b>ASIO</b>	Australian Security Intelligence Organisation
<b>ASIO Act</b>	<i>Australian Security Intelligence Organisation Act 1979</i>
<b>ASIS</b>	Australian Secret Intelligence Service
<b>AUSTRAC</b>	Australian Transaction Reports and Analysis Centre
<b>DFAT</b>	Department of Foreign Affairs and Trade
<b>DIO</b>	Defence Intelligence Organisation
<b>FIC</b>	Foreign intelligence collection
<b>FOI</b>	Freedom of Information
<b>FOI Act</b>	<i>Freedom of Information Act 1982</i>
<b>ICCPR</b>	<i>International Covenant on Civil and Political Rights</i>
<b>IGIS</b>	Inspector-General of Intelligence and Security
<b>IGIS Act</b>	<i>Inspector-General of Intelligence and Security Act 1986</i>
<b>ISA</b>	<i>Intelligence Services Act 2001</i>
<b>MSIC</b>	Maritime Security Identification Card
<b>OCO</b>	Office of the Commonwealth Ombudsman
<b>OIGIS</b>	Office of the Inspector-General of Intelligence and Security
<b>ONA</b>	Office of National Assessments
<b>ONA Act</b>	<i>Office of National Assessments Act 1977</i>
<b>PGPA Act</b>	<i>Public Governance, Performance and Accountability Act 2013</i>
<b>PGPA Rule</b>	Public Governance, Performance and Accountability Rule 2014
<b>PID Act</b>	<i>Public Interest Disclosure Act 2013</i>
<b>SES</b>	Senior Executive Service
<b>TIA Act</b>	<i>Telecommunications (Interception and Access) Act 1979</i>
<b>WHS Act</b>	<i>Work Health and Safety Act 2011</i>

# Index

## A

abbreviations, 84

Activity performance *see* performance

address and contact details, *inside front cover*

Administrative Appeals Tribunal, 3, 8, 12, 42–3

administrative tribunal decisions  
(external scrutiny), 48

advertising and market research, 50

ANAO *see* Australian National Audit Office

annual report 2014–15 correction, 51

annual report availability, *inside front cover*

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

*Archives Act 1983*, 3, 42

Assistant Inspector-General of Intelligence  
and Security, 46

assumed identities, 32

Attorney-General

responsibilities, 3

Guidelines under ASIO Act, 21

Audit Committee, 46

audits

ANAO report on financial statements,  
48, 53–4

internal audit, 47

AusTender, 50

Australian Geospatial-Intelligence  
Organisation (AGO)

AUSTRAC information access and use, 34

Director's approvals, 29–30

inspections of, 29–30, 34

intelligence on Australian persons,  
23–4, 30

Ministerial authorisations, 30

presumption of nationality, 24

privacy rules compliance, 24, 30

role and functions, 5

Australian Government Protective Security  
Policy Framework, 46

Australian Human Rights Commission, 9, 44  
referrals to OIGIS, 38

Australian Information Commissioner, 3, 8,  
12, 42, 48

Australian Intelligence Community *see*  
intelligence agencies

Australian National Audit Office

access clauses, 50

audit report, 48, 53–4

Australian persons

intelligence collection on, 23–4,  
25–6, 28, 30 *see also* privacy rules  
compliance

Australian Secret Intelligence Service (ASIS)  
assumed identities, 32

- AUSTRAC information access and use, 34
  - cooperation with foreign liaisons, 25
  - inspections of, 24–7, 34
  - intelligence on Australian persons, 23–4, 25–6, 28
  - Ministerial authorisations, 25–8
  - presumption of nationality, 24
  - privacy rules compliance, 24, 26
  - review of operational files, 25
  - role and functions, 4
  - weapons use and issues, 26–7
  - Australian Security Intelligence Organisation (ASIO)
    - analytical tradecraft, 16
    - assumed identities, 32
    - AUSTRAC information access and use, 34
    - complaints, 9, 36–9
    - computer access warrants, 17
    - foreign liaisons information exchange, 21, 25
    - human source management, 16
    - identified person warrants, 17, 18
    - information exchange, 20, 21
    - inspections of, 15–23, 34
    - internal policies and procedures, 16
    - journalist information warrants, 18
    - legal representative attendance at ASIO interviews, 23
    - Ministerial submissions, 20
    - questioning and detention warrants, 18
    - recordkeeping, 21
    - role and functions, 3–4
    - search warrants, 17, 38, 39
    - security assessments, 21, 39
    - Special Intelligence Operations, 19
    - staff use of information holdings, 22
    - surveillance device warrants, 17
    - taxation information access, 20
    - telecommunications data and interception warrants, 16–17, 19–20, 22
    - use of force, 19
    - warrants ‘whole of life’ project, 22–3
  - Australian Security Intelligence Organisation Act 1979*, 3–4, 15, 17, 18, 19
  - Attorney-General’s Guidelines, 21
  - breaches of, 17
  - foreign liaison, 21
  - Australian Signals Directorate (ASD)
    - AUSTRAC information access and use, 34
    - inquiries relating to, 7, 13–14
    - inspections of, 27–9, 34
    - intelligence on Australian persons, 23–4
    - Ministerial authorisations, 27–8
    - presumption of nationality, 24
    - privacy rules compliance, 24
    - role and functions, 5
  - Australian Transaction Reports and Analysis Centre (AUSTRAC), intelligence agency access to and use of information, 33–4
  - Australians *see* Australian persons
  - Aviation Security Identification Cards, 39
- ## B
- Blight, Jake, 46

## C

Canadian Privy Council Office, 9, 45  
case studies, 39  
changes in agency procedures *see*  
    procedural changes as a result of  
    IGIS recommendations  
coercive powers, 13  
Commonwealth Disability Strategy, 51  
*Commonwealth Electoral Act 1918* reporting  
    requirements, 50  
Commonwealth Indigenous Procurement  
    Policy, 49  
Commonwealth Ombudsman, 9, 37, 45, 48  
Commonwealth Procurement Rules, 49  
complaints handling  
    case studies, 39  
    complaints handled administratively,  
        9, 38  
    non-visa related, 36–7, 38, 39  
    other contacts with the office, 37, 38  
    performance discussion, 9, 35–9  
    recruitment complaints, 39  
    statistics, 35–6  
    timeliness, 7  
    visa security assessment related, 9, 36,  
        37–8  
    *see also* inquiries  
consultants, 50  
contact details, inside front cover  
corporate and operational planning, 46  
corporate governance, 46–8  
corporate plan, 3, 12  
correction to 2014–15 Annual Report, 51

*Crimes Act 1914*, 32

cross-agency inspections, 32–4 *see also*  
    inspections

cyber project, 32–3

## D

Defence intelligence agencies, 4–5

Defence Intelligence Organisation (DIO), 30  
    AUSTRAC information access and use, 34  
    inspections of, 30–1, 34  
    privacy guidelines compliance, 31  
    role and functions, 4–5

Defence Signals Directorate (DSD) *see*  
    Australian Signals Directorate (ASD)

Department of Immigration and Border  
    Protection, 37–8

Department of the Prime Minister and  
    Cabinet, 50

detention warrants, 18

disability reporting, 50–1

## E

ecologically sustainable development, 50

effecting change in agencies *see*  
    procedural changes as a result of  
    IGIS recommendations

efficiency dividend exemption, v

emergency authorisations, 26

engagement of IGIS with other agencies,  
    8–9, 43–5

enterprise agreements, 49

entity resource statement, 74–5

environmental performance, 50

ethical standards, 47

exchange of information, 21, 25

exempt contracts, 50

## F

finance law compliance, 50

financial intelligence information, 33–4

financial performance

entity resource statement, 74–5

resources for outcome, 10–11, 74–5

summary, 10–11

financial statements, 53–72

firearms, 26–7

force, use of, 19

foreign intelligence collection review, 33

foreign liaisons, exchange of information with, 21, 25

fraud control, 47–8

*Freedom of information Act 1982*, 3, 42–3

OIGIS as exempt agency, 50

functions *see* roles and functions

## G

gender balance of staff, 49

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

glossary, 84

## H

human resources management, 48–9 *see*  
*also* staff

human rights and discrimination matters,  
38 *see also* Australian Human Rights  
Commission

human source operations

ASIO, 16

ASIS, 25

## I

identified person warrants, 17, 18

identities, assumed, 32

inquiries

acceptance of recommendations by  
agencies, 7, 14 *see also* procedural  
changes

employment of persons for a particular  
inquiry, 48

IGIS function and powers, 12–13

performance discussion, 12–14

results against performance criteria, 7

statistics, 13

timeliness, 7

inquiries by parliamentary committees,  
submissions by IGIS, 41–2

inspections, 9

AGO activities, 29–30

ASD activities, 27–9

ASIO activities, 15–23

ASIS activities, 24–7

AUSTRAC access and use, 33–4

cross-agency inspections, 32–4

DIO activities, 30–1

ONA activities, 31–2

overview of activities, 14–15

- privacy rules compliance, 24, 26, 30, 31, 32
- results against performance criteria, 7
- Inspector-General of Intelligence and Security
  - powers, 12–13
  - purpose, 3, 6–7
  - review of year, v
  - role and functions, 2–3, 6–7
  - statutory officer, 46
- Inspector-General of Intelligence and Security Act 1986*, iv, 2, 12–13
  - section 32AA delegations, 14, 48
  - section 8(1)(d) or 8(3)(c) inquiries, 14
  - subsection 32(3) employment, 14, 48
- intelligence agencies, 3–5
  - AUSTRAC information access and use, 33–4
  - complaints against agencies *see* complaints handling; inquiries
  - cross-agency inspections, 32–4 *see also* inspections
  - IGIS engagement with, 8, 43–4
  - limits on functions, 23
  - Ministerial authorisations, 23–4, 25, 26
  - recruitment complaints, 39
  - see also names of agencies*
- Intelligence Services Act 2001*, 23–4
  - limits on intelligence agencies' functions, 23
  - privacy rules, 24
- internal audit, 47
- international engagement, 9, 45
- Internet home page, *inside front cover*

## J

- joint teams, 33
- journalist information warrants, 18
- judicial decisions, 48

## L

- legal representative attendance at ASIO interviews, 23
- legislation (enabling Act), 2, 3
- legislative changes, v
- letter of transmittal, i
- liaising with other accountability or integrity agencies
  - performance discussion, 44–5
- Lindt Café siege, 8, 42

## M

- Maritime Security Identification Cards, 39
- market research, 50
- ministerial and other authorisations to collect intelligence, 23–4, 25, 26
- Ministerial submissions by ASIO, 20

## N

- National Disability Strategy, 51
- National Security Legislation Amendment Bill (No. 1) 2014, 21
- nationality, presumption of, 24
- New Zealand Inspector-General of Intelligence and Security, 9, 45
- non-salary benefits, 49
- notifiable incidents (WHS), 48

## O

Office of Migration Agents Registration Authority, 37–8

Office of National Assessments (ONA)

- AUSTRAC information access and use, 34
- inspections of, 31–2, 34
- privacy guidelines compliance, 32
- role and functions, 4

Ombudsman, 9, 37, 45, 48

operational files (ASIS), review of, 25

operational planning (OIGIS), 46

organisational structure, 46

outcome and program, 2–3

outreach program *see* presentations and outreach

overview by Inspector-General, v

overview of activities, 2–5

## P

parliamentary committees

- advice to (performance discussion), 41–2

Parliamentary Joint Committee on Intelligence and Security inquiries, 8, 42

performance

- analysis of performance against purpose, 9
- annual performance statement, 6
- entity resource statement, 74–5
- financial performance summary, 10–11
- performance summary, 6–11
- resources for outcomes, 10–11

- results against performance criteria, 7–9

results discussion:

- Activity 1, Conducting inquiries, 12–14
- Activity 2, Undertaking inspections, 14–34
- Activity 3, Responding to complaints, 35–9
- Activity 4, Public Interest Disclosures, 40–1
- Activity 5, Advice to parliamentary committees and others, 41–2
- Activity 6, Evidence to the AAT and the Australian Information Commissioner, 42–3
- Activity 7, Presentations and outreach, 43–4
- Activity 8, Liaising with other accountability or integrity agencies, 44–5

performance pay, 49

personal security *see* protective security

planning (OIGIS), 46, 47

Portfolio Budget Statements, 2, 7, 8

portfolio relationship, 2

presentations and outreach, v, 8, 9

- performance discussion, 43–4

presumption of nationality, 24

Prime Minister, 2

privacy rules compliance, 24, 26, 30, 31, 32

procedural changes resulting from IGIS recommendations

- ASD, 8
- results against performance criteria, 8–9

procurement, 50

protective security, 47



*Public Governance, Performance and Accountability Act 2013*, iv, 6, 47, 50

*Public Interest Disclosure Act 2013*, 3, 40  
statutory review, 8, 41, 42

Public Interest Disclosure matters, 7, 8  
performance discussion, 40–1

purchasing, 49

purpose, 3, 6–7

## Q

questioning and detention warrants, 18

## R

recordkeeping

ASIO, 21

review of ASIS operational files, 25

recruitment complaints, 39

remuneration

non-salary benefits, 49

performance pay, 49

salary scale, 76

SES, 48

resources for outcome, 10–11, 74–5

risk management, 47–8

roles and functions

intelligence agencies, 3–5

OIGIS, 2–3, 6–7

## S

salary ranges, 76

search warrants, 17, 38, 39

section 24(1) determinations, 48, 49

security assessments by ASIO, 21, 39

complaints, 9, 36, 37–8

Senate Standing Committee on Finance  
and Public Administration, 42

senior executive, 46

Senior Executive Service (SES) officers, 48

senior management committees, 46

small business participation in  
procurement, 49

Special Intelligence Operations, 19

staff

average staffing level, 75

employment arrangements, 49

employment of persons for a particular  
inquiry, 48

gender balance, 49

non-salary benefits, 49

numbers and profile, 48–9

salary scale, 76

training and development, 49

Stone, Hon Margaret, 2, 46 *see also*  
Inspector-General of Intelligence  
and Security

submissions to inquiries and reviews, 41–2

## T

*Taxation Administration Act 1953*, 20

taxation information, 20

*Telecommunications (Interception and  
Access) Act 1979*

ASD compliance, 29

ASIO compliance, 16–17

telecommunications data, 19–20

telecommunications interception warrants,  
16–17

telecommunications testing activity, 29

Thom, Vivienne, 46

timeliness, 7

training and development (OIGIS), 49

## U

use of force, 19

## V

visa security assessment processes

complaints, 9, 36, 37–8

## W

weapons use and issues

ASIS, 26–7

website address, inside front cover

whistleblower protection scheme *see*  
Public Interest Disclosure matters

Willing, Annette, 46

*Work Health and Safety Act 2011*

ASIO and ASIS reporting exemptions, 33

reporting (OIGIS), 48



