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

Annual report:

ISSN: 1030-4657

© Commonwealth of Australia 2015

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.

Design and typesetting by Spectrum Graphics
sg.com.au

Printed by New Millennium Print
Dear Prime Minister

I am pleased to present my annual report for the period 1 July 2014–30 June 2015.

This report has been prepared in accordance with section 35 of the Inspector-General of Intelligence and Security Act 1986 and reflects the Requirements for annual reports – for departments, executive agencies and other non-corporate Commonwealth entities, as approved by the Joint Committee of Public Accounts and Audit in June 2015.

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

1st October 2015
Contents

Letter of transmittal

Glossary

Part One

Overview

The role of the Inspector-General of Intelligence and Security 1
The intelligence agencies 2
The year in review - highlights 3

Part Two

Performance

Outcomes and programs 8
Performance indicators 8
Agency Engagement 9
Inquiries 9
Complaints and contacts 10
IGIS role in FOI and Archives matters 19
Effecting change in agencies 19
Overview of inspection activities 19
Inspection of ASIO activities 21
Inspection of agencies subject to the Intelligence Services Act 2001 30
Inspection of ASIS activities 32
Inspection of ASD activities 35
Inspection of AGO activities 37
Monitoring DIO and ONA 38
Cross-agency inspections 38
Summary of IGIS financial performance and resources for outcomes (PGPA Act) 40
Part Three
Management and Accountability

- Corporate governance
- Management of human resources
- Other information

Part Four
Financial Statements

Part Five
Annexures

- Annex 1: Summary of inquiries and complaints
- Annex 2: Salary ranges for APS employees in OIGIS in 2014–15
- Annex 3: Agency resource statements
- Annex 4: Requirements for annual reports
- Index
# Glossary

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAT</td>
<td>Administrative Appeals Tribunal</td>
</tr>
<tr>
<td>AFP</td>
<td>Australian Federal Police</td>
</tr>
<tr>
<td>AGO</td>
<td>Australian Geospatial-Intelligence Organisation</td>
</tr>
<tr>
<td>AHRC</td>
<td>Australian Human Rights Commission</td>
</tr>
<tr>
<td>ASD</td>
<td>Australian Signals Directorate</td>
</tr>
<tr>
<td>AML/CTF Act</td>
<td>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</td>
</tr>
<tr>
<td>APS</td>
<td>Australian Public Service</td>
</tr>
<tr>
<td>ASIO</td>
<td>Australian Security Intelligence Organisation</td>
</tr>
<tr>
<td>ASIO Act</td>
<td>Australian Security Intelligence Organisation Act 1979</td>
</tr>
<tr>
<td>ASIS</td>
<td>Australian Secret Intelligence Service</td>
</tr>
<tr>
<td>AUSTRAC</td>
<td>Australian Transaction Reports and Analysis Centre</td>
</tr>
<tr>
<td>DIBP</td>
<td>Department of Immigration and Border Protection</td>
</tr>
<tr>
<td>DIO</td>
<td>Defence Intelligence Organisation</td>
</tr>
<tr>
<td>FOI</td>
<td>Freedom of Information</td>
</tr>
<tr>
<td>FOI Act</td>
<td>Freedom of Information Act 1982</td>
</tr>
<tr>
<td>IGIS</td>
<td>Inspector-General of Intelligence and Security</td>
</tr>
<tr>
<td>IGIS Act</td>
<td>Inspector-General of Intelligence and Security Act 1986</td>
</tr>
<tr>
<td>ISA</td>
<td>Intelligence Services Act 2001</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>OIGIS</td>
<td>Office of the Inspector-General of Intelligence and Security</td>
</tr>
<tr>
<td>ONA</td>
<td>Office of National Assessments</td>
</tr>
<tr>
<td>ONA Act</td>
<td>Office of National Assessments Act 1977</td>
</tr>
<tr>
<td>PGPA Act</td>
<td>Public Governance, Performance and Accountability Act 2013</td>
</tr>
<tr>
<td>PID Act</td>
<td>Public Interest Disclosure Act 2013</td>
</tr>
<tr>
<td>PJCIS</td>
<td>Parliamentary Joint Committee on Intelligence and Security</td>
</tr>
<tr>
<td>SES</td>
<td>Senior Executive Service</td>
</tr>
<tr>
<td>TIA Act</td>
<td>Telecommunications (Interception and Access) Act 1979</td>
</tr>
<tr>
<td>WHS Act</td>
<td>Work Health and Safety Act 2011</td>
</tr>
</tbody>
</table>
The role of the Inspector-General of Intelligence and Security

The Inspector-General of Intelligence and Security (IGIS) is an independent statutory office established by the Inspector-General of Intelligence and Security Act 1986 (IGIS Act) which commenced on 1 February 1987. Dr Vivienne Thom was appointed as Inspector-General for a term of five years from 19 July 2010 and held the office throughout the reporting period. Shortly after the end of the reporting period the Hon Margaret Stone was appointed for a five year term from 24 August 2015.

The Office of the IGIS (OIGIS) is situated 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 IGIS is not subject to general direction from the Prime Minister, or other ministers, on how responsibilities under the IGIS Act should be carried out.

The role of the IGIS is set out in the IGIS Act and is, broadly, to assist ministers in overseeing and reviewing the legality and propriety of Australian intelligence agencies’ activities, to assist ministers in ensuring that these activities are consistent with human rights, and to assist the Government in assuring the Parliament and the public that intelligence and security matters relating to Commonwealth agencies are open to scrutiny.

Regular inspections of the intelligence agencies are designed to identify issues, including with agencies’ governance and control frameworks, before there is a requirement for major remedial action.

IGIS’s inspection role is complemented by an inquiry function. In undertaking inquiries the IGIS has strong investigative powers, akin to those of a royal commission, including 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 an action taken by an intelligence agency.

The IGIS also has a role under the Archives Act 1983 and the Freedom of Information Act 1982 (FOI Act) to provide expert evidence to the Administrative Appeals Tribunal (AAT) and the Information Commissioner in relation to national security, defence, international relations and confidential foreign government communications exemptions.

The role and functions of the IGIS are an important part of the overall accountability framework applied to the intelligence agencies. The focus of the IGIS on intelligence agencies’ operational activities complements the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and Australian National Audit Office oversight of other aspects of governance in those agencies.
The 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 security.

The Organisation’s functions are set out in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). ASIO is also subject to guidelines issued by the Attorney-General under the ASIO Act.

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 published 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. ONA also has responsibility for open source collection through the Open Source Centre.

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.

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 in 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.

The Minister for Defence is responsible for these Defence agencies.

The year in review – highlights

The reporting period was a time of intense activity for the office. The Government introduced a national security legislative reform program with amendments that substantially affected the powers of the intelligence agencies and oversight arrangements. The office was invited to provide submissions and appear before four PJCIS inquiries related to these reforms.

The office had to design and implement new oversight programs as a result of this new legislation. The changes required a re-prioritisation of our work program and a comprehensive revision of existing inspection methodology to focus on the use of the new powers and higher risk activities. By the end of the reporting period the office had new programs in place and had inspected the agencies’ use of the new and amended powers.

The Government announced increased funding for the office as part of the National Security – additional counter-terrorism funding measure. The additional funding allowed for the recruitment of five additional staff members to enable the office to continue to provide a comprehensive and effective oversight program. The Government also announced that the office would be exempt from the efficiency dividend from 2015–16. The office had no difficulty in attracting skilled and experienced applicants for the positions. During the year the office engaged a number of new recruits and also secondees from other agencies. An external provider was engaged to deliver advanced investigation training to most staff and the internal training program continued.

In July 2014 the Inspector-General was invited to speak at the 9th International Intelligence Review Agency Conference held in London. A key theme of the conference was how oversight regimes needed to be more transparent to enhance public credibility. In the two years since the previous conference many agencies had developed outwardly focused media strategies and were exploring ways of informing the public about their work.

1 The National Security Legislation Amendment Act (No.1) 2014 renamed the Defence Imagery and Geospatial Organisation as the Australian Geospatial-Intelligence Organisation and the Defence Signals Directorate as the Australian Signals Directorate.
The challenge of ensuring that oversight is transparent continues in Australia. The office conducted two major inquiries: one into ASIS and the other into activities of ASD. Details are given elsewhere in this report. It is not possible to publish detailed reports about these inquiries because to do so could prejudice security. It is difficult for the office to continue to demonstrate rigorous and credible oversight given the strict limitations on public reporting. Both inquiries found areas of concern within the agencies and both resulted in a number of recommendations. ASIS accepted all recommendations and has been diligent in their implementation. The final report of the ASD inquiry was provided to ASD after the conclusion of the present reporting period. ASD's response to the inquiry is a subject for the next annual report. The Inspector-General is required to continue to monitor and report on the adequacy of any actions that are taken by the agencies in response to these inquiries.

Legislative changes

Amendments to intelligence agency powers and oversight requirements were made through a number of pieces of legislation enacted during the reporting period.

National Security Legislation Amendment Act (No. 1) 2014

The National Security Legislation Amendment Act (No. 1) 2014 commenced in October 2014. It made a range of changes to the Australian Security Intelligence Organisation Act 1979 and the Intelligence Services Act 2001. Some of the key measures include:

- changes to ASIO’s employment framework to bring it more into line with that of the Australian Public Service, and creation of a category of people termed ‘ASIO affiliates’ who can exercise certain powers under the ASIO Act
- expanding ASIO’s warrant-based intelligence collection powers (including expanding the definition of ‘computer’, and introducing a new single surveillance device warrant and an identified person warrant)
- authorising people executing ASIO warrants to use force against persons
- establishing a regime for authorising Special Intelligence Operations (SIOs)
- allowing ASIS to collect intelligence on Australian persons involved in activities in relation to its operational security, and to cooperate with ASIO without ministerial authorisation when undertaking certain intelligence collection activities
- allowing ASIS to train certain additional individuals in the use of weapons and self-defence techniques
- introducing new offences, and updating existing ones, related to the protection of sensitive intelligence-related information, and amending secrecy provisions to make it clear there is no legal barrier to concerned staff or members of the public raising matters with the IGIS.

The changes are accompanied by increased reporting and notification requirements to assist the IGIS in conducting effective oversight. These legislative requirements include:

- ASIO notifying the IGIS if force is used against a person in the execution of a warrant
- ASIO reporting to the Attorney-General on whether anything done in the execution of a warrant materially interfered with, interrupted or obstructed the lawful use by other persons of a computer or device
- ASIO notifying the IGIS if a SIO is authorised
- ASIO providing the Attorney-General and IGIS with a written report on any authorised SIO which must include information on the extent to which the SIO has assisted ASIO in the performance of relevant functions, and whether any conduct of a participant in the SIO caused or involved death, injury, a sexual offence or loss of or damage to property
ASIS notifying the IGIS when it undertakes certain activity in support of ASIO’s functions, and ASIS retaining a copy of any notice about ASIO requiring production of intelligence on an Australian person or class of Australian persons for inspection on request by the IGIS.

We have liaised closely with agencies in the development of notification and reporting practices, guidance and training material, and inspection programs to ensure strong oversight of the new powers, and will continue to pay close attention to these matters in the period ahead.

Review of the Attorney-General’s Guidelines issued under the ASIO Act

As part of its review of the National Security Legislation Amendment Bill (No. 1) 2014, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) recommended that the Government initiate a review of the Attorney-General’s Guidelines issued under section 8A of the ASIO Act, 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. In its public response to the PJCIS’s report on the Bill, the Government agreed to this recommendation stating that it would request ASIO and the Attorney-General’s Department to undertake the review.

The IGIS has a strong interest in this review and anticipates providing input as it progresses.

Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014

The Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014 was enacted on 3 November 2014. It makes amendments to a range of national security and counter-terrorism related legislation focusing primarily on measures to address the threat of ‘foreign fighters’. The matters of key relevance to IGIS oversight include:

- changes to ASIO’s questioning and detention legislative regime including extension of the sunset date to 7 September 2018, lowering the threshold for questioning warrants, and amending the provision relating to use of force by police in the execution of a questioning warrant
- the amendment of the definition of ‘security’ in the ASIO Act that occurred through changes to various offences, particularly those relating to foreign incursions
- ASIO’s role under new powers relating to cancellation of welfare payments, cancellation of visas on security grounds and suspension of passports.

The IGIS is overseeing ASIO’s role in these matters as part of our ongoing inspection and review activities.

Counter-Terrorism Legislation Amendment Act (No. 1) 2014

The Counter-Terrorism Legislation Amendment Act (No. 1) 2014 was enacted in December 2014. Schedule 2 of the Act, which commenced on 13 December 2014, amends the Intelligence Services Act 2001 in two areas:

- to increase ASIS’s ability to provide assistance to the Australian Defence Force (ADF) in support of military operations and its cooperation with the ADF on intelligence matters (by making it clear this is a specific statutory function of ASIS and enabling class agreements and class authorisations in relation to that function)
- to address practical limitations in the arrangements for emergency ministerial authorisations which apply to ASIS, ASD and AGO, including through enabling oral authorisations by Ministers, authorisations by the agency head where a relevant minister is unavailable, and agreement by the Director-General of Security where the Attorney-General is unavailable.
In order to address concerns raised by the PJCIS in its review of the Bill, the legislation includes detailed notification and reporting requirements for both the relevant agencies and the IGIS, including requirements for:

▶ the agency head to retain records of relevant documentation relating to ASIS support for the ADF (ministerial authorisation, Defence Minister request and Attorney-General agreement)
▶ the agency head to give the IGIS a written record of any oral emergency ministerial authorisation
▶ the agency head to give the IGIS notification and copies of documentation when emergency authorisations are given when the Attorney-General is unavailable, or when an agency head makes an emergency authorisation in the absence of relevant Ministers
▶ the IGIS to provide a report to the relevant Minister on agency heads’ compliance with the legislative requirements in giving emergency authorisations, and to advise the PJCIS of the conclusions in any such report.

The IGIS is paying close attention to these matters in the course of ongoing inspection and review activities.

**Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015**

The Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 was enacted in April 2015, with the substantive provisions commencing on 13 October 2015.

In addition to ongoing oversight of ASIO’s access to and retention of information, the IGIS will have a specific role under this legislation. The legislation includes particular measures relating to identification of journalists’ sources. Under this regime, ASIO is prohibited from authorising disclosure of a journalist’s or their employer’s telecommunications data for the purpose of identifying a source of the journalist without a warrant issued by the Attorney-General.

In line with recommendations of the PJCIS, the Act includes oversight and reporting obligations relating to the journalist source provisions, including for:

▶ the Director-General of ASIO to give a copy of the warrant and any authorisation under the warrant to the IGIS
▶ the Attorney-General to provide to the PJCIS a copy of any IGIS report on an inquiry or inspection under the IGIS Act relating to a journalist information warrant or authorisation, and for the PJCIS to request a briefing from the IGIS on those matters.

Our office will ensure appropriate procedures are in place for the IGIS’s role under these provisions prior to their commencement.

**Parliamentary oversight**


**Submissions to inquiries and reviews**

The Parliamentary Joint Committee on Intelligence and Security conducted a number of inquiries in 2014–15 and invited the Inspector-General to make a submission and appear before the Committee on a number of occasions:

▶ On 4 August 2014 the IGIS made a submission to the Inquiry into the National Security Legislation Amendment Bill (No. 1) 2014 and appeared before the committee on 15 August 2014.
▶ On 1 October 2014 the IGIS made a submission to the Inquiry into the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014 and appeared before the committee on 2 October 2014.
On 10 November 2014 the IGIS made a submission to the Inquiry into the Counter-Terrorism Legislation Amendment (No. 1) Bill 2014 and appeared before the committee on 13 November 2014.

On 3 December 2014 the IGIS made a submission to the Review of Administration and Expenditure No. 13 (2014–15) Australian Intelligence Agencies and appeared before the committee at a private hearing on 19 March 2015.

On 21 January 2015 the IGIS made a submission to the Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 and appeared before the committee at a hearing on 29 January 2015.

The Committee commented on a number of occasions that the members appreciate the submissions and evidence of the IGIS given its oversight role.

Outcomes and programs

The 2014–15 Portfolio Budget Statements provided a strategic direction statement with one planned outcome for the Office of the Inspector-General of Intelligence and Security. That outcome was:

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 employed to achieve this outcome were:

▶ to continue the agency’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 of a non-intelligence agency.

The single program outcome reflects the small size of the agency and the relatively narrow focus of its activities.

Program Deliverables

The program deliverables include:

▶ conducting own motion inquiries as appropriate
▶ undertaking a comprehensive inspection and visits program to monitor and review casework
▶ providing effective and timely responses to complaints or referrals received from members of the public, ministers or members of parliament
▶ undertaking presentations to new and existing members of the intelligence agencies to ensure an awareness and understanding of their responsibilities and accountability
▶ liaising with other accountability or integrity agencies in Australia and overseas.

Performance indicators

The effectiveness of the office is assessed against four key performance indicators. These measures take into account the unique role and functions of the office as a specialised review body:

▶ the breadth and depth of inspection work undertaken
▶ the timeliness of completion of inquiries or complaint resolution
▶ the level of acceptance by agencies, complainants and ministers of findings and recommendations of inquiries conducted
▶ the extent to which there has been change within the agencies as a result of the activities of the office.
Agency Engagement

The Inspector-General met 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 where appropriate.

Each agency has also established regular points of contact to facilitate our visits and to coordinate our various requirements, while within the OIGIS, 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 the work of the office during the 2014–15 reporting period.

Outreach

Each year, OIGIS staff deliver presentations to staff in the intelligence agencies. These presentations provide a good opportunity to explain the role and functions of the office and to discuss matters relating to compliance, professionalism, accountability and ethical conduct. In the reporting period, we delivered a total of 13 presentations. Of these, five were to staff in the intelligence agencies, including in regional offices and other sites outside of Canberra; and eight were to external groups.

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 University’s National Security College and the Safeguarding Australia 2015 Conference.

The Assistant Inspector-General, Jake Blight, presented at the Department of Defence Senior Intelligence Managers’ Course, the ADF Advanced Intelligence Course as well as at the Australian National University as a guest lecturer.

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

Inquiries

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 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 a particular 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.
Inquiry into the management of weapons by ASIS in a particular location

During 2014–15 the Inspector-General completed one inquiry that had commenced in June 2014 into the management of weapons by ASIS in a particular location. It is not possible to publish further details of this inquiry as to do so could prejudice security or Australia’s relations with other countries. ASIS agreed to all thirteen of the report’s recommendations. ASIS reported its progress in implementation of the recommendations and the Inspector-General was satisfied that senior management had taken actions that demonstrated a strong commitment to reform.

Inquiry into certain ASD actions

In February 2015 the Inspector-General initiated an inquiry into certain actions of ASD. The report was finalised shortly after the end of the reporting period. It will be further addressed in the next annual report.

Complaints and contacts

We consider a matter to be a ‘complaint’ if it concerns a credible allegation about illegality or impropriety in relation to an action of an intelligence agency. Complaints can be made orally or in writing.

Each contact made with the office is assessed to determine whether it falls within the functions of the office and what is the most appropriate course of action. Where it is assessed that a complaint justifies further action, it will be handled administratively in the first instance. Contacts are also assessed to determine whether they should be handled under the Public Interest Disclosure scheme.

In most cases complaints and other matters can be resolved quite quickly and efficiently by IGIS staff speaking to the relevant agency or looking at their records. This approach can resolve 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 also help the Inspector-General to decide whether to pursue an inquiry for more serious or complex matters.

Notwithstanding how a matter is handled, all persons contacting the office are advised of the actions taken, and the outcomes, to the extent possible.

For approaches about delay with 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, where an individual has previously approached the office, whether six months have passed since previous inquiries were made. Approaches about delay with visa-related security assessments that do not meet these criteria are counted as ‘contacts’ (see below).

In 2014–15, IGIS received a total of 496 complaints, of which 473 were about delay with visa-related security assessments and 23 were non visa-related (see also Annex 1 Table 1.2).

In 2013–14, IGIS received a total of 504 complaints, of which 487 were about visa-related security assessments and 17 concerned non visa-related matters.

In 2012–13, IGIS received a total of 375 complaints, of which 361 were about visa-related security assessments and 14 concerned non visa-related matters.

The number of visa-related complaints has remained fairly stable. The number of non-visa matters which were treated by our office as complaints has increased somewhat but the number still remains relatively low.

Complaints about security assessments for visa applicants

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 request a change in the priority of processing of cases, or request that any particular case be expedited. However, where visa applicants have reasonable concerns that an error may have occurred, we examine ASIO’s processes.

During 2014–15 we continued to focus on ASIO’s handling of visa security assessments because of the significant impact this can have on individuals. We continued to directly access ASIO’s systems as well as increase liaison with other government stakeholders including the Department of Immigration and Border Protection (Immigration) and the Office of the Commonwealth Ombudsman. Three OGIS staff members attended a familiarisation visit of the Villawood Immigration Detention Centre in Sydney in 2015.

In cases where a complaint is about delay in relation to a visa application lodged more than 12 months previously, we examined ASIO’s systems to determine whether or not the applicant had been referred to ASIO for a security assessment and, if so, reviewed ASIO’s handling of the matter. In each case, we looked at whether ASIO had acted unreasonably or had made a processing error.

We do not ordinarily advise complainants whether they have or have not been the subject of a security assessment by ASIO, unless this has already been confirmed to them by Immigration or ASIO, or where we have found a significant issue of concern involving ASIO which would justify the office doing so. Where we are satisfied that there is no evidence of error by ASIO, staff will advise complainants of that. While we identify few errors, where we do find ASIO has made an error, we request that it rectify the matter. Where we find that no referral to ASIO has been made, or that one has been made and finalised, we advise the complainant that there is currently no referral with ASIO.

The office received 473 visa security assessment related complaints in 2014–15, a decrease of 14 from 2013–14. This is an average of 40 complaints per month.

The visa complaints inspections identified a small number of issues. In each case ASIO took action to rectify the issue. In one case an inspection found that ASIO had not given advice to Immigration about a particular visa case even though ASIO’s assessment had been completed. This meant Immigration could not progress the case. We brought this to ASIO’s attention and it provided the relevant advice to Immigration and reminded ASIO staff of the need to communicate the outcome of ASIO assessments promptly. Another issue identified related to ensuring that cases are administratively ‘unassigned’ when a staff member who had been assigned the case leaves the area or ceases working on the case for some other reason. If cases are not ‘unassigned’ appropriately they cannot be ‘reassigned’ to another staff member and this can lead to unnecessary delays. ASIO provided further guidance and training to staff on this issue and subsequent inspections indicate an improvement in practice in this area.

Complaints by visa type

As in previous years, complaints about visa security assessments came from a wide variety of individuals, with the largest number of complaints coming from individuals seeking skilled business or work visas (64%). There were also a substantial number of complaints in relation to family reunion visas (18%) and protection or refugee visas (16%).

During the reporting period we received a small number of complaints from individuals who had received adverse security assessments (ASAs) in relation to their visa applications or had their visas cancelled. These individuals were all in immigration detention. OGIS staff examined procedural aspects of the ASAs made by ASIO and did not identify any issues of concern except in the one case highlighted below. ASIO reviews certain categories of Migration Act related adverse and qualified assessments of individuals based in Australia when it becomes aware of new information of sufficient relevance to impact the assessment. Most individuals with an adverse security assessment in immigration detention are able to apply for an administrative review of their security assessment annually (see page 26 on the work of the Independent Reviewer of Adverse Security Assessments).

Visa-related security assessment complaints continue to represent around 95 per cent of complaints made to the IGIS since 2011–12. The main complaint about
Review of an ASIO adverse security assessment for a visa applicant

During the reporting period the office received a complaint from an individual in immigration detention about the adverse security assessment (ASA) they had received in relation to their visa application. As the person’s protection claims had not been processed they were not eligible for a review by the Independent Reviewer of Adverse Security Assessments. In August 2014 the Inspector-General suggested to the Attorney-General’s Department that it would be reasonable for a separate request or arrangement to be made for the Reviewer to review this assessment. This was not agreed to.

The Inspector-General reviewed the person’s ASA as there were no other practical review mechanisms available to that person. The review of ASIO records did not identify any issues that caused the IGIS to suggest that ASIO should reconsider the assessment immediately. From the documents provided to the IGIS the submission did not appear to take into consideration all relevant factors and current circumstances. However, ASIO considered that all relevant factors were considered. The Inspector-General suggested that ASIO review its decision to issue the ASA within 18 months and consider whether any changes in circumstances would change the risk to security.

Non visa-related complaints

We received 23 non visa-related complaints in the reporting period. This is comparable to the seventeen complaints received in 2013–14. Nineteen complaints in this reporting period were about ASIO, while three related to ASIS and one to ASD. All 23 complaints were investigated administratively.

The complaints covered a broad array of matters, including:

- concerns about the manner in which search warrants were executed and related interactions between the subjects of those warrants and ASIO
- the basis for, and processes associated with, several sensitive individual security assessments
- the removal of security clearances from agency employees leading to the termination of their employment
- members of the public making credible claims of detriment caused by the actions of intelligence agencies
- the potential impact of organisational suitability testing results on private sector employment opportunities
- the effectiveness or otherwise of IT security arrangements to protect personal information contained in on-line job applications from prospective employees.
- delays in Aviation Security Identification Card (ASIC) and Maritime Security Identification Card (MSIC) security checks.

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 public interest disclosure scheme are summarised on page 16.
Execution of an ASIO search warrant

An individual whose family home had been the subject of an overt ASIO entry and search warrant earlier that day made a complaint about the conduct of that search. The complainant alleged that the entry into the premises had been made in an unnecessarily aggressive manner causing significant distress to a young child; that the ASIO officers conducting the search refused to personally identify themselves; and that no timeframe was provided for the return of seized materials.

We sought a briefing on the execution of this and several other search warrants which had also been executed on the same day. OIGIS staff reviewed internal ASIO guidance on how operations of this kind should be planned and conducted, inspected relevant operational files, logs and running sheets, and also viewed a video recording which had been made as the search of the premises commenced.

The video did not record the entry to the premises, so we were unable to reach a firm view on the manner of entry. We suggested to ASIO that in future it should ensure that such recordings should commence prior to entry being effected.

Despite this deficiency, the video recording confirmed that the complainant was properly advised of the purpose of the persons who had entered the premises, and that entry into the premises was lawfully authorised under a warrant.

While the unexpected entry into a house of a large number of individuals in the early hours of the morning would likely cause alarm or disquiet to any person, regardless of age, it seemed from the material available, that the child who was present was given appropriate care and attention until such time as other family members could arrive at the premises.

In respect of the other matters raised, we found that the ASIO team leader had properly identified himself by providing his name and a contact number, and that while other ASIO officers present did not provide their names, they could nonetheless be identified for accountability purposes, should the need arise, as each carried a unique identification number.

The complainant also advised us that ASIO had provided the household with an incorrect ASIO phone number. When OIGIS asked ASIO to look into the matter, ASIO confirmed that an incorrect phone number was inadvertently given to individuals at all Sydney addresses where search warrants were executed on that date. At OIGIS request, ASIO ensured all those affected by the error were provided the correct contact number.

On the question of the seized goods, IGIS was satisfied that it was reasonable for the ASIO team leader not to provide a definite timeframe for their return on the day the warrant was executed, and that appropriate arrangements had been put in place to facilitate further discussion on the subject, at a later date.
Misconduct investigation

An ASIS employee contacted us with concerns about the outcome of a misconduct investigation conducted by ASIS. After examining records and discussing the case with relevant staff, it appeared that the misconduct investigation and recommendation were appropriate. However the complainant had raised similar concerns with ASIS some years earlier and these were only partially addressed via informal means. The IGIS recommended that ASIS consider particular aspects of the case as ASIS had not given sufficient regard to the seriousness of the issues when they were first raised.

Rowdy neighbours

ASIO’s Canberra-based staff moved into new premises in the second half of the reporting period.

In March 2015, we received a complaint from an individual living in the suburb adjacent to ASIO’s new building. The complainant said that the emergency alarm systems in the new building:

… continually goes off, often in the middle of the night waking our whole family and our neighbours … I have found it hard to find someone who actually cares about the problem as there doesn’t appear to be anyone in the actual building when I have gone down there when the alarms are going off. … This problem has gone on for the last year and must not be allowed to continue.

The complainant suggested that either the alarm systems were faulty or the operators were incompetent, and that ASIO was unresponsive in addressing local residents’ concerns about the resulting noise and disruption caused in their otherwise peaceful neighbourhood.

Following receipt of this complaint we sought and received a detailed briefing from the ASIO senior executive responsible for the new building project on these concerns. This briefing revealed the nature and extent of the problem with the alarms, and also detailed the total number of alarms which had occurred since ASIO took possession of the building, and the number of those alarms which had occurred out of hours.

We also separately reviewed ASIO’s files which indicated that ASIO, the building owner (the Department of Finance), the body responsible for property on which the new ASIO building sits (the National Capital Authority) and the contractor responsible for installing the alarm system, were acutely aware of the issue and were working as quickly as they could to address the issue.

While satisfied with ASIO’s response to the issues which had been raised, we also referred this matter to the Commonwealth Ombudsman, so that the Ombudsman could consider whether the actions of the Department of Finance and the National Capital Authority were also reasonable in the circumstances described above. ASIO advise that the issues associated with the alarm system have now been resolved.

Application for Compensation for Detriment

In December 2014, a former complainant to this office complained about the manner in which ASIO was managing an application submitted by him under the Commonwealth scheme for Compensation for Detriment Caused by Defective Administration (CDDA).

Putting aside the basis or merits of the complainant’s CDDA claim, the complainant raised concerns about the length of time it took ASIO to acknowledge and respond to his CDDA application and the allegedly complex and legalistic nature of the process.

Our investigation of these concerns involved a thorough review of relevant ASIO files, examination of guidance from the Department of Finance and the Commonwealth Ombudsman, and detailed discussions with the senior executive responsible for handling this matter.

At the conclusion of our investigation ASIO acknowledged that it would have been better if this CDDA application had been progressed in a more timely manner and that existing internal arrangements for processing future CDDA claims should be enhanced, including through the allocation of dedicated resources and the development of guidelines to better support staff involved in the process.
The impact of organisational suitability testing on employment with contractors

In February 2015, we received a complaint from an individual seeking employment with several private sector companies which regularly provide contract services to the Department of Defence.

The complainant expressed concern that ASD had blocked his prospective employment on security grounds. The complainant was concerned that those grounds had not been revealed to him, that he therefore had no basis to appeal, and this meant that his career opportunities in his chosen field were greatly diminished.

An examination of this complaint revealed that rather than raising security concerns ASD had raised reservations about the complainant’s organisational suitability (that is, the capacity of the complainant to quickly accept and adapt to the agency’s culture and established work methods).

This judgement was informed by an organisational suitability assessment that relied upon recent psychological and organisational test results.

ASD has an obligation to ensure that it operates as securely, effectively and efficiently as possible, and it is appropriate for ASD to raise concerns with contractors about the suitability or otherwise of prospective employees who will undertake work in a specialised environment.

We informed the complainant that they had been found not to be suitable for employment with the agency and that there was no evidence that ASD has acted unlawfully or without propriety.

Other contacts with the office

We also received around 300 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 200 contacts in the previous reporting period.

The increase might 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 which are actually available to the intelligence agencies.

When we are contacted about matters that fall outside of our jurisdiction, we provide written or verbal advice about the jurisdiction of the office and suggest alternative avenues that may be appropriate, including other complaint-handling bodies, the police and the National Security Hotline. In appropriate cases and with the agreement of the individual concerned we can also pass matters directly to the Commonwealth Ombudsman. In cases where there had been previous contact about matters that had already been assessed, we took no further action unless substantially new and credible information was provided.

Statistics on matters raised are at Annex 1 – Summary of inquiries and complaints.
Public Interest Disclosure scheme

The Public Interest Disclosure Act 2013 (PID Act) is intended to promote integrity and accountability within the Commonwealth public sector including by: encouraging the making of 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 belong or had previously belonged to 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.

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

One of these disclosures was made by a former employee of an intelligence agency who raised concerns about the legality and propriety of operational activities allegedly undertaken by an Australian intelligence agency in cooperation with a foreign intelligence agency in Australia a number of years earlier at a specific location. This matter was investigated under the IGIS Act. There were comprehensive records of activities undertaken at the relevant time and location. On the basis of these records and other inquiries the Inspector-General was satisfied that no evidence existed to substantiate claims that conduct of the kind alleged by the discloser had in fact occurred. The agency concerned has a comprehensive policy and appropriate training in place to prevent the type of misconduct which had been alleged.

The IGIS investigation identified another matter, not raised in the original complaint; this was pursued separately with the agency. In relation to that matter the IGIS recommended the agency undertake specific actions to provide enhanced assurance about relevant past and current practices of the agency. The agency has acted in accordance with this recommendation.

The second disclosure was made by an individual who had previously had a close working relationship with one of the intelligence agencies. This individual was deemed to be a ‘public official’ for the purposes of the PID Act to facilitate investigation of the discloser’s complaint. This matter included a contractual dispute and also raised broader concerns about agency conduct which fell within the ambit of the PID Act.

After a lengthy investigation which was conducted under the IGIS Act, the IGIS found that there were serious gaps in the record keeping of the relevant agency which impeded the IGIS investigation. Some of the discloser’s concerns were serious and IGIS considered that better systems should have been in place to ensure these were detected and addressed earlier. In relation to other matters raised, IGIS considered it was not unreasonable for the agency to rely on the contract signed by the parties when a claim for additional payments was made; and that while there was concern about how another entitlements issue was handled, once it was brought to the agency’s attention, proper action was initiated. At the conclusion of the investigation the agency concerned agreed that valuable lessons had been learnt.

The third public interest disclosure received by this office revolved around claims of workplace bullying and harassment which were allegedly left unaddressed by management; that partiality was shown in the conduct of a functional review and subsequent ‘spill and fill’ selection exercise; and that a manager sought to obtain private advantage by use of their office. This matter was allocated to the agency in question for investigation, with the investigation report being provided to the IGIS at its conclusion.
The investigation of these matters found that responsible line managers had sought to address inappropriate workplace behaviours and that counselling was provided to those involved to enable them to align their behaviour to the expected workplace standard.

The investigation found no evidence that there was anything improper about the functional review and subsequent ‘spill and fill’ process which the discloser had raised concerns about. The report’s author noted that the panel involved in making a recommendation regarding the preferred candidate for the one ongoing position: was comprised of experienced senior staff; did not include a direct line manager from the affected work area; included a member from the recruitment area of the agency; and, had acted in an independent way.

The investigation also concluded that there was no evidence to corroborate claims made by the discloser that an agency staff member had sought to obtain private advantage by use of their office.

The fourth internal disclosure made to the Inspector-General raised issues which had previously been the subject of thorough review, and the new issues raised in the disclosure were found not to meet the PID threshold.

In addition to the four disclosures made directly to the Inspector-General the intelligence agencies advised this office that four PID cases had been processed by the agencies during the reporting period.

In addition to the four disclosures made directly to the Inspector-General the intelligence agencies advised this office that four PID cases had been processed by the agencies during the reporting period.

Investigations were completed in two of these cases prior to 30 June 2015 and reports provided to the Inspector-General on the outcomes:

- An anonymous discloser raised concerns that sensitive information had been ‘leaked’ to a media outlet. Investigation of this concern revealed that this was an authorised rather than an unauthorised disclosure, and that no further action was warranted.

- A discloser alleged that partiality was shown in identifying staff who were to be made voluntary redundancy offers and in how some senior level appointments were made. The resulting investigation did not identify evidence of conduct which could be construed as amounting to maladministration, wastage of public money, or abuse of public trust, as alleged in the original disclosure.

The other two PID disclosures made directly to agencies were not pursued under the PID Act but are being investigated under other relevant Commonwealth laws. These investigations were ongoing as at 30 June 2015. One relates to alleged potential procurement fraud and the other is an allegation which is being investigated as a potential security matter.

**Commonwealth Ombudsman**

The work of the OIGIS complements the work of the Commonwealth Ombudsman and there is a Memorandum of Understanding between the offices. During 2014–15 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 relates to the handling of immigration and visa-related security assessment complaints. Where appropriate OIGIS officers 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, for example in cases where the application was never referred to ASIO for security checks. OIGIS staff also raise any systemic issues that appear to relate to Immigration with the OCO, for example in cases where that has apparently been prolonged delay by Immigration in processing certain visa applications.

This office also liaised closely with OCO during 2014–15 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, IGIS is responsible for overseeing the scheme for the intelligence and security agencies.
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 human rights and discrimination matters relating to an act or practice of the intelligence and security agencies to the IGIS.

In this reporting period the AHRC referred three cases to IGIS. Broadly these cases alleged that:

- the failure by ASIO to provide access to sensitive records to a complainant was contrary to the complainant’s human rights under the United Nations International Covenant on Civil and Political Rights (ICCPR)
- surveillance by ASIO, and interference in the complainant’s personal affairs, was contrary to their human rights under the ICCPR
- the dismissal of an ASIO staff member on security grounds and the lack of any avenue for independent review of that decision was contrary to the International Labour Organization Convention (No.111) concerning Discrimination in Respect of Employment and Occupation.

In respect of the first complaint the Inspector-General found that while there had not been a breach of human rights ASIO had not handled a request for access to open period files as efficiently as it could have. The processing of the request was subject to a number of internal delays and it was apparent that the access request should have been resolved earlier. ASIO may not have prioritised the request appropriately, given the applicant’s personal circumstances. The Inspector-General suggested to ASIO that it apologise for the delays which arose in its handling of the access request. ASIO wrote to the complainant explaining its reasons for the delay but did not make an apology.

The second matter is one that had been investigated by this office on a number of previous occasions. Having regard to all the circumstances the Inspector-General decided that further inquiry into the matter was not warranted.

Investigation into the third matter was ongoing at the end of the 2014–15 reporting period.

Timeliness

As discussed elsewhere in this report, we concluded one inquiry during the 2014–15 reporting period and a further one shortly afterwards.

The first of these inquiries examined the management of weapons by ASIS at a particular overseas location. This inquiry was completed 184 days after it commenced.

The IGIS Act has prescriptive and comprehensive procedural fairness requirements allowing individuals, agency heads and ministers the opportunity to comment on or discuss a report’s findings before the report is finalised. It is not uncommon for these processes and requirements to take longer than the investigative phase of an inquiry and add months to the length an inquiry runs.

All contacts with the office were assessed promptly upon receipt during the reporting period, to determine whether they should be treated as a credible complaint requiring investigation, handled administratively, or referred to another agency (such as the Commonwealth Ombudsman) if they fall outside of IGIS jurisdiction.

We aim to acknowledge a written contact or complaint made to the IGIS within five business days. This benchmark is sometimes exceeded in cases where we are reliant on external inputs to our proposed response that take more than five days to be received, or due to unanticipated staff absences.

Of the 473 complaints about visa security assessments that were handled administratively during 2014–15, around 90 per cent were completed within two weeks of the complaint being received, with the average time taken being nine days.

For the 23 other complaints received and investigated by this office during 2014–15, 21 were finalised and 2 cases remained open as at 30 June 2015. 14 per cent of the finalised cases were completed within two weeks of the complaint being received (compared to 35 per cent in 2013–14), while the average time taken on each
completed case was 52 days (compared to an average of 55 days in 2013–14).

These variations in timeliness for resolving complaints reflects wide differences in the nature of the complaints which the office receives, with common themes arising in many of the complaints we receive about visa security assessments compared to the diversity of complex issues that can arise in other types of complaints. We are also implementing changes to our management of complaints about ASIO to improve our direct access to ASIO information in order to reduce the time it takes to obtain relevant information.

IGIS role in FOI and Archives matters

The Freedom of Information Act 1982 (FOI Act) sets out various exemptions to the requirement for government agencies to provide documents. One of the exemptions applies to documents affecting national security, defence or international relations. Before deciding that a document is not exempt under this provision the Administrative Appeals Tribunal (AAT) and the Information Commissioner are required to seek evidence from the IGIS. There are equivalent provisions in the Archives Act 1983 for the AAT.

In this reporting period the IGIS was called on once by the Information Commissioner to give evidence in an FOI matter. The IGIS was notified by the AAT of two new cases where the IGIS may be required to give evidence. At the end of the reporting period the IGIS had not been called to give evidence in either case. In addition, one case in which there was a possibility the IGIS may need to give further evidence was carried over from the previous reporting period. In that case, Fernandes and National Archives of Australia [2014] AATA 180 (2 April 2014), the IGIS had given evidence about a number of documents. The AAT’s decision that two parts of one contested document could be released was appealed to the Federal Court. On 17 November 2014 the Federal Court remitted the matter to the AAT for reconsideration. The AAT decided it did not need to call upon the IGIS to provide further evidence. On 26 May 2015 the AAT decided that the relevant material should remain exempt.

The number of cases referred to the IGIS by the Information Commissioner and the AAT is similar to previous reporting periods. If the Freedom of Information Amendment (New Arrangements) Bill 2014, currently before the Senate, is passed by Parliament the AAT would have sole jurisdiction for external merits review of FOI decisions which would impact on the IGIS’s future role in these matters.

Effecting change in agencies

Where an inquiry makes recommendations, we obtain advice from agencies as to whether they have been accepted and what, if any, action has been taken as a result. Where appropriate, we also follow up at the end of the reporting period the progress of outstanding recommendations including those from previous years.

Our inspection and complaint activities also provide opportunities for the office to effect change in the intelligence agencies. Some of the changes that have occurred as a result of IGIS inspection and complaint activities are mentioned elsewhere in this report.

Overview of inspection activities

The office regularly examines selected agency records to ensure that the activities of the intelligence agencies comply with the relevant legislative and policy frameworks and to identify issues before there is a need for major remedial action.

These inspections largely focus on the activities of ASIO, ASIS, AGO and ASD. This is because each of these agencies has access to intrusive powers and investigative techniques. In the second half of the reporting period we have focused on activities affected by the implementation and use of new legislative powers.
Implementation of recommendations – 2013 and 2014 Weapons Inquiries

During 2014-15 ASIS finalised the implementation of IGIS recommendations arising from the 2013 Weapons Inquiry. This included:

- Updated weapons related standard operating procedures for all stations where ASIS staff are or may be issued with weapons.
- Revised ASIS Guidelines for the use of weapons and self defence techniques. This was preceded by an extensive briefing process for all staff with weapons qualifications.
- A review of operational environments to identify stations that require weapons and self-defence training.
- New safeguards and controls implemented in all stations where ASIS staff are or may be issued with weapons.

As noted in our previous annual report, in June 2014 the IGIS initiated a further inquiry into the management of weapons by ASIS in a particular location. This followed a serious incident in that location in December 2013.

This inquiry was completed in December 2014. The report of the findings is not able to be made public due to national security and foreign relations considerations.

ASIS accepted all the recommendations from the inquiry and at the end of the reporting period the IGIS was satisfied these recommendations have either already been implemented or are in the process of being implemented.

The IGIS inquiry findings have been communicated widely throughout ASIS. At the invitation of the Director-General of ASIS the IGIS presented her findings to the ASIS senior leadership group and also to all ASIS staff in December 2014.

ASIS is in the process of undertaking change to address areas of concern. This includes:

- the introduction of a compliance branch
- an extensive compliance outreach training program
- widespread consultation with staff
- a review of all ASIS policy and procedures, to be made centrally available on a new platform.

The IGIS reported to the Minister for Foreign Affairs on the status of the implementation of recommendations in June 2015.

Inspection activities relating to DIO and ONA are generally limited to ensuring that their assessments comply with administrative privacy guidelines (which have a similar effect to the privacy rules which apply to ASIS, ASD and AGO).

Inspection activities consider whether or not each agency is acting in accordance with its statutory functions, any guidance provided by the responsible minister and its own internal policies and procedures. Inspection activity is a combination of routine inspections (for example ASIO investigative cases and warrants) and inspection projects that target specific areas.

In the reporting period the relatively high inquiry workload together with amendments to the intelligence agencies’ enabling legislation resulted in prioritisation of inspections work based on a risk management approach.
Inspection of ASIO activities

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, and 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.

Regular inspection of investigative cases

Each month we review a sample of ASIO investigative cases 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 (using less intrusive methods where possible and only progressing to increasingly intrusive methods as required).

Sample selection is oriented to 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.

Another ongoing focus of inspections has been to ensure a high standard of recordkeeping and decision making is maintained, particularly in regard to appropriate guidance being provided by authorising officers to more junior staff.

During 2014–15, we paid particular attention to ASIO’s investigative activities in relation to people under 18 years of age. Although no issues of concern were identified, OGIS staff have highlighted a requirement for improved record keeping and documenting of decisions in these particularly sensitive cases.

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

Human source management

This inspection activity focuses on ensuring the management of ASIO human source operations is both legal and proper. While the details of the results of these inspections are sensitive and cannot be disclosed in a public report, no significant concerns were identified in the inspections that were 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. The authority for these is in the Telecommunications (Interception and Access) Act 1979 (TIA Act) and the ASIO Act for other powers including searches, computer access and surveillance devices.

During this reporting period, inspection of ASIO warrants was primarily undertaken as part of the regular inspection of investigative cases, referred to above. This enables review of the warrant documentation and reporting within the context of the broader investigation. Additionally, we inspect a sample of ASIO foreign intelligence collection warrants on a quarterly basis.

During the reporting period, the Parliament passed the National Security Legislation Amendment Act (No. 1) 2014, which made a number of amendments to the warrant provisions in the ASIO Act. 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.

In order to provide close scrutiny of ASIO’s use of the new and amended warrants under the ASIO Act, in 2015 we undertook a separate
inspection activity to review a sample of relevant ASIO warrants on a quarterly basis.

The new identified person warrants have been and will continue to be a significant focus of this inspection activity. These warrants differ to other ASIO Act warrants as they involve the Attorney-General providing conditional approval for ASIO to use one or more different special powers against the identified person, with a separate authorisation from either the Attorney-General or the Director-General of Security required for the actual use of any of the powers for which conditional approval was provided. As the Director-General is now able to authorise the use of powers that would previously have required the Attorney-General’s approval, we consider this merits close scrutiny by our Office. Of the identified person warrants inspected, the majority of authorisations to use specific powers under approved warrants were given by the Director-General.

We have and intend to continue to pay close attention to those warrants that may authorise actions that relate to third parties, such as the ability to use a third party computer or communication in transit to execute a computer access warrant, and gaining entry to a target premises through a third party premises. Another new power given to ASIO in the reporting period was the use of force against persons where necessary and reasonable to do the things specified in the warrant. As discussed further below this is an area that merits particularly close scrutiny.

In the 2014–15 reporting period, approximately half of the warrants obtained by ASIO were reviewed. Our inspection program 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. In all these cases these errors did not impact on the legality or propriety of the warrant. Remedial actions were taken by ASIO once the administrative errors were identified.

ASIO continued to proactively self-report in relation to breaches or errors in execution of warrant powers. ASIO reported two breaches of the TIA Act and one breach of the ASIO Act:

- One breach occurred when a testing activity resulted in the incorrect connection and interception of a telecommunications service. No communications were intercepted or recorded as a result of this error, which was identified seven minutes after the connection had been actioned. ASIO has established more stringent procedures and advice for staff to ensure a similar error does not occur.

- The second breach was due to a fault of an interception system installed at a telecommunications service provider. This fault resulted in the delivery of non-warranted data to ASIO. ASIO immediately quarantined all data received from the provider and is working to identify the warranted data and purge the non-warranted data. ASIO has appropriately prioritised the significant work required to manage this breach. The provider has replaced its interception system and testing has confirmed that this error does not occur with the new system.

- The third breach occurred when data was collected from a computer that was not specified in the computer access warrant. The Inspector-General was satisfied with ASIO’s explanation of how this occurred and with the remedial action taken, which included prompt action to cease collection and deletion of the small amount of data that had been collected.

While generally satisfied by the overall manner in which warrants are processed, the Inspector-General did identify some additional issues which merit comment.

As noted in previous annual reports, the IGIS has a particular interest in ASIO’s use of B-party warrants because of the potential for intrusive collection of material that is not relevant to security.

B-party warrants were introduced in the TIA Act in 2006. They 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 other interception warrants which can last for six months. B-party warrants can only be issued if ASIO has exhausted
all other practicable means of identifying the telecommunications used or likely to be used by the person of security interest or if the interception of communications made to or from a telecommunications service likely to be used by the person would not otherwise be possible. When introduced, the then Attorney-General in his second reading speech referred to B-party warrants being used ‘as a last resort’ to address the use of ‘evasion techniques’ that would otherwise frustrate interception.

As noted in last year’s Annual Report, the IGIS has been consulting with the Attorney-General’s Department about ASIO’s interpretation of the provisions in the TIA Act that restrict the availability of B-party warrants. This issue has not yet been resolved.

Foreign intelligence collection warrant review

In 2012, we reviewed the Australian intelligence community’s processes for submitting foreign intelligence collection (FIC) warrant requests to the Attorney-General. That review recommended several changes to ASIO processes to aid the Attorney-General’s decision to authorise a warrant.

The recommendations aimed to make ASIO’s warrant requests and revocations more timely and improve the range of information ASIO provided to the Attorney-General to support the proposed activity.

We conducted a review in mid-2014 of ASIO’s FIC warrant files to confirm ASIO’s implementation of the recommendations. The review found ASIO had largely implemented the recommendations of the 2012 inspection and had made substantial improvements to the quality and timeliness of information supplied to the Attorney-General in support of FIC warrant requests.

Questioning and detention warrants

No questioning, or questioning and detention warrants were sought by, or issued to, ASIO during the reporting period.

Use of force

During the reporting period the ASIO Act was amended so that warrants issued under that Act must authorise the use of any force against persons or things that is necessary and reasonable to do the things specified in the warrant. As the Inspector-General said in her submission to the PJCIS inquiry into the National Security Legislation Amendment Bill (No. 1) 2014, ‘the ASIO Act did not [previously] authorise the use of force against persons in the exercise of a search warrant and that this would therefore be a new power… [and] a proper regime of training and oversight is required.’ If force is used against a person in the execution of a warrant under the ASIO Act, ASIO must notify the IGIS and the Minister in writing as soon as practicable after such force is used.

During the reporting period the IGIS received one notification relating to the use of force under an ASIO warrant. The force was exercised by law enforcement officers assisting ASIO in the execution of the warrant. The incident was subject to the usual police internal reporting and review process and there is no indication in the police report that the force was other than reasonable and proportionate for the purpose for which it was exercised.

ASIO provided the IGIS with a verbal briefing on the use of force in that case ten days after the incident, followed by a written notification 12 days after the incident. The IGIS advised ASIO that she expected to be notified of the fact that force has been used in a more prompt manner, noting that a more detailed report of the incident may be provided at a later date. While the ASIO Act does not specify a timeframe, the PJCIS recommended that the IGIS should be notified within 24 hours of any incident in which force is used and get a written report within seven days.

During consideration of the use of force amendment, the PJCIS recommended that the IGIS provide close oversight of the design and execution of training for ASIO officers who may be required to use force during the execution of warrants issued under the ASIO Act.

ASIO anticipates that ASIO officers will only use force in exceptional and urgent circumstances and primarily for self-defence. ASIO recently commenced self-defence training across the Organisation and is looking at developing additional training specifically for officers involved
in the execution of warrants. It remains the IGIS’s view that while such use of force is expected to be rare and used only in exceptional and urgent circumstances, this does not negate the need for suitable training, if anything it increases the need for regular training.

**Special Intelligence Operations**

Special intelligence operations (SIOs) are a new power available to ASIO since October 2014. SIOs are similar to law enforcement ‘controlled operations’. The Attorney-General may authorise a person to engage in authorised conduct, which would otherwise be unlawful.

The Attorney-General must be satisfied of a number of factors set out in section 35C of the ASIO Act, including that an SIO will assist ASIO in the performance of a special intelligence function; the circumstances are such as to justify the conduct of an SIO; unlawful conduct will be limited to the maximum extent possible and will not induce someone to commit an offence that they did not otherwise intend to commit. The Minister must also be satisfied that such conduct will not cause death or serious injury to any person, constitute torture or involve the commission of a sexual offence against any person, or result in significant loss of or serious damage to property.

SIOs may be authorised for periods of up to 12 months. ASIO is required to notify the IGIS when the Attorney-General approves an SIO, and must report to the Attorney-General and IGIS after six months and at the conclusion of the SIO.

As this is a significant new power, we intend to review each SIO that is authorised by the Attorney-General. ASIO has advised that there are security concerns with disclosing the exact number of SIOs. IGIS staff received relevant documents and attended relevant briefings, and did not identify any issues of legality or propriety.

**Access to telecommunications data**

The TIA Act provides the authority for a nominated group of ASIO senior managers to authorise collection of prospective and historical telecommunications data from telecommunications carriers or carriage service providers. Prospective data authorisations provide near real-time location and other subscriber information for the period that an authorisation is in force. The legislative threshold that ASIO is required to meet for access to the data is low; it is that the request is ‘in connection with the performance by ASIO of its functions’. In addition, the Attorney-General’s Guidelines state that investigative activities should be using as little intrusion into personal privacy as is possible, consistent with the performance of ASIO’s functions. As such, a request for access to telecommunications data should only be submitted once less intrusive methods have been attempted, or considered and found to be insufficient.

The **Telecommunications (Interception and Access)** Amendment (Data Retention) Act 2015 was enacted in April 2015, with the substantive provisions commencing on 13 October 2015. The scheme will require carriers to retain specified data for at least two years.

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

Prospective data authorisations reviewed were endorsed by an appropriate senior officer, and 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 a small number of cases, IGIS staff identified errors in compliance with ASIO’s internal approval policy for requests for historical telecommunications data, primarily these errors were: not recording the approval of requests or requests not being approved at the appropriate level. ASIO has undertaken to remind its staff of the relevant internal approval requirements.

During the reporting period we also identified a number of cases where requests for access to prospective data used ambiguous wording that did not adequately explain why less intrusive methods of obtaining the information had not been pursued and/or would not be appropriate
in the particular case. We raised this with ASIO and were provided with additional context as to why access to prospective data had been sought in those cases, and were satisfied that this was consistent with the Attorney-General's Guidelines. ASIO indicated they would remind staff of the need to clearly document whether less intrusive methods have been considered and explain if they are not likely to be effective in a particular case.

Preservation requests

Since late 2012 ASIO and law enforcement agencies have been able to give notice to telecommunications carriers to require them to retain certain stored communications for up to 90 days while ASIO seeks an appropriate warrant to access those communications. These notices are called Preservation Notices, and can only be used where they might assist the Organisation in carrying out its functions of obtaining intelligence relating to security.

Section 158A of the TIA Act specifically provides that the IGIS has functions in relation to providing assurance of compliance by ASIO in respect of preservation notices.

Throughout the reporting period there were a very small number of such notices raised by ASIO. These activities were reviewed as part of our ongoing inspection program and there were no issues of concern identified in relation to those reviewed.

Access to taxation information

Section 355-70 of Schedule 1 to the Taxation Administration Act 1953 provides for a taxation officer authorised by the Commissioner of Taxation or delegate to 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 MOU between the Commissioner of Taxation and the Director-General of Security, the Attorney-General’s Guidelines and ASIO’s internal guidelines and procedures, ensuring that a request for taxation information can only be made when less intrusive means have been exhausted and not yielded the required information.

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 2014–15, ASIO reported that no requests had been made to access ATO information. The ATO made three proactive disclosures to ASIO which will be reviewed in July 2015.

ASIO requests for information from Intelligence Services Act agencies

During the reporting period we finalised an inspection project that was initiated in November 2013 to review ASIO requests for information (RFI) to agencies governed by the Intelligence Services Act 2001 (ISA). The purpose of the project was to provide assurance that ISA agencies were being appropriately informed when requests for information from ASIO related to an Australian person.

During the information gathering phase we identified that while ASD had a robust system for receiving, processing and disseminating RFIs from external agencies, both ASIO and ASIS lacked any form of centralised system of receiving, processing and disseminating RFIs.

Despite this shortcoming, the review was able to conclude that in almost all of the RFIs reviewed, ASIO provided all available information required for ISA agencies to meet their obligations under the ISA. On the single occasion where it was identified that additional information was available but not provided, this omission was based on security grounds.

Relevant agencies were advised that while the Inspector-General was satisfied that ASIO provides sufficient information for ISA agencies to meet their legislative obligations, the introduction of a standard RFI process would improve record keeping, compliance and accountability. It was also suggested RFIs should include a mandatory
field to identify whether the subject is an Australian citizen, permanent resident or visa holder to minimise the risk of unauthorised targeting of an Australian person.

**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 co-operate with foreign authorities approved by the Attorney-General. In general, the types of foreign authorities that are approved by the Attorney-General perform broadly similar functions to ASIO, and include security and intelligence authorities, law enforcement, immigration and border control, and government coordination bodies.

ASIO has internal guidelines that govern the communication of information on Australians and foreign nationals to approved foreign authorities. These guidelines impose an internal framework for assessing and approving the passage of such information. ASIO’s internal requirements vary according to the country, based on factors such as ASIO’s previous experience dealing with authorities of that country and how the foreign authorities manage information received, including in relation to human rights issues.

During 2014–15, we inspected a sample of authorisation documentation and correspondence for such exchanges, both through regular reviews of ASIO investigative cases and through dedicated foreign liaison inspection activities.

Inspection activity focused on ASIO’s intelligence sharing activities where there may be potential additional risks to an individual as a result of their location. During this reporting period, this has been most often in relation to persons involved with the conflict in Syria or other global hotspots. In the case of this elevated risk, it may be appropriate for ASIO officers to escalate the approval for the liaison to a more senior officer. There were no issues of concern identified in relation to those higher risk intelligence exchanges reviewed.

More generally, inspections have identified some cases where ASIO could improve compliance with internal guidelines, particularly in relation to documenting human rights considerations which should be contemplated before exchanging information with foreign authorities.

**Review of submissions to the Attorney-General**

Each quarter we review a range of submissions and briefing notes made by ASIO to the Attorney-General on operational matters. In addition to the other ASIO inspection activities, these reviews continue to be useful in obtaining an overview of legality and propriety issues relevant to high risk activities.

**Independent Reviewer of Adverse Security Assessments**

The role of the Independent Reviewer of Adverse Security Assessments (the Reviewer) is to review ASIO adverse security assessments (ASAs) given to DIBP in relation to people who remain in immigration detention and have been found to engage Australia’s protection obligations under international law and not to be eligible for a permanent protection visa or have had their permanent protection visa cancelled. The Reviewer examines all material relied upon by ASIO as well as other relevant material, and forms an opinion on whether the assessment is an appropriate outcome. The Reviewer provides her recommendations to the Director-General of Security who must respond to the Reviewer. The IGIS also receive copies of the Reviewer’s reports and recommendations.

In the 2014–15 financial year the Reviewer completed 24 reviews of cases that she had not previously considered. Of these 24 cases:

- in six cases the Reviewer found the initial ASA was and remained appropriate.
- In three cases the Reviewer found the ASA was not appropriate and this resulted in ASIO issuing three non-prejudicial assessments
- In six cases the Reviewer formed the view that the ASA was appropriate at the time it was furnished but was no longer appropriate. This resulted in ASIO issuing four qualified assessments and two non-prejudicial assessments.
in five cases ASIO furnished new non-prejudicial or qualified assessments after considering new information referred to it by the Reviewer and on the basis of outcomes from ASIO’s own investigations. As a result ASIO issued two non-prejudicial and three qualified assessments.

In two cases the Reviewer formed the view that there were flaws in ASIO’s assessment such that she was unable to form a view as to the appropriateness of the ASA. In each of these cases ASIO subsequently issued a qualified assessment.

In two cases the Reviewer’s review was well advanced when ASIO issued a new assessment and the Reviewer found the new assessment was appropriate. One resulted in a nonprejudicial assessment and the other a qualified assessment.

In addition there were four cases where ASIO revised an adverse or qualified visa security assessment on its own initiative.

We have observed a significant improvement in ASIO’s approach to proactively reviewing ASAs for individuals in immigration detention since the work of the Reviewer commenced. The work of the Reviewer has brought focus and resources to bear on these cases. While difficult to measure there also appears to be an increase in the quality of decision making; this is a benefit of external review in combination with other factors.

The terms of reference for the Reviewer provide that eligible ASAs are to be reviewed annually. This regular review process provides assurance that if new information comes to light or if relevant circumstances change then a new assessment can be made.

There are some people subject to ASAs in immigration detention who are not eligible for review by the Reviewer because they have not had their protection claims assessed. In these cases ASIO reviews the assessment when new information of sufficient relevance is provided. The IGIS has received complaints from a small number of people in this situation and has examined their cases – see case study earlier.

**ASIO’s investigations of issues-motivated groups**

During the reporting period we conducted an inspection project to look at ASIO’s investigation of Australian issues-motivated groups (IMGs). This inspection did not arise out of any particular complaint or concern, but rather noted that this is an area of consistent public and media interest, and was also particularly relevant in light of the Brisbane G20 summit held in November 2014.

The project found that the overall scale of ASIO’s investigation of groups and individuals that may be associated with issues-motivated groups appeared to be reasonable and justified in the context of ASIO’s statutory functions and its assessments about risk.

The project found no systemic issues, but made a number of observations in relation to specific cases reviewed and matters of best practice.

The project observed a small number of cases where the IGIS considered that broad statements were made about a person’s ‘history’ of involvement in activities of security concern or ‘support for the use of violent protest’. These statements occurred in the context of requests to access information or undertake internally approved investigative activities. The review examined the underlying intelligence base and the IGIS concluded that while there was sufficient justification for the activities undertaken in the relevant cases, it was questionable as to whether the intelligence base did establish a ‘history’ or clearly indicate the ‘support’ as described. It is best practice to clearly articulate what is actually known or suspected about the person’s activities, rather than making general statements that could potentially suggest a stronger justification for investigative activities. The project also identified inconsistencies in record keeping and documentation of reasons for requests to access certain information and in the descriptors used in some of ASIO’s electronic records.

ASIO has advised it will consider those observations to ensure it meets best practice.
Passport cancellations

ASIO may request the cancellation of an Australian passport under the Australian Passports Act 2005 (“Passports Act”) and the Australian Passports Determination 2005 if it suspects on reasonable grounds that the person continuing to hold the passport would be likely to engage in conduct that might prejudice the security of Australia or a foreign country, and the cancellation should occur in order to prevent the person from engaging in the conduct.

During the reporting period we conducted an inspection project to review a sample of ASIO’s submissions to the Attorney-General requesting the cancellation of Australian passports held by individuals assessed to be in or intending to travel to Syria or Iraq. The review focused on whether ASIO’s use of the existing passport cancellation and refusal powers was consistent with the legislation.

Section 14 of the Passports Act makes a distinction between advice provided by ASIO and advice provided by the Director-General of Security, depending on whether the request concerns circumstances relating to a foreign country or whether it concerns prejudice to Australia’s security. The review found that ASIO’s advice to the Minister appeared not to make this distinction in relevant cases. In February 2015, ASIO agreed to review its passport cancellation and refusal ministerial submission templates to better reflect the legislative basis for recommendations under the Passport Act. In June 2015, we reviewed an additional sample of ASIO’s passport cancellation ministerial submissions and found that ASIO has not yet amended its templates to make a distinction between advice provided by ASIO and advice provided by the Director-General. We will provide a further update on this issue in next year’s annual report.

Passport suspension, emergency visa cancellation and welfare payment cancellation

In 2014, Parliament passed laws enabling Australian and foreign passports to be suspended on security grounds for 14 days, and for the emergency cancellation of visas for 28 days. Passport suspension or emergency visa cancellation on security grounds is triggered by advice from ASIO, and enables action to be taken pending more detailed consideration by ASIO as to whether there are grounds to issue an adverse security assessment recommending passport or visa cancellation. The threshold for passport suspension and emergency visa cancellation is lower, and although judicial review is available, merits review by the AAT is not.

In June 2015 we conducted an inspection to review all cases where ASIO had requested passport suspension or emergency visa cancellation. No issues were identified. We intend to conduct a similar inspection during the next reporting period. We pay particularly close attention to any passport suspensions or emergency visa cancellations that do not proceed to a cancellation.

New legislation also enables welfare payments to be cancelled on security grounds if the person has their passport cancelled or visa refused or cancelled on security grounds. ASIO is one of a number of agencies that may have a role in considering whether welfare payments should be cancelled. We sought briefing from ASIO and inspected records from a sample of cases where welfare cancellation was or may have been under consideration. ASIO’s role is to provide advice in relation to the security considerations in such cases, and this includes considering whether the welfare payments are being used for activities prejudicial to security and whether cancellation could have an adverse security outcome, such as by further radicalising an individual.

We will continue to monitor ASIO’s role in providing advice in cases where welfare payment cancellation is under consideration.

Analytic Integrity

In March 2013 the IGIS reported on an inquiry into the analytic independence of ASIO, DIO and ONA. In March 2014, the IGIS initiated an inspection project to review the progress of ASIO in implementing the recommendations of that report. The 2013 Inquiry had recommended a number of improvements to ASIO’s analytical and organisational processes, including key judgment
reviews, formalised dissent handling procedures and improved record-keeping regarding analytical sources and external consultation. ASIO had indicated it accepted all recommendations and intended to implement new policies to address these issues.

In early 2014, ASIO invited the former Director-General of ONA, Mr Allan Gyngell AO, to conduct a comprehensive review into the state of analytic tradecraft and practices supporting the assessment function in ASIO. The inspection project was undertaken shortly after this review, and ASIO was in the process of developing and trialling new organisation-wide policies. The review project noted that there remained inconsistency in relation to ASIO analytic tradecraft, but the adoption of the organisation-wide policies was expected to lead to improvements. In June 2015 ASIO advised that the policies had been endorsed and were now being implemented across the Organisation.

**Warrants ‘whole of life’ project**

In April 2015 the 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 is raised is accurate and balanced. The results of this inspection activity will be included in next year’s annual report.

**ASIO internal approval process project**

Before ASIO commences an investigation, the proposed investigation must be authorised in accordance with the requirements of the Attorney-General’s Guidelines. We initiated an inspection project during the previous reporting period to review ASIO’s internal approvals for accessing sensitive information from government and non-government agencies. The review concluded that ASIO generally managed these investigative activities with due consideration of its legislative obligations, but a number of breaches of internal policies and procedures were identified, such as activities not being approved by an officer of the correct level or verbal approvals not being documented.

As a result of the project findings the Inspector-General recommended that ASIO consider an annual refresher training program, or other type of education program, for authorising officers to ensure they clearly understand their obligations under the legislation and ASIO’s internal policies and procedures. The review also identified cases with long periods of inactivity, and recommended that ASIO officers responsible for reviewing investigations should record the reasons for any lack of progress of investigative activities in the regular reviews. Under the Attorney-General’s Guidelines, investigations are required to be reviewed at least annually. ASIO indicated that it will remind staff of their obligations regarding compliance with internal policies and procedures.

**ASIO’s record retention and destruction project**

In November 2014 the IGIS initiated a project to investigate the data destruction practices of ASIO with a specific focus on material obtained under warrants. This project followed on from a similar project finalised in 2010, which made a number of recommendations aimed at improving ASIO’s corporate recordkeeping practices in the context of an expected increase in the volume of data held by ASIO (due to the volume of intelligence collected and the use of electronic documents and systems). The 2010 report specifically recommended that ASIO revisit its records management framework to ensure information and intelligence is appropriately retained or destroyed in accordance with requirements in the Archives Act 1983, ASIO Act and the TIA Act. Since 2010, ASIO has undertaken a major review of its records management framework, including the introduction of an updated National Archives of Australia (NAA)-ASIO Records Authority (RA) in 2012 and a new electronic system for managing investigative files during 2012–13.

An issue of particular interest to the IGIS in the follow-up project was the extent to which section 31 of the ASIO Act and section 14 of the TIA Act were being utilised. Those provisions require that, where a record or copy has been made of material
obtained under warrant, and is in the possession of ASIO; and where the Director-General is satisfied that the record or copy is not required for the purposes of performing ASIO’s functions, or exercising powers under those Acts ‘...the Director-General shall cause the record or copy to be destroyed’.

While the project was ongoing at the end of the reporting period, the IGIS has made a number of preliminary observations relating to ASIO’s electronic and paper-based file keeping practices:

- There was no evidence that warrant-related material had been destroyed in reliance on section 31 of the ASIO Act and section 14 of the TIA Act. ASIO advised that it considers material for disposal or retention in accordance with the NAA RA, rather than under those specific legislative provisions. However, while the Archives regime permits destruction in appropriate cases, it does not require it, and it also does not address the handling of copies of material residing in other databases.

- In the absence of a current register of electronic data repositories, ASIO policy needs to be updated to ensure data on other systems is appropriately managed. ASIO has agreed that the current policy (developed in 2011) will need to be updated as a result of the project’s findings.

- ASIO currently has a backlog of paper-based files waiting to be checked and, if appropriate, destroyed. ASIO has policies and processes in place for working through this backlog and retains records of what has been destroyed.

- ASIO has appropriate systems for identifying human or technological errors resulting in the collection of material outside the authority of a warrant, and is diligent in purging all such information from its systems.

- There was no evidence that ASIO has actually destroyed any electronic records that are eligible for destruction. ASIO advised that the electronic files created in the current version of their case management system have not yet reached the full term of the disposal category assigned. IGIS will continue to monitor whether electronic records that are eligible for destruction are appropriately destroyed.

- Any changes to ASIO systems and policies as a result of the project will be reported in the next annual report.

- The findings from this project will also be taken into account in the IGIS’s input to the review to be undertaken by ASIO and the Attorney-General’s Department of the Attorney-General’s Guidelines issued under section 8A of the ASIO Act. The Government has indicated that review will include 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.

Inspection of agencies subject to the Intelligence Services Act 2001

Limits on intelligence agencies’ functions

The functions of the Intelligence Services Act 2001 (the ISA) agencies are set out in sections 6, 6B and 7 of the ISA. For example, for ASIS the most relevant 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 wellbeing and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia.

Ministerial authorisations

Previously all activities undertaken by ASIS, ASD or AGO to produce intelligence on an Australian
Person required individual consideration and approval by the agency minister; changes to legislation made during the current reporting period introduced a number of exceptions. In summary these are:

- 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;
- Agency heads may given an authorisation in an emergency when ministers are not available.

Agencies’ use of these new powers is discussed later in this report.

Ministers are still 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 person’ 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 agency 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 the 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 outside of Australia is not an Australian person unless there is evidence to the contrary.

An agency may later overturn an initial presumption of nationality, 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 overturned but there would have been no breach of the privacy rules.
- 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 overturned and if intelligence information had already been communicated about the Australian person there could 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 information which was available at the time, there is no breach of the privacy rules.
Where a presumption of nationality is later found to be incorrect ASIS, ASD and AGO must advise us of this and the measures taken to protect the privacy of the Australian concerned.

Inspection of ASIS activities

During the reporting period ASIS implemented an agency-wide compliance training program. The program focuses on compliance with ASIS’s legislative and internal policy framework, drawing on case studies for scenario based learning. Training is compulsory for all ASIS officers, whether based in Australia or overseas. This training is regularly updated to incorporate lessons learnt from IGIS reviews and inquiries.

Ministerial authorisations to produce intelligence on Australian persons

There were three cases where IGIS undertook further investigation to establish if ASIS had taken action to produce intelligence on an Australian person without appropriate ministerial authorisations. In one of these cases ASIS conducted a review of the operation and agreed collection had taken place against two Australian persons without ministerial authorisation. Specific additional training was provided to staff in the area where the unauthorised collection occurred. In another case the review is ongoing, and in the third case no breach was found.

If an agency head is satisfied that the grounds on which a ministerial authorisation is given cease to have effect, the agency head is required by the ISA to inform the Minister. In October 2014 ASIS advised us of a breach of this obligation that had occurred when in October 2013 ASIS had been advised that the subject of a ministerial authorisation was not an Australian person, as had originally been presumed. ASIS did not promptly inform the Minister that the grounds on which the authorisation was issued had ceased to exist.

During 2014–15 there were three instances where ASIS sought a renewal of an existing ministerial authorisation and where the renewal was not signed within the eligible period for renewal. In each case it was signed the day after the authorisation ceased to have effect which meant that in practice there was no ‘gap’ in authorisation. Nevertheless, this is not ideal, and ASIS has undertaken to improve its processes for renewal to ensure it does not happen again.

During 2014–15, IGIS inspections identified inconsistencies in the way the commencement and expiry dates of authorisations were worded; the lack of consistency increases the risk of breaches. This has been drawn to ASIS’ attention.

Implementation of new legislative provisions relating to ministerial authorisations

Legislative changes introduced during this reporting period allow ASIS to produce intelligence on an Australian person, or a class of Australian persons, to support ASIO in the performance of its functions, without first obtaining authorisation from the Minister for Foreign Affairs. For this new power to be enlivened either ASIO needs to give ASIS a notice saying that it requires the production of intelligence on the Australian person or class of Australian persons or 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.

As at 30 June 2015, ASIO had provided a number of notices to ASIS stating that it requires the production of intelligence on Australian persons to support the performance of ASIO’s functions. This included three requests from ASIO in respect of a class of Australian persons. There were no instances where ASIS relied on an ASIS officer reasonably believing that it was not practicable in the circumstances for ASIO to notify ASIS before the intelligence about an Australian could be collected.

In June 2015 we conducted an inspection project in relation to the requests from ASIO; the inspection did not identify any issues of concern.
Changes to the ISA introduced in the reporting period also make provision for the Minister for Foreign Affairs to authorise the production of intelligence on, or have a direct effect on, one or more members of a class of Australian persons when providing assistance to the Australian Defence Force. No such authorisations were given during the reporting period.

New provisions were also inserted in the ISA to allow approval to be given to produce intelligence on an Australian in an emergency. ASIS did not use these emergency provisions during the reporting period.

We will continue to review the use of these new powers throughout 2015–16.

Privacy rules

OIGIS staff pay close attention to the distribution of intelligence about Australian persons by ASIS during regular inspection activities and the subject is also discussed with the IGIS at bi-monthly meetings.

ASIS reported one occasion in 2014–15 where the ‘presumption of nationality’ was overturned; that is, information came to light that an individual was actually an Australian person and the privacy rules were applied retrospectively to reporting. In this instance there was no breach of the rules as presumption was reasonable at the time it was made and the information suggesting the person was Australian was not available at that time.

Throughout 2014–15 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. Some of these occasions were identified by OIGIS staff during routine operational file inspections, others were reported by ASIS (see case study on page 34). ASIS has acknowledged that the errors were due to a combination of a lack of understanding of the correct procedures by staff, unclear policies and the effect of an ageing IT system.

The total number of cases where there were issues was a very small percentage of the overall amount of intelligence activity undertaken by ASIS.

Cooperation with foreign liaisons

In October 2014, ASIS advised that information had been communicated to a foreign liaison, without the application of the privacy rules and without approval under the ASIS internal policy. ASIS advised the communication of this information was also a breach of section 9 of the ISA, which requires ministerial authorisation to undertake an activity that will or is likely to have a direct effect on an Australian person. More information is provided on this incident on page 34.

In March 2015 ASIS provided a summary of seven occasions where intelligence information had been provided to foreign liaisons, without the application of the privacy rules and without approval under the ASIS internal policy. One of the cases was originally identified through an IGIS operational file inspection in February 2015 and the other cases were mostly self reported by ASIS staff following raised awareness of the issue as a result of ASIS compliance training.

At a subsequent operational file inspection in April 2015 OIGIS staff identified a number of additional cases where intelligence information had been provided to foreign liaisons, without the application of the privacy rules and without approval under the ASIS internal policy. One of those incidents had been reported by ASIS on the same day as the inspection.

ASIS advised that a lack of awareness by staff of the breadth of the definition of ‘intelligence information’ for the purpose of the privacy rules was a significant contributing factor.

In June 2015 ASIS advised IGIS that in April 2015 they had ‘cooperated’ with a foreign liaison service prior to obtaining ministerial approval to do so contrary to section 13(1)(c) of the ISA and internal ASIS policy. ASIS may only have limited interaction with a foreign liaison service prior to ministerial approval being obtained. An ASIS review of the incident was conducted in April 2015. The review resulted in a number of recommendations, including reinforcing ASIS policy on the legislative requirement for cooperation with foreign authorities.
Intelligence collected and provided to a foreign authority without approval

In October 2014 ASIS advised IGIS about a case where:

- intelligence information about an Australian person was provided to a foreign liaison without the application of the privacy rules as required by the ISA
- the communication was made without the relevant internal approval, which should have been obtained in accordance with internal ASIS policy
- the communication of the intelligence required prior ministerial authorisation because it was, or was likely have, a direct effect on an Australian person. That authorisation was not sought from the Minister.

The day after the incident, ASIS took steps to obtain the appropriate authorisation and the ministerial submission noted that ASIS had already undertaken activities in breach of the ISA and had not applied the privacy rules. The ministerial authorisation was granted the same day. ASIS also subsequently applied the privacy rules to the communication, and the Director-General retrospectively approved the release of the information to the foreign liaison. ASIS provided a full report of the incident to IGIS in February 2015.

This case highlighted the challenges ASIS faces in complying with legislative obligations and internal policies in time critical situations. In its report ASIS noted that recently passed National Security Legislation Amendment Act (No.1) 2014 and Counter-Terrorism Legislation Amendment Act (No. 1) 2014 introduced new arrangements for emergency authorisations.

Review of operational files

ASIS activities often 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 operational activities in a diverse range of countries where ASIS has a presence.

The sensitive nature of ASIS’s operational activities means specific detail about the nature of certain issues arising from these inspections cannot be disclosed in a public report. In addition to the ministerial authorisation issues outlined above, it was noted that internal approvals for operational activities were not always apparent on the relevant files. While in some cases there were explanations for why approvals were not documented, ASIS was reminded of the importance of official records containing a complete and accurate record of approvals. This issue is being addressed by ASIS.

Authorisations relating to the use of weapons

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

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

This reporting requirement was met during 2014–15 and the IGIS was satisfied that the need for limited numbers of ASIS staff to have access to weapons for self-defence in order to perform their duties is genuine.
During the 2014 Weapons Inquiry (see page 10) an occasion was identified where ASIS staff had participated in weapons familiarisation in controlled conditions under ADF supervision without the required prior approval by the Minister to fire the weapons concerned. It became apparent that ASIS staff did not realise this was a breach of the ISA, which suggested a deficiency in ASIS training for staff about the requirements around weapons. At our request, ASIS provided a report of all the other occasions where a similar breach of the ISA had occurred. A very significant number of ASIS officers had fired weapons they were not authorised for, either once or on several occasions in these circumstances, indicating a widespread lack of understanding about the legal requirements. However, in all cases the weapons were fired in a controlled environment under qualified ADF supervision. Changes made to the ISA during the reporting period mean that in future such activities will not constitute a breach of the ISA.

We conducted two inspections of ASIS weapons and self-defence training records in 2014–15, in November 2014 and May 2015. The inspections found that ASIS’s current governance and recordkeeping on this matter was effective, with no new breaches of the ISA or non-compliance with the ASIS internal weapons guidelines noted during the reporting period.

While reviewing files as a part of an IGIS Act investigation into a complaint, we identified a further breach of the ASIS weapons guidelines that had occurred a number of years earlier. In that case appropriate internal approval had not been obtained prior to the appointment of an external training provider being engaged. Although the training provider met the necessary competency standards to provide specialist training of the kind ASIS required, ASIS acknowledged that under the guidelines the provision of this training should not have occurred without this internal approval having first been obtained.

### Inspection of ASD activities

In addition to the major inquiry relating to ASD activities conducted during this reporting period, routine IGIS inspections of ASD activities for compliance with the ISA and internal policies and procedures continued. This inspection activity included IGIS staff directly accessing relevant classified databases and reviewing relevant hardcopy documentation. Inspections of ASD had a particular focus on the potential impact of ASD’s intelligence collection activities on the privacy of Australians. For a number of years ASD has had a substantial internal compliance area and IGIS has, in addition to our own inspections, taken account of advice from the ASD compliance area about the outcomes of their internal compliance processes and investigations.

### Ministerial authorisations

IGIS staff have access to each of ASD’s ministerial authorisations including the submissions to the Minister for Defence and the underlying information which supports the authorisation. In the reporting period we looked at a significant sample of these authorisations (approximately 75%). IGIS inspections in 2014–15 looked at the adequacy of record keeping, collection activities, internal compliance policy and reports given to the Minister at the end of an authorisation period.

Ministerial authorisations to produce intelligence on an Australian person last for a maximum of six months. Authorisations can only be granted in circumstances where the person is, or is likely to be, involved in one or more of the activities listed in section 9 of the ISA. A large percentage of the authorisations that were granted to ASD in 2014–15 were granted on the basis that the person was, or was likely to be, involved in activities that are, or are likely to be, a threat to security. These authorisations are not granted lightly and significant Commonwealth resources go into seeking the authorisations and collecting intelligence under them to meet high priority requirements. It is not uncommon for intelligence collection requirements to continue for more
than six months. In these cases the ministerial authorisation to produce intelligence on the Australian person needs to be renewed. During 2014–15 a number of ministerial authorisations which were identified for renewal lapsed for a period of time between expiring and being renewed. Because ASD and AGO do joint submissions in most cases both agencies were affected. Legally, intelligence collection activities had to be suspended until a new authorisation was put in place. Administration for the authorisations is managed by ASD. In most cases, it appears the issue was caused by the delayed receipt of information required from another agency and finalising the submission for the minister. The scale of this issue became apparent late in the reporting period. We will continue to review the administrative processes and procedures in place to support ministerial authorisations in the next reporting period.

ASD identified and reported to IGIS on a breach of the ISA that occurred when ASD undertook activity for the purpose of collecting intelligence on an Australian person without the required ministerial authority. ASD’s internal compliance area undertook an investigation into this incident. Key points were that:

- ASD had a ministerial authorisation to allow it to collect intelligence on the Australian person. That authorisation expired in mid-July 2014
- ASD did not cease activities in relation to the individual until nine days later
- No information was collected or reported during the nine day period
- At the time manual intervention was required to cease the relevant collection, this has now been linked to an automated system reducing the risk of reoccurrence
- OIGIS was initially informed of this incident within two days (July 2014) and received the internal investigation report seven weeks later (September 2014).

The ISA requires agencies to report to their minister on the activities that they have conducted under a ministerial authorisation within three months of that authorisation ceasing to have effect. During the reporting period ASD advised that on four occasions they had failed to report within the specified period. Two of these incidents occurred in April 2015 and the internal investigation report had not yet been received from ASD at the time this report was compiled. The remaining two incidents occurred late in the previous reporting period (June 2014) and the internal investigation report into both incidents was received shortly after the end of the current reporting period (July 2014). In the latter instance, ASD identified the need for a report to the Minister to be produced but that no action was taken to prepare such a report within the required timeframe.

In late 2014 the circumstances relevant to an activity conducted under a ministerial authorisation changed in a material way without ASD becoming aware of that change until after its occurrence. Once alerted to these changed circumstances (which were beyond the control of ASD), immediate and appropriate steps were taken to cease the activity. The IGIS was satisfied with the internal investigation of this matter and the remedial actions proposed and taken, including the ongoing technical development of equipment to improve compliance should similar circumstances arise in the future.

During the reporting period a ministerial authorisation was given to ASD in relation to support to a specified activity conducted by the Australian Defence Force. An extended period of time elapsed between the cessation of the Australian Defence Force activity this MA supported and ASD actions to cancel the MA and provide a report to the minister. ASD advised that this was due to uncertainty as to whether further assistance may be required.

**Emergency ministerial authorisations**

In the first half of the reporting period a situation arose where ASD were advised of a significant emergent threat out of hours and an oral ministerial authorisation for ASD to collect intelligence in relation to an identified Australian person was given. At the time this decision was made, the ISA allowed for the Attorney-General to provide verbal agreement in relation to a threat to

---

36 Annual Report 2014–15
security and allowed for certain other ministers to give a ministerial authorisation in writing where the minister responsible for the agency was not reasonably contactable or available. However, the ISA did not at that time provide for the ministerial authorisation itself to be given orally. In this instance the decision was followed up by a written authorisation in the standard format within twenty four hours. Legislative amendments have now been made to address the practical issues that this situation highlighted, allowing for emergency ministerial authorisations to be given orally by ministers and, in extremely limited circumstances, by agency heads.

A small number of emergency ministerial authorisations have been given to ASD since the legislation was enacted. On each occasion the IGIS was notified promptly and the formal reporting requirements set out in the ISA were complied with. The IGIS was satisfied with the records produced in relation to each event. In two cases an issue was identified with the way that the subject of the authorisation was described but it was clear the minister intended to authorise the proposed operation.

The new provision allowing an agency head to give an authorisation in an emergency when the minister is not available were not used by ASD during the reporting period.

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

At the end of the reporting period there were a small number of internal ASD compliance investigations still ongoing, including two possible breaches of the TIA Act. We continue to monitor these matters.

**Protecting the privacy of Australians**

In accordance with their obligations, ASD continued to report to IGIS on cases where a presumption of nationality had later been found to be incorrect, and the measures taken to protect the privacy of the Australian person involved.

Two instances have been identified where ASD incorrectly applied the presumption of nationality resulting in a breach of the privacy rules. In both cases information indicating that the individuals were Australian was available within ASD at the time nationality was assessed but this information was not sufficiently communicated and considered. No intelligence collection activities occurred against Australian persons under the incorrect presumption of nationality. In one case internal ASD processes and procedures were sufficient to identify and rectify the issue in less than thirty six hours. The other case was identified and remediated in nine days.

ASD undertook an internal review of how these cases occurred and has proposed follow on actions including the revision of internal policy.

ASD also reported to IGIS on a number of occasions where a presumption of nationality had been made, and was reasonable at the time it was made, but was later overturned by new information. These cases were managed consistently with the privacy rules. The ASD processes in place for reporting to IGIS and informing other intelligence agencies when a presumption of nationality is overturned are sound.

**Inspection of AGO activities**

**Inspection and review activities**

During 2014–15 we conducted three inspection visits to AGO headquarters, as well as reviewing records of some of its intelligence collection activities on-line and discussing relevant matters with the Director of AGO and relevant officers. In the course of these activities, this office paid particular attention to AGO’s compliance with the terms of each ministerial authorisation which was issued to the agency by the Minister for Defence, noted the time taken to cancel collection activities when the grounds on which a ministerial authorisation had materially changed, and reviewed the accuracy of reports provided to the Minister for Defence following the expiry or cancellation of a ministerial authorisation.
The Director of AGO is required to personally authorise any intelligence collection activity undertaken by AGO in relation to Australian territory. These approvals are reported to the minister on a quarterly basis. OIGIS staff reviewed approximately 70% of the approvals given by the Director of AGO and subsequent post activity reports in 2014–2015, no issues of concern were identified.

OIGIS staff also examined the adequacy of checks undertaken by AGO to determine the nationality of individuals or entities before targeted collection activities took place (to establish whether or not a ministerial authorisation needed to be obtained), and the extent of cooperation between AGO and other intelligence collection agencies when seeking to obtain intelligence information about the same target, or lodge a submission to obtain a joint ministerial authorisation. The only significant issue was that on a number of occasions joint ASD-AGO submissions to the minister to renew authorisations do not appear to have been processed in time; as discussed above ASD is the lead agency for administration of these arrangements.

AGO advised this office of one occasion where the information provided to their Minister about activities conducted in reliance on a ministerial authorisation was incomplete. We are satisfied with the steps that AGO subsequently took to correct the information provided and to inform this office of the issue. We have reviewed the remedial actions taken by AGO and consider them to be satisfactory.

Based on these inspection and review activities, the IGIS was satisfied that AGO takes its statutory obligations under the ISA seriously and has put in place robust systems to encourage compliance with its obligations. AGO has effective mechanisms for identifying legal issues and ensuring that legal advice is appropriately recorded and potential issues brought to the attention of the Director of AGO.

Monitoring DIO and ONA

As has been the practice of this office over many years, we continued to exercise a light touch inspection regime with respect to the activities of ONA and DIO. As these agencies do not directly collect covert intelligence, their activities are far less likely than those of the collection agencies to intrude upon the personal affairs of Australian persons.

We aim to review the compliance of ONA and DIO with their respective privacy guidelines at least twice a year, via privacy guidelines inspections. In 2014–15 we undertook three such inspections of DIO, and two of ONA.

These inspections revealed that ONA and DIO are generally compliant with the requirements of their privacy guidelines and that they each take their privacy responsibilities seriously. To the extent that non-compliance issues were identified these tended to be administrative in nature and there was no evidence that intelligence was passed in breach of the guidelines.

Cross-agency inspections

Light cover

Light cover is used by ASIO and ASIS staff to conceal their employment. Where more robust cover is required the agencies are able to use the assumed identities scheme (see below). In 2014, the IGIS conducted an inspection project on the agencies’ use of light cover, focusing on advice, training and support provided to staff. The project identified four key areas of potential concern for staff using light cover: risk of penalties for impersonating a Commonwealth Officer when using alternative government departments as light cover; court appearances; dealing with police; and obtaining private insurance policies. Both agencies were aware of the issues, but the communication to staff in the form of policy, intranet advice and training varied. Since the completion of this project, ASIO has finalised a light cover policy. ASIO and ASIS have also sought to identify suitable life insurance options for their staff.
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 a circumstance 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 a requirement for ASIO and ASIS to conduct six monthly audits of assumed identity records and 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 the IGIS with reports covering the activities of their respective agencies for the 2013–14 reporting period. There was nothing in the reports that caused concern.

ASIS provided the IGIS with a copy of their internal audit reporting on assumed identities during this reporting period in addition to the annual report. This was in response to our request for this information following an inspection of ASIS assumed identity records conducted during the previous reporting period. There was nothing in the reports that caused concern.

Access to sensitive financial information by intelligence agencies

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

The IGIS is party to a memorandum of understanding (MOU) with AUSTRAC. This MOU establishes an agreed understanding of IGIS's role in monitoring 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 focused, and information passed to both Australian agencies and foreign intelligence counterparts is correctly authorised.

During 2014–15, in accordance with the MOU, the IGIS sent an annual statement to the Attorney-General and the Minister for Foreign Affairs on the outcome of compliance monitoring activities in ASIO and ASIS respectively, concerning their access to, and use of, AUSTRAC information in the previous reporting period. AUSTRAC provided insufficient information for compliance monitoring activities to be carried out in relation to AGO, ASD, DIO and ONA concerning their access to, and use of AUSTRAC information in the 2013–2014 reporting period. This issue has been raised with AUSTRAC and the flow of information for this reporting period has improved and will be reported on in the 2015–2016 annual report.

ASIO

We conducted regular inspections of ASIO's access to AUSTRAC material. An ongoing issue that has been raised in our inspections is an inconsistency between two of ASIO's internal policies relating to setting limitations for searches of AUSTRAC databases. As at the end of the reporting period this issue was yet to be resolved, though ASIO have advised that there are changes to AUSTRAC databases and policies to be implemented in the next reporting period.

During our inspections two cases were identified where requests for AUSTRAC data were not authorised prior to the search being conducted. Another request was not authorised by an ASIO officer at the correct level as required by ASIO policies.

Our inspections also revealed one search of AUSTRAC database was conducted on a partial
number and returned a large number of records unconnected to the subject of the AUSTRAC request. ASIO advised that these records were not viewed by ASIO staff.

**ASIS**

Inspections throughout 2014–15 did not identify any significant concerns relating to the receipt of AUSTRAC material. This is a significant improvement on previous years. ASIS has recently re-established direct access to AUSTRAC databases and information and our inspection activities are being expanded to cover this development.

Also during the reporting period ASIS advised that the AUSTRAC CEO had provided ASIS with an exemption from s.53, 55 and 59 of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 dated 16 April 2015. Essentially, this exempts ASIS from reporting movements of physical currency and bearer negotiable instruments into or out of Australia, when carrying out a statutory function under section 6 of the Intelligence Services Act 2001. This was in response to issues identified by the IGIS, as noted in our previous annual report.

**Summary of IGIS financial performance and resources for outcomes (PGPA Act)**

IGIS received an unqualified audit report from the Australian National Audit Office for its 2014–15 financial statements. A summary of the office’s financial performance can be found on the following page.

The office operated within available resources in 2014–15 and ended the year with a surplus of $585 131.

During 2014–15 the office received significant additional appropriation funding ($840 000) to provide additional resources to enable the office to maintain effective oversight of the activities of the intelligence agencies.

In relation to expenditure, the most significant budget variance related to employee expenses ($480 557 underspend). This occurred because the office received additional funding for new staff part way through the reporting period and although recruitment action commenced promptly there was an inevitable delay in recruiting. Other variances included expenses linked to the additional funding including international travel ($24 000 underspend) and consultants ($30 000 underspend). Variances in ongoing items included security clearances for ongoing staff members ($5 000 underspend) and potential software licence fees ($13 000 underspend).

Net equity increased from $1 653 529 in 2013–14 to $2 253 786 in 2014–15. Movements in equity included a $585 131 increase in retained surplus. Contributed Equity also increased from $463 000 in 2013–14 to $478 126 in 2014–15. Movements in Contributed Equity included capital funding of $26 000 offset by a reduction of $10 874 following the lapsing of unspent 2010–11 and 2011–12 departmental capital budgets.

The following tables can be found in Annex 3.

Table 3.1 - Agency Resource Statement and Resource for Outcomes 2014–15, and

Table 3.2 Expenses and Resources for Outcome 1.

IGIS has one outcome and one program.

**Trends in finances**

Significant changes to the finances of the office during 2014–15 included:

- An $824 000 increase in revenue from government. This consisted of $840 000 additional funding received to enhance the agency’s ability to oversight the activities of the intelligence agencies in the context of those agencies receiving significant new powers and additional funding. This increase was offset by a $16 000 reduction in base funding compared to the previous year.
A $144,525 decrease in own-source revenue primarily due to the significant inquiry funding received in the previous year ($139,000).

A $272,384 increase in employee expenses largely due to additional staff being recruited with the additional funding.

A $52,249 increase in supplier expenses. Increases in expenditure included $14,000 in staff training expenses, $11,000 increase in translation expenses and $5,000 increase in transcription services.

A $49,905 increase in other payables due to outstanding reimbursements to home agencies for seconded staff.

<table>
<thead>
<tr>
<th></th>
<th>2014–15 OUTCOME 1 $</th>
<th>2013–14 OUTCOME 1 $</th>
<th>Change from previous year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue from Government</td>
<td>3,003,000</td>
<td>2,179,000</td>
<td>+38%</td>
</tr>
<tr>
<td>Other Income</td>
<td>130,023</td>
<td>274,548</td>
<td>-53%</td>
</tr>
<tr>
<td><strong>TOTAL INCOME</strong></td>
<td>3,133,023</td>
<td>2,453,548</td>
<td></td>
</tr>
<tr>
<td>Employee expenses</td>
<td>2,188,443</td>
<td>1,916,059</td>
<td>+14%</td>
</tr>
<tr>
<td>Supplier expenses</td>
<td>322,932</td>
<td>270,683</td>
<td>+19%</td>
</tr>
<tr>
<td>Other expenses</td>
<td>36,517</td>
<td>40,473</td>
<td>-10%</td>
</tr>
<tr>
<td><strong>TOTAL EXPENSES</strong></td>
<td>2,547,892</td>
<td>2,227,215</td>
<td></td>
</tr>
<tr>
<td><strong>OPERATING RESULT</strong></td>
<td>585,131</td>
<td>226,333</td>
<td></td>
</tr>
<tr>
<td>Financial assets</td>
<td>A 3,240,736</td>
<td>2,437,208</td>
<td>+33%</td>
</tr>
<tr>
<td>Non-financial assets</td>
<td>B 27,218</td>
<td>63,735</td>
<td>-57%</td>
</tr>
<tr>
<td>Liabilities</td>
<td>C 1,014,168</td>
<td>847,414</td>
<td>+19%</td>
</tr>
<tr>
<td><strong>NET ASSETS = A + B - C</strong></td>
<td>2,253,786</td>
<td>1,653,529</td>
<td></td>
</tr>
</tbody>
</table>
Part Three

Management and Accountability

Corporate Governance

Organisational structure
Senior positions occupied during 2014–15 were as follows:

Inspector-General of Intelligence and Security (Statutory officer)
   Dr Vivienne Thom
Assistant Inspector-General of Intelligence and Security (SES Band 1)
   Mr Jake Blight

Senior management committees
The OIGIS Audit Committee is the only senior management committee for the agency. The functions of this committee are detailed in the ‘Internal Audit and Risk Management’ section of this chapter.

Corporate and operational planning
OIGIS’s corporate and operational planning processes are straightforward in nature, reflecting the small size and specialist function of the office.

The office addresses these matters through:

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

Protective security
The Australian Government’s Protective Security Policy Framework provides a structure for Australian government agencies to proportionately and effectively manage security risks 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 requirements that the IGIS office is required to comply with.

As at 30 June 2015, we were fully compliant with 34 of the 36 mandatory requirements and partially compliant with two. A risk mitigation strategy is in place for the partially compliant requirements.
Ethical standards and fraud control

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

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

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

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

Employment of persons for a particular inquiry

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

Reports by the Auditor-General, Parliamentary Committees, the Commonwealth Ombudsman or an agency capability review

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

The office has received an unqualified audit report from the Australian National Audit Office (ANAO) in relation to its financial statements.

Further details of OIGIS interaction with parliamentary committees are available in the Overview section of this report.

Decisions by the judiciary, tribunals or the Information Commissioner

No judicial decisions or decisions of administrative tribunals or of the Information Commissioner made in 2014–15 had, or may have, a significant impact on the operations of the office.
Management of Human Resources

Organisational profile

At 30 June 2015, the office had 14 ongoing and 1 non-ongoing APS employees located in the Australian Capital Territory (not including the Inspector-General). Five employees worked part-time. This compares to 12 ongoing APS employees located in the Australian Capital Territory at 30 June 2014.

No employees identified as Indigenous.

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

Organisational Profile as at 30 June 2015 (employment level and status)

Gender Balance as at 30 June 2015 (by employment level)

Internal audit and risk management

The membership and functions of the Audit Committee are structured according to the PGPA Act. At 30 June 2015 the members were Mr Matthew King (Treasury) as Chair, Mr Trevor Kennedy (Attorney-General’s Department) and Mr Jake Blight (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.

Employment frameworks

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

The salary range available to APS employees in OIGIS throughout 2014–15 is provided at Annex 2.

The only notable non-salary benefit for OIGIS non-SES staff is a taxable annual allowance in recognition of the requirement to undergo regular and intrusive security clearance processes necessary to maintain a 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 2015.

Training and staff development

We continued the internal training program introduced in early 2012. The program of short training sessions, run once a fortnight, ensures that staff develop and maintain specialised knowledge and skills, and supplements on the job training. Topics covered in 2014–15 included:

- Recent changes to legislation
- Parliamentary Committees
- Independent Reviewer of Adverse Security Assessments
- Issue Motivated Groups
- Law of Armed Conflict

One staff member completed a Certificate IV in Government (Investigations) in 2014–15. We also obtained the services of an external trainer to provide a tailored Certificate IV in Government (Investigations) for this office. 11 staff are currently enrolled to complete the Certificate.

Staff were also provided with regular opportunities throughout 2014–15 to attend other training courses and seminars relevant to their roles. A studies assistance scheme is available to reimburse employees for approved courses of study.

Performance pay

OIGIS does not have a performance based pay scheme.

Other information

Purchasing


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

Consultants

Total actual expenditure on consultancy contracts for 2014–15 was $18,813 (GST inclusive). This represents one consultancy contract for legal services. This compares to consultancy expenditure of $15,993 (GST inclusive) in 2013–14.

ANAO access clauses

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

Exempt contracts

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

Information publication scheme

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

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

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

Due to the small size of the office, PM&C does not separately measure the utilities used by OIGIS and provides these utilities free of charge. For this reason, ecologically sustainable development and details of environmental performance are not specifically quantified in this report.

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

- recycled paper was used for around 98 per cent of the office’s photocopying, facsimile reports and document printing in 2014–15
- staff configure printers to default to double-sided print
- all unclassified office paper and cardboard waste is recycled
- empty toner cartridges are recycled, except where security considerations apply

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

The Commonwealth Disability Strategy has been overtaken by the National Disability Strategy 2010-2020, which sets out a ten year national policy framework to improve the lives of people with disability, promote participation and create a more inclusive society. A high level two-yearly report will track progress against each of the six outcome areas of the Strategy and present a picture of how people with disability are faring. The first of these reports will be available in late 2014, and can be found at www.dss.gov.au.

Work health and safety
Due to its small size, the office does not have a Health and Safety Committee. Instead, health and safety matters are addressed at all-staff meetings, Audit Committee meetings, and, as the need arises, directly with me through team leaders and the 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.
Part Four

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 2015, which comprise:

- 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;
- Schedule of Commitments; and
- Notes to and forming part of the Financial Statements, including a Summary of Significant Accounting Policies and other explanatory information.

Inspector-General of Intelligence and Security’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. The Inspector-General of Intelligence and Security is also responsible for such internal control as 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 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 Inspector-General of Intelligence and Security, 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.

**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 2015 and its financial performance and cash flows for the year then ended.

Australian National Audit Office

Rebecca Reilly  
Executive Director

Delegate of the Auditor-General

Canberra  
29 September 2015
STATEMENT BY THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2015 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.

Hon Margaret Stone
Inspector-General of Intelligence and Security

29 September 2015
OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY
STATEMENT OF COMPREHENSIVE INCOME
for the year ended 30 June 2015

### NET COST OF SERVICES

<table>
<thead>
<tr>
<th>Expenses</th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee benefits</td>
<td>4A</td>
<td>2 188 443</td>
</tr>
<tr>
<td>Supplier</td>
<td>4B</td>
<td>322 932</td>
</tr>
<tr>
<td>Depreciation and amortisation</td>
<td></td>
<td>36 481</td>
</tr>
<tr>
<td>Loss on asset disposal</td>
<td></td>
<td>36</td>
</tr>
<tr>
<td><strong>Total Expenses</strong></td>
<td></td>
<td><strong>2 547 892</strong></td>
</tr>
</tbody>
</table>

### Own-Source Income

<table>
<thead>
<tr>
<th>Own-source revenue</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Other revenue</td>
<td>5A</td>
<td>28 023</td>
</tr>
<tr>
<td><strong>Total own-source revenue</strong></td>
<td></td>
<td><strong>28 023</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Gains</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Other gains</td>
<td>5B</td>
<td>102 000</td>
</tr>
<tr>
<td><strong>Total gains</strong></td>
<td></td>
<td><strong>102 000</strong></td>
</tr>
<tr>
<td><strong>Total own-source income</strong></td>
<td></td>
<td><strong>130 023</strong></td>
</tr>
<tr>
<td><strong>Net Cost of services</strong></td>
<td></td>
<td><strong>2 417 869</strong></td>
</tr>
</tbody>
</table>

| Revenue from Government          | 5C    | 3 003 000 | 2 179 000 |
| **Surplus attributable to the Australian Government** | 585 131 | 226 333 |

### OTHER COMPREHENSIVE INCOME

**Items not subject to subsequent reclassification to net cost of services**

| Changes in asset revaluation surplus |       | -    | 9 308 |
| **Total comprehensive income attributable to the Australian Government** | 585 131 | 235 641 |

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 2015

<table>
<thead>
<tr>
<th>Notes</th>
<th>2015 $</th>
<th>2014 $</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ASSETS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Assets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash and cash equivalents</td>
<td>174 814</td>
<td>207 005</td>
</tr>
<tr>
<td>Trade and other receivables</td>
<td>3 065 922</td>
<td>2 230 203</td>
</tr>
<tr>
<td>Total financial assets</td>
<td>3 240 736</td>
<td>2 437 208</td>
</tr>
<tr>
<td>Non-Financial Assets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Property, plant and equipment</td>
<td>27 218</td>
<td>63 735</td>
</tr>
<tr>
<td>Total non-financial assets</td>
<td>27 218</td>
<td>63 735</td>
</tr>
<tr>
<td>Total Assets</td>
<td>3 267 954</td>
<td>2 500 943</td>
</tr>
<tr>
<td><strong>LIABILITIES</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payables</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suppliers</td>
<td>20 690</td>
<td>38 800</td>
</tr>
<tr>
<td>Other payables</td>
<td>128 131</td>
<td>78 226</td>
</tr>
<tr>
<td>Total payables</td>
<td>148 821</td>
<td>117 026</td>
</tr>
<tr>
<td>Provisions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee provisions</td>
<td>865 347</td>
<td>730 388</td>
</tr>
<tr>
<td>Total provisions</td>
<td>865 347</td>
<td>730 388</td>
</tr>
<tr>
<td>Total Liabilities</td>
<td>1 014 168</td>
<td>847 414</td>
</tr>
<tr>
<td>Net Assets</td>
<td>2 253 786</td>
<td>1 653 529</td>
</tr>
<tr>
<td><strong>EQUITY</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contributed equity</td>
<td>478 126</td>
<td>463 000</td>
</tr>
<tr>
<td>Reserves</td>
<td>16 105</td>
<td>16 105</td>
</tr>
<tr>
<td>Retained surplus</td>
<td>1 759 555</td>
<td>1 174 424</td>
</tr>
<tr>
<td>Total Equity</td>
<td>2 253 786</td>
<td>1 653 529</td>
</tr>
</tbody>
</table>

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 year ended 30 June 2015

<table>
<thead>
<tr>
<th></th>
<th>Retained Earnings</th>
<th>Asset Revaluation Surplus</th>
<th>Contributed Equity/Capital</th>
<th>Total Equity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2015 $</td>
<td>2014 $</td>
<td>2015 $</td>
<td>2014 $</td>
</tr>
<tr>
<td>Opening balance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Balance carried forward from previous period</td>
<td>1 174 424</td>
<td>948 091</td>
<td>16 105</td>
<td>6 796</td>
</tr>
<tr>
<td>Adjusted opening balance</td>
<td>1 174 424</td>
<td>948 091</td>
<td>16 105</td>
<td>6 796</td>
</tr>
<tr>
<td>Comprehensive Income</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other comprehensive income</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>9 309</td>
</tr>
<tr>
<td>Surplus for the period</td>
<td>585 131</td>
<td>226 333</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Total comprehensive income</td>
<td>585 131</td>
<td>226 333</td>
<td>-</td>
<td>9 309</td>
</tr>
<tr>
<td>Transactions with owners</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contribution by Owners</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equity Injection – Appropriation – repealed</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Appropriations repealed</td>
<td>(10 874)</td>
<td></td>
<td>(10 874)</td>
<td></td>
</tr>
<tr>
<td>Departmental Capital Budget</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>26 000</td>
</tr>
<tr>
<td>Total transactions with owners</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>15 126</td>
</tr>
<tr>
<td>Closing balance as at 30 June attributable to the Australian Government</td>
<td>1 759 555</td>
<td>1 174 424</td>
<td>16 105</td>
<td>16 105</td>
</tr>
</tbody>
</table>

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

CASH FLOW STATEMENT
for the year ended 30 June 2015

Notes

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
</tr>
</tbody>
</table>

**OPERATING ACTIVITIES**

**Cash received**
- Appropriations: 2,371,063
- Net GST received: 8,598
- Other cash received: 116,499

**Total cash received**: 2,496,160

**Cash used**
- Employees: (2,092,294)
- Suppliers: (31,402)
- Section 74 receipts transferred to OPA: (116,499)

**Total cash used**: (2,522,816)

**Net cash from (used by) operating activities**: 11 (26,656) (2,312)

**INVESTING ACTIVITIES**

**Cash used**
- Purchase of property, plant and equipment: (5,535)

**Total cash used**: (5,535)

**Net cash from (used by) investing activities**: (5,535) (2,723)

**FINANCING ACTIVITIES**

**Cash received**
- Contributed equity: 8,257

**Total cash received**: 8,257

**Net cash from financing activities**: 8,257

**Net increase/(decrease) in cash held**
- (32,191) 3,222

**Cash and cash equivalents at the beginning of the reporting period**: 207,005 203,783

**Cash and cash equivalents at the end of the reporting period**: 11 174,814 207,005

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

1 In 2013-14 relates to FMA Act Section 31.
## SCHEDULE OF COMMITMENTS

*as at 30 June 2015*

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td><strong>BY TYPE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commitments Receivable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net GST receivable on commitments</td>
<td>24,816</td>
<td>25,654</td>
</tr>
<tr>
<td>Total Commitments Receivable</td>
<td>24,816</td>
<td>25,654</td>
</tr>
<tr>
<td>Commitments Payable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Commitments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>272,971</td>
<td>272,971</td>
</tr>
<tr>
<td>Operating Leases</td>
<td>34,520</td>
<td>9,216</td>
</tr>
<tr>
<td>Total Other Commitments Payable</td>
<td>307,491</td>
<td>282,187</td>
</tr>
<tr>
<td>Net Commitments by Type</td>
<td>282,675</td>
<td>256,533</td>
</tr>
<tr>
<td><strong>BY MATURITY</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commitments Receivable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Within 1 year</td>
<td>4,963</td>
<td>5,634</td>
</tr>
<tr>
<td>Between 1 to 5 years</td>
<td>19,853</td>
<td>20,020</td>
</tr>
<tr>
<td>More than 5 years</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Total Commitments Receivable</td>
<td>24,816</td>
<td>25,654</td>
</tr>
<tr>
<td>Commitments Payable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Lease Commitments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Within 1 year</td>
<td>10,396</td>
<td>7,373</td>
</tr>
<tr>
<td>Between 1 to 5 years</td>
<td>24,124</td>
<td>1,843</td>
</tr>
<tr>
<td>More than 5 years</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Total Operating Lease Commitments Payable</td>
<td>34,520</td>
<td>9,216</td>
</tr>
<tr>
<td>Other Commitments Payable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Within 1 year</td>
<td>54,594</td>
<td>54,594</td>
</tr>
<tr>
<td>Between 1 to 5 years</td>
<td>218,377</td>
<td>218,377</td>
</tr>
<tr>
<td>More than 5 years</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Total Other Commitments Payable</td>
<td>272,971</td>
<td>272,971</td>
</tr>
<tr>
<td>Total Commitments Payable</td>
<td>307,491</td>
<td>282,187</td>
</tr>
<tr>
<td>Net Commitments by Maturity</td>
<td>282,675</td>
<td>256,533</td>
</tr>
</tbody>
</table>

Note: Commitments are GST inclusive where relevant.

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

OIGIS holds agreements with PM&C requiring an annual payment of $50,600 for IT support services and $3,994 for payroll services. These agreements are in place for 2015-16 and the following four years.

OIGIS in its capacity as a lessee holds one motor vehicle operating lease.
NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2015

Note 1 – Summary of Significant Accounting Policies

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:

• Financial Reporting Rule (FRR) for reporting periods ending on or after 1 July 2014; 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.

Unless an alternative treatment is specifically required by an accounting standard or the FRR, assets and liabilities are recognised in the statement of financial position when and only when it is probable that future economic benefits will flow to the entity or a future sacrifice of economic benefits will be required and the amounts of the assets or liabilities can be reliably measured. However, assets and liabilities arising under executory contracts are not recognised unless required by an accounting standard. Liabilities and assets that are unrecognised are reported in the schedule of commitments.

Unless alternative treatment is specifically required by an accounting standard, income and expenses are recognised in the Statement of Comprehensive Income when and only when the flow, consumption or loss of economic benefits has occurred and can be reliably measured.

1.3 Significant Accounting Judgments and Estimates

In the process of applying the accounting policies listed in this note, OIGIS has made the following judgments that have the most 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.
NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2015

1.4 New Australian Accounting Standards

Adoption of New Australian Accounting Standard Requirements

OIGIS has elected to apply AASB 2015-7 Amendments to Australian Accounting Standards – Fair Value Disclosures of Not-for-Profit Public Sector Entities for this financial year, even though the Standard is not required to be applied until annual reporting periods beginning on or after 1 July 2016. AASB 2015-7 provides relief from disclosing quantitative information about significant unobservable inputs used in fair value, where property, plant and equipment is held for its current service potential rather than to generate future net cash inflows.

The following new standard was issued prior to the sign-off date and is applicable to the current reporting period:

- AASB 1055 Budgetary Reporting applied from 1 July 2014 and resulted in significant disclosure requirement changes.

Future Australian Accounting Standard Requirements

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

1.5 Revenue

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.

Other Types of Revenue

Revenue from the sale of goods is recognised when:

- the risks and rewards of ownership have been transferred to the buyer;
- the agency retains no managerial involvement or effective control over the goods;
- the revenue and transaction costs incurred can be reliably measured; and
- it is probable that the economic benefits associated with the transaction will flow to the entity.

Revenue from rendering of services is recognised by reference to the stage of completion of contracts at the reporting date. The revenue is recognised when:

- the amount of revenue, stage of completion and transaction costs incurred can be reliably measured; and
- the probable economic benefits associated with the transaction will flow to the entity.

The stage of completion of contracts at the reporting date is determined by reference to the proportion that costs incurred to date bear to the estimated total costs of the transaction.

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.
NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2015

1.6 Gains

Resources Received Free of Charge

Resources received free of charge are recognised as gains 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.

The main resources received free of charge in 2014-15 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 Defence 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.

Sale of Assets

Gains from disposal of assets are recognised when control of the asset has passed to the buyer.

1.7 Transactions with the Government as Owner

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.

1.8 Employee Benefits

Liabilities for ‘short-term employee benefits’ (as defined in AASB 119 Employee Benefits) and termination
benefits expected within twelve months of the end of the reporting period are measured at their nominal amounts.

The nominal amount is calculated with regard to the rates expected to be paid on settlement of the liability.

Other long-term employee benefits are measured as net total of the present value of the defined benefit obligation
at the end of the reporting period minus the fair value at the end of the reporting period of plan assets (if any) out
of which the obligations are to be settled directly.

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 outside the Commonwealth.

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.

The liability for superannuation recognised as at 30 June represents outstanding contributions for the final fortnight of the year.

1.9 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.

1.10 Financial Assets

OIGIS classifies its financial assets as ‘loans and receivables’.

Financial assets are recognised and derecognised upon trade date.

Effective Interest Method

The effective interest method is a method of calculating the amortised cost of a financial asset and of allocating interest income over the relevant period. The effective interest rate is the rate that exactly discounts estimated future cash receipts through the expected life of the financial asset, or, where appropriate, a shorter period.

Loans and receivables

Trade receivables, loans and other receivables that have fixed or determinable payments that are not quoted in an active market are classified as ‘loans and receivables’. Loans and receivables are measured at amortised cost using the effective interest method less impairment. Interest is recognised by applying the effective interest rate.

Credit terms are net 30 days (2013–14: 30 days).

Impairment of financial assets

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

1.11 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 2015

Other Financial Liabilities

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.

1.12 Contingent Liabilities and Contingent Assets

Contingent liabilities and contingent assets are not recognised in the statement of financial position but are reported in the relevant schedules and 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 2013-14 or in 2014-15.

No contingent rentals exist.

1.13 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.

Assets acquired at no cost, or for nominal consideration, are initially recognised as assets and income at their fair value at the date of acquisition, unless acquired as a consequence of restructuring of administrative arrangements. In the latter case, assets are initially recognised as contributions by owners at the amounts at which they were recognised in the transferor agency’s accounts immediately prior to the restructuring.

1.14 Property, Plant and Equipment

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.

**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 (2014: 1 – 14 years).

**Impairment**

All assets were assessed for impairment at 30 June 2015. Where indicators of impairment were identified an assessment of recoverable value has been undertaken and the value of the assets adjusted accordingly.

**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.

**1.15 Intangibles**

Previously OIGIS’s intangibles have consisted of purchased software only. These assets were carried at cost less accumulated amortisation and accumulated impairment losses. Software is amortised on a straight-line basis over its anticipated useful life. Software is assigned a useful life of 4 years (2014: 4 years).

All software assets were fully amortised as at 30 June 2009.

**1.16 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.

**1.17 Legal Compliance**

The Australian Government continues to have regard to developments in case law, including the High Court’s most recent decision on Commonwealth expenditure in *Williams v Commonwealth* (2014) HCA 23, as they contribute to the larger body of law relevant to the development of Commonwealth programs. In accordance with its general practice, the Government will continue to monitor and assess risk and decide on any appropriate actions to respond to risks of expenditure not being consistent with constitutional or other legal requirements.

**Note 2 – 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.
Note 3 – Net Cash Appropriation Arrangements

<table>
<thead>
<tr>
<th>Description</th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Comprehensive Income (loss) less depreciation/amortisation expenses previously funded through revenue appropriations</td>
<td>$621,612</td>
<td>$273,640</td>
</tr>
<tr>
<td>Depreciation/amortisation expenses previously funded through revenue appropriation</td>
<td>($36,481)</td>
<td>($37,999)</td>
</tr>
<tr>
<td>Total comprehensive income (loss) as per the Statement of Comprehensive Income</td>
<td>$585,131</td>
<td>$235,641</td>
</tr>
</tbody>
</table>

1. From 2010-11, the Government introduced net cash appropriation arrangements, where revenue appropriations for depreciation/amortisation expenses ceased. Entities now receive a separate capital budget provided through equity appropriations. Capital budgets are to be appropriated in the period when cash payment for capital expenditure is required.
NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2015

Note 4 – Expenses

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td><strong>Expenses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Employee Benefits</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wages and salaries</td>
<td>1 644 289</td>
<td>1 495 856</td>
</tr>
<tr>
<td>Superannuation:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defined benefit plans</td>
<td>223 658</td>
<td>218 309</td>
</tr>
<tr>
<td>Defined contribution plans</td>
<td>97 823</td>
<td>53 396</td>
</tr>
<tr>
<td>Leave and other entitlements</td>
<td>222 673</td>
<td>148 498</td>
</tr>
<tr>
<td>Separation and Redundancies</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Total employee benefits</strong></td>
<td>2 188 443</td>
<td>1 916 059</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td><strong>Suppliers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Goods and services supplied or rendered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consultants</td>
<td>-</td>
<td>800</td>
</tr>
<tr>
<td>ICT support</td>
<td>46 000</td>
<td>46 000</td>
</tr>
<tr>
<td>Legal expenses</td>
<td>17 104</td>
<td>13 739</td>
</tr>
<tr>
<td>Printing non publications</td>
<td>8 868</td>
<td>7 837</td>
</tr>
<tr>
<td>Resources received free of charge:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notional Rent Charge</td>
<td>102 000</td>
<td>102 000</td>
</tr>
<tr>
<td>Notional Audit Fees</td>
<td>18 000</td>
<td>18 000</td>
</tr>
<tr>
<td>Notional IT Support Costs</td>
<td>4 545</td>
<td>4 545</td>
</tr>
<tr>
<td>Stationery</td>
<td>9 758</td>
<td>5 452</td>
</tr>
<tr>
<td>Training</td>
<td>33 657</td>
<td>20 186</td>
</tr>
<tr>
<td>Travel</td>
<td>24 111</td>
<td>13 577</td>
</tr>
<tr>
<td>Translation Services</td>
<td>11 804</td>
<td>-</td>
</tr>
<tr>
<td>Other</td>
<td>42 325</td>
<td>33 888</td>
</tr>
<tr>
<td><strong>Total goods and services supplied or rendered</strong></td>
<td>318 172</td>
<td>266 024</td>
</tr>
</tbody>
</table>

**Goods and services are made up of:**

| Provision of goods – external entities | 12 677 | 7 727 |
| Rendering of services – related entities | 210 257 | 211 009 |
| Rendering of services – external entities | 95 238 | 47 288 |
| **Total goods and services** | 318 172 | 266 024 |

**Other supplier expenses**

| Workers compensation premiums | 4 760 | 4 659 |
| **Total other supplier expenses** | 4 760 | 4 659 |
| **Total supplier expenses** | 322 932 | 270 683 |
NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2015

Note 5 – Own-Source Income

OWN-SOURCE REVENUE

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td>Note 5A – Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inquiry Funding</td>
<td>-</td>
<td>139 741</td>
</tr>
</tbody>
</table>
| Employee FBT
| Contributions     | 5 403  | 8 329  |
| Other               | 75     | 1 933  |
| Resources Received Free of Charge: | | |
| Australian National Audit Office | 18 000 | 18 000 |
| Defence Signals
| Directorate       | 4 545  | 4 545  |
| Total other own-source revenue | 28 023 | 172 548 |

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td>Note 5B – Other Gains</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resources Received Free of Charge:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Department of the Prime Minister &amp; Cabinet</td>
<td>102 000</td>
<td>102 000</td>
</tr>
<tr>
<td>Total other gains</td>
<td>102 000</td>
<td>102 000</td>
</tr>
</tbody>
</table>

REVENUE FROM GOVERNMENT

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td>Note 5C – Revenue from Government</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appropriations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Departmental Appropriation</td>
<td>3 003 000</td>
<td>2 179 000</td>
</tr>
<tr>
<td>Total revenue from government</td>
<td>3 003 000</td>
<td>2 179 000</td>
</tr>
</tbody>
</table>

Note 6 – 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 6A – Fair Value Measurements, Valuation Techniques and Inputs Used

<table>
<thead>
<tr>
<th>Non-Financial Assets</th>
<th>Fair value measurement at the end of the reporting period</th>
<th>Category (Level 1, 2 or 3)</th>
<th>For Levels 2 and 3 fair value measurements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property, plant and equipment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 2 assets included office equipment and furniture</td>
<td>22 338</td>
<td>30 035</td>
<td>Level 2</td>
</tr>
<tr>
<td>Level 3 assets included computer equipment and office furniture</td>
<td>4 880</td>
<td>33 700</td>
<td>Level 3</td>
</tr>
</tbody>
</table>

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 6B – Level 1 and Level 2 Transfers for Recurring Fair Value Measurements

There were no transfers between levels during 2014-15.

OIGIS’s policy for determining when transfers between levels are deemed to have occurred can be found in Note 1.
NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2015

Note 7 – Financial Assets

Note 7A – Trade and other receivables

<table>
<thead>
<tr>
<th>Appropriations receivable:</th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>For existing programs</td>
<td>2,987,155</td>
<td>2,223,593</td>
</tr>
<tr>
<td><strong>Total appropriation receivable</strong></td>
<td><strong>2,987,155</strong></td>
<td><strong>2,223,593</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other Receivables:</th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>GST receivable from the Australian Taxation Office</td>
<td>1,752</td>
<td>153</td>
</tr>
<tr>
<td>Other receivables</td>
<td>77,015</td>
<td>6,457</td>
</tr>
<tr>
<td><strong>Total other receivables</strong></td>
<td><strong>78,767</strong></td>
<td><strong>6,610</strong></td>
</tr>
<tr>
<td><strong>Total trade and other receivables (gross)</strong></td>
<td><strong>3,065,922</strong></td>
<td><strong>2,230,203</strong></td>
</tr>
</tbody>
</table>

**Less Impairment Allowance:**

<table>
<thead>
<tr>
<th>Other</th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total trade and other receivables (net)</strong></td>
<td><strong>3,065,922</strong></td>
<td><strong>2,230,203</strong></td>
</tr>
</tbody>
</table>

**Receivables are aged as follows:**

Not overdue

<table>
<thead>
<tr>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>3,065,922</td>
<td>2,230,203</td>
</tr>
</tbody>
</table>

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

Note 8 – Non-Financial Assets

Note 8A – Property, plant and equipment

<table>
<thead>
<tr>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Other property, plant and equipment:</strong></td>
<td></td>
</tr>
<tr>
<td>Fair value</td>
<td>63,635</td>
</tr>
<tr>
<td>Accumulated depreciation</td>
<td>(36,417)</td>
</tr>
<tr>
<td><strong>Total property, plant and equipment</strong></td>
<td><strong>27,218</strong></td>
</tr>
</tbody>
</table>

All revaluations are independent and are conducted in accordance with the revaluation policy stated in Note 1.14. 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 2015 and none were found. With the exception of the secure IT system (which is due to be upgraded in late 2015) no items of property plant and equipment are expected to be sold or disposed of within the next 12 months. Note: the components of the secure IT system which are due for upgrading were given appropriate useful lives during the revaluation exercise in 2014 and were consequently not assessed as impaired at 30 June 2015.
# Notes to and forming part of the financial statements

for year ended 30 June 2015

Note 8B – Reconciliation of the Opening and Closing Balances of Property, Plant and Equipment (2014-15)

<table>
<thead>
<tr>
<th>Item</th>
<th>Other property, plant &amp; equipment $</th>
<th>Total $</th>
</tr>
</thead>
<tbody>
<tr>
<td>As at 1 July 2014</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gross book value</td>
<td>63 735</td>
<td>63 735</td>
</tr>
<tr>
<td>Accumulated depreciation and impairment</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Net book value as at 1 July 2014</td>
<td>63 735</td>
<td>63 735</td>
</tr>
</tbody>
</table>

Revaluations and impairments recognised in other comprehensive income

<table>
<thead>
<tr>
<th>Item</th>
<th>Other property, plant &amp; equipment $</th>
<th>Total $</th>
</tr>
</thead>
<tbody>
<tr>
<td>Depreciation expense</td>
<td>(36 481)</td>
<td>(36 481)</td>
</tr>
<tr>
<td>Disposals</td>
<td>(36)</td>
<td>(36)</td>
</tr>
<tr>
<td>Other</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Net Book Value 30 June 2015</td>
<td>27 218</td>
<td>27 218</td>
</tr>
</tbody>
</table>

Net Bank Value as at 30 June 2015 represented by:

<table>
<thead>
<tr>
<th>Item</th>
<th>Other property, plant &amp; equipment $</th>
<th>Total $</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gross book value</td>
<td>63 635</td>
<td>63 635</td>
</tr>
<tr>
<td>Accumulated depreciation and impairment</td>
<td>36 417</td>
<td>36 417</td>
</tr>
</tbody>
</table>

Note 8B – Reconciliation of the Opening and Closing Balances of Property, Plant and Equipment (2013-14)

<table>
<thead>
<tr>
<th>Item</th>
<th>Other property, plant &amp; equipment $</th>
<th>Total $</th>
</tr>
</thead>
<tbody>
<tr>
<td>As at 1 July 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gross book value</td>
<td>165 059</td>
<td>165 059</td>
</tr>
<tr>
<td>Accumulated depreciation and impairment</td>
<td>(78 416)</td>
<td>(78 416)</td>
</tr>
<tr>
<td>Net book value as at 1 July 2013</td>
<td>86 643</td>
<td>86 643</td>
</tr>
</tbody>
</table>

Additions

by purchase

<table>
<thead>
<tr>
<th>Item</th>
<th>Other property, plant &amp; equipment $</th>
<th>Total $</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 258</td>
<td></td>
<td>8 258</td>
</tr>
</tbody>
</table>

Revaluations and impairments recognised in other comprehensive income

<table>
<thead>
<tr>
<th>Item</th>
<th>Other property, plant &amp; equipment $</th>
<th>Total $</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 308</td>
<td></td>
<td>9 308</td>
</tr>
</tbody>
</table>

Depreciation expense

<table>
<thead>
<tr>
<th>Item</th>
<th>Other property, plant &amp; equipment $</th>
<th>Total $</th>
</tr>
</thead>
<tbody>
<tr>
<td>(37 999)</td>
<td></td>
<td>(37 999)</td>
</tr>
</tbody>
</table>

Disposals

<table>
<thead>
<tr>
<th>Item</th>
<th>Other property, plant &amp; equipment $</th>
<th>Total $</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2 475)</td>
<td></td>
<td>(2 475)</td>
</tr>
</tbody>
</table>

Net Book Value 30 June 2014

<table>
<thead>
<tr>
<th>Item</th>
<th>Other property, plant &amp; equipment $</th>
<th>Total $</th>
</tr>
</thead>
<tbody>
<tr>
<td>63 735</td>
<td></td>
<td>63 735</td>
</tr>
</tbody>
</table>

Net Bank Value as at 30 June 2014 represented by:

<table>
<thead>
<tr>
<th>Item</th>
<th>Other property, plant &amp; equipment $</th>
<th>Total $</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gross book value</td>
<td>63 735</td>
<td>63 735</td>
</tr>
<tr>
<td>Accumulated depreciation and impairment</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
## Note 9 – Payables

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td><strong>Note 9A - Suppliers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trade creditors and accruals</td>
<td>20,690</td>
<td>38,800</td>
</tr>
<tr>
<td><strong>Total suppliers</strong></td>
<td>20,690</td>
<td>38,800</td>
</tr>
<tr>
<td><strong>Supplier payables expected to be settled within 12 months:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Related entities</td>
<td>19,626</td>
<td>28,882</td>
</tr>
<tr>
<td>External parties</td>
<td>1,064</td>
<td>9,918</td>
</tr>
<tr>
<td><strong>Total supplier payables</strong></td>
<td>20,690</td>
<td>38,800</td>
</tr>
<tr>
<td>No supplier payables expected to be settled in greater than 12 months.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td><strong>Note 9B – Other Payables</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salaries and wages</td>
<td>67,338</td>
<td>48,968</td>
</tr>
<tr>
<td>Superannuation</td>
<td>10,572</td>
<td>8,411</td>
</tr>
<tr>
<td>Other</td>
<td>50,221</td>
<td>20,847</td>
</tr>
<tr>
<td><strong>Total other payables</strong></td>
<td>128,131</td>
<td>78,226</td>
</tr>
<tr>
<td><strong>Total other payables are expected to be settled in:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No more than 12 months</td>
<td>128,131</td>
<td>78,226</td>
</tr>
<tr>
<td><strong>Total other payables</strong></td>
<td>128,131</td>
<td>78,226</td>
</tr>
</tbody>
</table>

## Note 10 – Provisions

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td><strong>Note 10A – Employee Provisions</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leave</td>
<td>865,347</td>
<td>730,388</td>
</tr>
<tr>
<td><strong>Total employee provisions</strong></td>
<td>865,347</td>
<td>730,388</td>
</tr>
<tr>
<td><strong>Employee provisions are expected to be settled in:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No more than 12 months</td>
<td>145,538</td>
<td>106,878</td>
</tr>
<tr>
<td>More than 12 months</td>
<td>719,809</td>
<td>623,510</td>
</tr>
<tr>
<td><strong>Total employee provisions</strong></td>
<td>865,347</td>
<td>730,388</td>
</tr>
</tbody>
</table>
Note 11 – Cash Flow Reconciliation

Reconciliation of Cash and cash equivalents as per Statement of Financial Position to Cash flow statement

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td>Report cash and cash equivalents as per:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash Flow Statement</td>
<td>174 814</td>
<td>207 005</td>
</tr>
<tr>
<td>Statement of Financial Position</td>
<td>174 814</td>
<td>207 005</td>
</tr>
<tr>
<td>Difference</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Reconciliation of net cost of services to net cash from operating activities:

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td>Net cost of services</td>
<td>(2 417 869)</td>
<td>(1 952 667)</td>
</tr>
<tr>
<td>Add revenue from Government</td>
<td>3 003 000</td>
<td>2 179 000</td>
</tr>
<tr>
<td>Adjustments for non-cash items</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Depreciation/amortisation</td>
<td>36 481</td>
<td>37 999</td>
</tr>
<tr>
<td>Loss on disposal of assets</td>
<td>36</td>
<td>2 474</td>
</tr>
</tbody>
</table>

Movements in assets and liabilities

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td>Increase/(Decrease) in provision of employee liabilities</td>
<td>134 959</td>
<td>(6 679)</td>
</tr>
<tr>
<td>Increase/(Decrease) in other payables</td>
<td>49 905</td>
<td>25 418</td>
</tr>
<tr>
<td>Increase/(Decrease) in supplier trade creditors</td>
<td>(12 575)</td>
<td>28 308</td>
</tr>
<tr>
<td>(Increase)/Decrease in appropriation receivables</td>
<td>(748 436)</td>
<td>(317 623)</td>
</tr>
<tr>
<td>(Increase)/Decrease in other assets</td>
<td>(70 558)</td>
<td>(1 975)</td>
</tr>
<tr>
<td>(Increase)/Decrease in other prepayments</td>
<td>-</td>
<td>3 341</td>
</tr>
<tr>
<td>(Increase)/Decrease in GST receivable</td>
<td>(1 599)</td>
<td>92</td>
</tr>
<tr>
<td>Net cash from (used by) operating activities</td>
<td>(26 656)</td>
<td>(2 312)</td>
</tr>
</tbody>
</table>
NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2015

Note 12 – Senior Management Personnel Remuneration

2015  2014
$    $

Short-term employee benefits:
Salary  521 028  489 240
Annual leave\(^1\)  29 772 -
Total short-term employee benefits  550 800  489 240

Post-employment benefits:
Superannuation  94 438  82 538
Total post-employment benefits  94 438  82 538

Other long-term employee benefits:
Annual Leave  10 742  39 404
Long Service Leave  18 997  17 732
Total other long-term employee benefits  29 739  57 136

Termination benefits - -
Total senior executive remuneration expenses  674 977  628 914

The total number of senior management personnel that are included in the above table are 3 individuals (2014: 2 individuals). The 2015 figure includes one seconded officer for part of the year.

1 Annual Leave expected to be taken within 12 months.

Note 13 – Financial Instruments

2015  2014
$    $

Note 13A – Categories of Financial Instruments

Financial Assets
Loans and Receivables
Loans and receivables
Cash and cash equivalents  174 814  207 005
Trade receivables  77 015  6 457
Total carrying amount of financial assets  251 829  213 462

Financial Liabilities
At amortised cost
Trade creditors  20 690  38 800
Total carrying amount of financial liabilities  20 690  38 800

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.

Note 13B – 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.
NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2015

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.

Note 13C – 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.

Note 13D – 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 14 – Financial Asset Reconciliation

<table>
<thead>
<tr>
<th>Financial Assets</th>
<th>2015 $</th>
<th>2014 $</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total financial assets as per statement of financial position</td>
<td>3,240,736</td>
<td>2,437,208</td>
</tr>
<tr>
<td>Less: non-financial instrument components:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appropriation Receivable</td>
<td>2,987,155</td>
<td>2,223,593</td>
</tr>
<tr>
<td>GST Receivable</td>
<td>1,752</td>
<td>153</td>
</tr>
<tr>
<td>Total non-financial instrument components</td>
<td>2,988,907</td>
<td>2,223,746</td>
</tr>
<tr>
<td>Total financial assets as per financial instruments note</td>
<td>251,829</td>
<td>213,462</td>
</tr>
</tbody>
</table>

Note 15 – Appropriations

Note 15A – Annual Appropriations (‘ Recoverable GST exclusive’)

<table>
<thead>
<tr>
<th>Ordinary Annual Services</th>
<th>2015 $</th>
<th>2014 $</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annual Appropriation</td>
<td>3,029,000</td>
<td>2,248,000</td>
</tr>
<tr>
<td>PGPA Act – Section 74</td>
<td>116,500</td>
<td>401,110</td>
</tr>
<tr>
<td>PGPA Act – Section 75</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Total appropriation</td>
<td>3,145,500</td>
<td>2,649,110</td>
</tr>
<tr>
<td>Appropriation applied (current and prior years)</td>
<td>2,371,063</td>
<td>2,270,744</td>
</tr>
<tr>
<td>Variance</td>
<td>774,437</td>
<td>378,366</td>
</tr>
</tbody>
</table>

1 In 2013-14 relates to FMA Act Section 31.
2 Variance between Total Appropriation and Appropriation Applied is due to section 74 receipts and the additional appropriation received midyear. The additional appropriation was not fully expended largely due to recruitment delays associated with security clearance requirements.
Note 15B: Departmental Capital Budget (‘Recoverable GST exclusive)

<table>
<thead>
<tr>
<th>Departmental Capital Budget</th>
<th>2015 $</th>
<th>2014 $</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annual Departmental Capital Budget</td>
<td>26 000</td>
<td>69 000</td>
</tr>
<tr>
<td>Payments for non-financial assets</td>
<td>5 535</td>
<td>2 723</td>
</tr>
<tr>
<td>Variance</td>
<td>20 465</td>
<td>66 277</td>
</tr>
</tbody>
</table>

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. For more information on ordinary annual services appropriations, please see Table A: Annual Appropriations.

2. Payments made for non-financial assets include purchases of assets and expenditure on assets which have been capitalised.

Note 15C: Unspent Annual Appropriations (‘Recoverable GST exclusive)

<table>
<thead>
<tr>
<th>Department</th>
<th>2015 $</th>
<th>2014 $</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appropriation Act (No 1) 2010-11 – DCB</td>
<td>-</td>
<td>1 874</td>
</tr>
<tr>
<td>Appropriation Act (No 1) 2011-12 – DCB</td>
<td>-</td>
<td>9 000</td>
</tr>
<tr>
<td>Appropriation Act (No 1) 2013-14</td>
<td>-</td>
<td>2 142 718</td>
</tr>
<tr>
<td>Appropriation Act (No 1) 2013-14 - DCB</td>
<td>69 000</td>
<td>69 000</td>
</tr>
<tr>
<td>Appropriation Act (No 1) 2014-15</td>
<td>2 051 155</td>
<td></td>
</tr>
<tr>
<td>Appropriation Act (No 3) 2014-15</td>
<td>840 000</td>
<td></td>
</tr>
<tr>
<td>Appropriation Act (No 1) 2014-15 – DCB</td>
<td>26 000</td>
<td></td>
</tr>
<tr>
<td>Cash</td>
<td>174 814</td>
<td>207 005</td>
</tr>
<tr>
<td>Total Departmental</td>
<td>3 160 969</td>
<td>2 429 597</td>
</tr>
</tbody>
</table>

1. Appropriation Act (No. 1) 2010-2011 – DCB and Appropriation Act (No 1) 2011-2012 -DCB lapsed with effect from 1 July 2014. The effect has been reflected in the Statement of Financial Position in Contributed Equity.

Note 16 – Reporting of Outcomes

There is only one outcome for OGIS as detailed in the objectives in Note 1.1.

Note 16A – Net Cost of Outcome Delivery

<table>
<thead>
<tr>
<th>Outcome 1</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2015 $</td>
</tr>
<tr>
<td>Departmental Expenses</td>
<td>2 547 892</td>
</tr>
<tr>
<td>Own-source income</td>
<td>130 023</td>
</tr>
<tr>
<td>Net cost/(contribution) of outcome delivery</td>
<td>2 417 869</td>
</tr>
</tbody>
</table>
NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2015

Note 17 – Budgetary Reports and Explanation of Major Variances

The following tables provide a comparison of the original budget as presented in the 2014-15 Portfolio Budget Statements (PBS) to the 2014-15 final outcome as presented in accordance with Australian Accounting Standards for OIGIS. The Budget is not audited. Explanations of major variances are provided further below.

Note 17A: Departmental Budgetary Reports

Statement of Comprehensive Income for not-for-profit Reporting Entities
for the year ended 30 June 2015

<table>
<thead>
<tr>
<th></th>
<th>Actual 2015</th>
<th>Budget Estimate 2015</th>
<th>Variance 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td><strong>NET COST OF SERVICES</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expenses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee benefits</td>
<td>2 188 443</td>
<td>1 905 000</td>
<td>283 443</td>
</tr>
<tr>
<td>Supplier</td>
<td>322 932</td>
<td>376 000</td>
<td>(53 068)</td>
</tr>
<tr>
<td>Depreciation and amortisation</td>
<td>36 481</td>
<td>13 000</td>
<td>23 481</td>
</tr>
<tr>
<td>Loss on asset disposal</td>
<td>36</td>
<td>-</td>
<td>36</td>
</tr>
<tr>
<td><strong>Total Expenses</strong></td>
<td>2 547 892</td>
<td>2 294 000</td>
<td>253 892</td>
</tr>
<tr>
<td>Own-Source Income</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Own-source revenue</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other revenue</td>
<td>28 023</td>
<td>-</td>
<td>28 023</td>
</tr>
<tr>
<td><strong>Total own-source income</strong></td>
<td>28 023</td>
<td>-</td>
<td>28 023</td>
</tr>
<tr>
<td>Gains</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other gains</td>
<td>102 000</td>
<td>118 000</td>
<td>(16 000)</td>
</tr>
<tr>
<td><strong>Total gains</strong></td>
<td>102 000</td>
<td>118 000</td>
<td>(16 000)</td>
</tr>
<tr>
<td><strong>Total own-source income</strong></td>
<td>130 023</td>
<td>118 000</td>
<td>12 023</td>
</tr>
<tr>
<td><strong>Net Cost of services</strong></td>
<td>2 417 869</td>
<td>2 176 000</td>
<td>241 869</td>
</tr>
<tr>
<td>Revenue from Government</td>
<td>3 003 000</td>
<td>2 163 000</td>
<td>840 000</td>
</tr>
<tr>
<td><strong>Surplus attributable to the Australian Government</strong></td>
<td>585 131</td>
<td>(13 000)</td>
<td>598 131</td>
</tr>
<tr>
<td><strong>OTHER COMPREHENSIVE INCOME</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Items not subject to subsequent reclassification to net cost of services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Changes in asset revaluation surplus</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Total comprehensive income</strong></td>
<td>585 131</td>
<td>(13 000)</td>
<td>598 131</td>
</tr>
</tbody>
</table>
NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for year ended 30 June 2015

Statement of Financial Position for not-for-profit Reporting Entities
As at 30 June 2015

<table>
<thead>
<tr>
<th></th>
<th>Actual 2015</th>
<th>Budget Estimate 2015</th>
<th>Variance 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td><strong>ASSETS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Financial Assets</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash and cash equivalents</td>
<td>174 814</td>
<td>202 000</td>
<td>(27 186)</td>
</tr>
<tr>
<td>Trade and other receivables</td>
<td>3 065 922</td>
<td>1 840 000</td>
<td>1 225 922</td>
</tr>
<tr>
<td><strong>Total financial assets</strong></td>
<td>3 240 736</td>
<td>2 042 000</td>
<td>1 198 736</td>
</tr>
<tr>
<td><strong>Non-Financial Assets</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Property, plant and equipment</td>
<td>27 218</td>
<td>157 000</td>
<td>(129 782)</td>
</tr>
<tr>
<td>Other non-financial assets</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Total non-financial assets</strong></td>
<td>27 218</td>
<td>157 000</td>
<td>(129 782)</td>
</tr>
<tr>
<td><strong>Total Assets</strong></td>
<td>3 267 954</td>
<td>2 199 000</td>
<td>1 068 954</td>
</tr>
<tr>
<td><strong>LIABILITIES</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Payables</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suppliers</td>
<td>20 690</td>
<td>5 000</td>
<td>15 690</td>
</tr>
<tr>
<td>Other payables</td>
<td>128 131</td>
<td>-</td>
<td>128 131</td>
</tr>
<tr>
<td><strong>Total payables</strong></td>
<td>148 821</td>
<td>5 000</td>
<td>143 821</td>
</tr>
<tr>
<td><strong>Provisions</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee provisions</td>
<td>865 347</td>
<td>774 000</td>
<td>91 347</td>
</tr>
<tr>
<td><strong>Total provisions</strong></td>
<td>865 347</td>
<td>774 000</td>
<td>91 347</td>
</tr>
<tr>
<td><strong>Total Liabilities</strong></td>
<td>1 014 168</td>
<td>779 000</td>
<td>235 168</td>
</tr>
<tr>
<td><strong>Net Assets</strong></td>
<td>2 253 786</td>
<td>1 420 000</td>
<td>833 786</td>
</tr>
<tr>
<td><strong>EQUITY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contributed equity</td>
<td>478 126</td>
<td>489 000</td>
<td>(10 874)</td>
</tr>
<tr>
<td>Reserves</td>
<td>16 105</td>
<td>7 000</td>
<td>9 105</td>
</tr>
<tr>
<td>Retained surplus</td>
<td>1 759 555</td>
<td>924 000</td>
<td>835 555</td>
</tr>
<tr>
<td><strong>Total Equity</strong></td>
<td>2 253 786</td>
<td>1 420 000</td>
<td>833 786</td>
</tr>
</tbody>
</table>
## Statement of Changes in Equity for not-for-profit Reporting Entities

**for the period ended 30 June 2015**

<table>
<thead>
<tr>
<th></th>
<th>Retained Earnings</th>
<th>Asset Revaluation Surplus</th>
<th>Contributed Equity/Capital</th>
<th>Total Equity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Actual</td>
<td>Budget Estimate</td>
<td>Actual</td>
<td>Budget Estimate</td>
</tr>
<tr>
<td></td>
<td>Original Variance</td>
<td>Original Variance</td>
<td>Original Variance</td>
<td>Original Variance</td>
</tr>
<tr>
<td>2015</td>
<td>$</td>
<td>$</td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td>Opening Balance</td>
<td>1 174 424</td>
<td>937 000</td>
<td>237 424</td>
<td>16 105</td>
</tr>
<tr>
<td>Adjusted opening balance</td>
<td>1 174 424</td>
<td>937 000</td>
<td>237 424</td>
<td>16 105</td>
</tr>
<tr>
<td>Comprehensive Income</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Surplus for the period</td>
<td>585 131</td>
<td>(13 000)</td>
<td>598 131</td>
<td>-</td>
</tr>
<tr>
<td>Other Comprehensive Income</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Comprehensive Income</td>
<td>585 131</td>
<td>(13 000)</td>
<td>598 131</td>
<td>-</td>
</tr>
<tr>
<td>Transactions with owners</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contributions by owners</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduction of Appropriation – Omnibus Repeal Day Act 2014</td>
<td></td>
<td>(10 874)</td>
<td>-</td>
<td>(10 874)</td>
</tr>
<tr>
<td>Departmental Capital Budget</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Total Transactions with Owners</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Closing balance as at 30 June</td>
<td>1 759 555</td>
<td>924 000</td>
<td>835 555</td>
<td>16 105</td>
</tr>
</tbody>
</table>
### Cash Flow Statement for not-for-profit Reporting Entities

#### for the period ended 30 June 2015

<table>
<thead>
<tr>
<th></th>
<th>Actual 2015</th>
<th>Budget Estimate 2015 Original</th>
<th>Variance 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OPERATING ACTIVITIES</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash received</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appropriations</td>
<td>2 371 063</td>
<td>2 339 000</td>
<td>32 063</td>
</tr>
<tr>
<td>Sales of goods and rendering of services</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Other</td>
<td>125 097</td>
<td>-</td>
<td>125 097</td>
</tr>
<tr>
<td>Total cash received</td>
<td>2 496 160</td>
<td>2 339 000</td>
<td>157 160</td>
</tr>
<tr>
<td>Cash used</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employees</td>
<td>(2 092 294)</td>
<td>(1 932 000)</td>
<td>160 294</td>
</tr>
<tr>
<td>Suppliers</td>
<td>(314 023)</td>
<td>(407 000)</td>
<td>(92 977)</td>
</tr>
<tr>
<td>Net GST paid</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Other</td>
<td>(116 499)</td>
<td>-</td>
<td>116 499</td>
</tr>
<tr>
<td>Total cash used</td>
<td>(2 522 816)</td>
<td>(2 339 000)</td>
<td>(183 816)</td>
</tr>
<tr>
<td>Net cash from operating activities</td>
<td>(26 656)</td>
<td>-</td>
<td>(26 656)</td>
</tr>
<tr>
<td><strong>INVESTING ACTIVITIES</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash received</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proceeds from sales of property, plant and equipment</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Total cash received</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Cash used</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purchase of property, plant and equipment</td>
<td>(5 535)</td>
<td>(92 000)</td>
<td>86 465</td>
</tr>
<tr>
<td>Total cash used</td>
<td>(5 535)</td>
<td>(92 000)</td>
<td>86 465</td>
</tr>
<tr>
<td>Net cash from (used by) investing activities</td>
<td>(5 535)</td>
<td>(92 000)</td>
<td>86 465</td>
</tr>
<tr>
<td><strong>FINANCING ACTIVITIES</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash received</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contributed equity</td>
<td>-</td>
<td>92 000</td>
<td>(92 000)</td>
</tr>
<tr>
<td>Total cash received</td>
<td>-</td>
<td>92 000</td>
<td>(92 000)</td>
</tr>
<tr>
<td>Net cash from financing activities</td>
<td>-</td>
<td>92 000</td>
<td>(92 000)</td>
</tr>
<tr>
<td>Net increase in cash held</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash and cash equivalents at the beginning of the reporting period</td>
<td>207 005</td>
<td>202 000</td>
<td>5 005</td>
</tr>
<tr>
<td>Cash and cash equivalents at the end of the reporting period</td>
<td>174 814</td>
<td>202 000</td>
<td>(27 186)</td>
</tr>
</tbody>
</table>
### Note 17B – Departmental Major Budget Variances for 2015

<table>
<thead>
<tr>
<th>Explanation of major variances</th>
<th>Affected line items (and statement)</th>
</tr>
</thead>
<tbody>
<tr>
<td>At MYEFO the office received additional funding as part of the measure ‘National Security- additional counter-terrorism funding’. This included funding for five additional ASL for the full financial year. Three of these positions were filled with already cleared staff. Recruitment delays are associated with the lengthy security clearance process.</td>
<td>Impacted: Revenue from government Employee expenses Supplier expenses Appropriations receivable Employee provisions Other payables Retained surplus Cashflow statement operating activities</td>
</tr>
<tr>
<td>The variance is partly due to the effect on depreciation of changes in asset values and estimated remaining lives after the asset revaluation conducted at 30 June 2014.</td>
<td>Impacted: Depreciation Expenses</td>
</tr>
<tr>
<td>The value of resources received free of charge (office space) was less than originally budgeted for.</td>
<td>Impacted: Other Gains</td>
</tr>
<tr>
<td>The planned secure IT system upgrade was deferred until late 2015. The departmental capital funding was moved to 2015-16 during the year.</td>
<td>Impacted: Property, plant and equipment Cash flow statement – cash used for investing activities and cash received from contributed equity.</td>
</tr>
</tbody>
</table>
Annex 1

Summary of Inquiries and Complaints

Table 1.1 IGIS Act Inquiries actioned between 1 July 2014 and 30 June 2015

<table>
<thead>
<tr>
<th>Agency</th>
<th>Source</th>
<th>Inquiry</th>
<th>Date initiated</th>
<th>Date finalised</th>
<th>Duration (days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASIS</td>
<td>IGIS</td>
<td>Inquiry into the management of weapons by ASIS in a particular location</td>
<td>10 June 2014</td>
<td>12 December 2014</td>
<td>184</td>
</tr>
<tr>
<td>ASD</td>
<td>IGIS</td>
<td>Inquiry into a matter relating to ASD</td>
<td>9 February 2015</td>
<td>Ongoing</td>
<td></td>
</tr>
</tbody>
</table>

Table 1.2 Summary of complaints handled administratively by OIGIS between 1 July 2014 and 30 June 2015

<table>
<thead>
<tr>
<th>Agency</th>
<th>Number of complaints</th>
<th>From public</th>
<th>From intelligence agency employee or ex-employee</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASIO (visa security assessments)</td>
<td>473</td>
<td>473</td>
<td>0</td>
</tr>
<tr>
<td>ASIO (all other complaints)</td>
<td>19</td>
<td>16</td>
<td>3</td>
</tr>
<tr>
<td>ASIS</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>ASD</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>AGO</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DIO</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ONA</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TOTAL Complaints</td>
<td>496</td>
<td>492</td>
<td>4</td>
</tr>
</tbody>
</table>
## Annex 2

### Salary ranges for APS Employees in OIGIS in 2014–15

<table>
<thead>
<tr>
<th>OIGIS Band</th>
<th>APS Level</th>
<th>Salary Range 1 July 2014 – 30 June 2015 ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SES Band 1</td>
<td>SES Band 1</td>
<td>179,458</td>
</tr>
<tr>
<td>OIGIS Band 4</td>
<td>EL2</td>
<td>133,967</td>
</tr>
<tr>
<td></td>
<td></td>
<td>130,796</td>
</tr>
<tr>
<td></td>
<td></td>
<td>128,258</td>
</tr>
<tr>
<td></td>
<td></td>
<td>119,013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>112,564</td>
</tr>
<tr>
<td>OIGIS Band 3</td>
<td>EL1</td>
<td>107,810</td>
</tr>
<tr>
<td></td>
<td></td>
<td>104,635</td>
</tr>
<tr>
<td></td>
<td></td>
<td>96,710</td>
</tr>
<tr>
<td>OIGIS Band 2</td>
<td>APS6</td>
<td>89,973</td>
</tr>
<tr>
<td></td>
<td></td>
<td>87,199</td>
</tr>
<tr>
<td></td>
<td></td>
<td>84,027</td>
</tr>
<tr>
<td></td>
<td></td>
<td>80,063</td>
</tr>
<tr>
<td></td>
<td>APS5</td>
<td>76,101</td>
</tr>
<tr>
<td></td>
<td></td>
<td>74,513</td>
</tr>
<tr>
<td></td>
<td></td>
<td>72,531</td>
</tr>
<tr>
<td></td>
<td></td>
<td>70,155</td>
</tr>
<tr>
<td></td>
<td>APS4</td>
<td>68,569</td>
</tr>
<tr>
<td></td>
<td></td>
<td>66,586</td>
</tr>
<tr>
<td></td>
<td></td>
<td>65,003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>63,021</td>
</tr>
</tbody>
</table>
Annex 2 continued

<table>
<thead>
<tr>
<th>OIGIS Band</th>
<th>APS Level</th>
<th>Salary Range 1 July 2014 – 30 June 2015 ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OIGIS Band 1</td>
<td>APS3</td>
<td>61,038</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>59,453</td>
</tr>
<tr>
<td></td>
<td></td>
<td>57,866</td>
</tr>
<tr>
<td></td>
<td></td>
<td>56,680</td>
</tr>
<tr>
<td></td>
<td>APS2</td>
<td>55,092</td>
</tr>
<tr>
<td></td>
<td></td>
<td>53,509</td>
</tr>
<tr>
<td></td>
<td></td>
<td>51,129</td>
</tr>
<tr>
<td></td>
<td></td>
<td>49,543</td>
</tr>
<tr>
<td></td>
<td>APS1</td>
<td>48,355</td>
</tr>
<tr>
<td></td>
<td></td>
<td>46,373</td>
</tr>
<tr>
<td></td>
<td></td>
<td>45,184</td>
</tr>
<tr>
<td></td>
<td></td>
<td>45,138</td>
</tr>
</tbody>
</table>
# Annex 3

## Agency resource statements

### Table 3.1 Agency Resource Statement and Resources for Outcomes 2014-15

<table>
<thead>
<tr>
<th></th>
<th>Actual available appropriation for 2014-15 $’000 (a)</th>
<th>Payments made 2014-15 $’000 (b)</th>
<th>Balance remaining 2014-15 (a) – (b)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ordinary Annual Services</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Departmental Appropriation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prior year departmental appropriation</td>
<td>2 419</td>
<td>2 142</td>
<td>277</td>
</tr>
<tr>
<td>Departmental appropriation</td>
<td>3 029</td>
<td>269</td>
<td>2 760</td>
</tr>
<tr>
<td>S74 Relevant Agency Receipts</td>
<td>125</td>
<td>-</td>
<td>125</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>5 573</strong></td>
<td><strong>2 411</strong></td>
<td><strong>3 162</strong></td>
</tr>
<tr>
<td>Administered expenses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total available annual services</strong></td>
<td><strong>5 573</strong></td>
<td><strong>2 411</strong></td>
<td><strong>3 162</strong></td>
</tr>
<tr>
<td><strong>Other services</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Departmental non-operating</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total other services</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total available annual appropriations</strong></td>
<td><strong>5 573</strong></td>
<td><strong>2 411</strong></td>
<td><strong>3 162</strong></td>
</tr>
<tr>
<td><strong>Special appropriations</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total special appropriations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Special accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total special accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total resourcing</strong></td>
<td><strong>5 573</strong></td>
<td><strong>2 411</strong></td>
<td><strong>3 162</strong></td>
</tr>
<tr>
<td>A + B + C + D</td>
<td><strong>5 573</strong></td>
<td><strong>2 411</strong></td>
<td><strong>3 162</strong></td>
</tr>
<tr>
<td>Less appropriations drawn from annual or special appropriations above and credited to special accounts and/or CAC Act bodies through annual appropriations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total net resourcing for agency</strong></td>
<td><strong>5 573</strong></td>
<td><strong>2 411</strong></td>
<td><strong>3 162</strong></td>
</tr>
</tbody>
</table>
### Table 3.2 Expenses and Resources for Outcome 1

<table>
<thead>
<tr>
<th>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</th>
<th>Budget 2014-15 $’000</th>
<th>Actual expenses 2014-15 $’000</th>
<th>Variation 2014-15 $’000</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Program 1.1: Office of the Inspector-General of Intelligence and Security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Departmental expenses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ordinary annual services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Appropriation Bill No.1)</td>
<td>3 003</td>
<td>3 003</td>
<td>-</td>
</tr>
<tr>
<td>Revenue from independent sources</td>
<td>-</td>
<td>5</td>
<td>(5)</td>
</tr>
<tr>
<td>Special appropriations</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Special Accounts</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Expenses not requiring appropriation in the Budget year</td>
<td>131</td>
<td>160</td>
<td>(29)</td>
</tr>
<tr>
<td><strong>Total for Program 1.1</strong></td>
<td>3 134</td>
<td>3 168</td>
<td>(34)</td>
</tr>
<tr>
<td><strong>Outcome 1 Totals by appropriation type</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Departmental expenses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ordinary annual services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Appropriation Bill No.1)</td>
<td>3 003</td>
<td>3 003</td>
<td>-</td>
</tr>
<tr>
<td>Revenue from independent sources</td>
<td>-</td>
<td>5</td>
<td>(5)</td>
</tr>
<tr>
<td>Special appropriations</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Special Accounts</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Expenses not requiring appropriation in the Budget year</td>
<td>131</td>
<td>160</td>
<td>(29)</td>
</tr>
<tr>
<td><strong>Total expenses for Outcome 1</strong></td>
<td>3 134</td>
<td>3 168</td>
<td>(34)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Budget 2014-15</th>
<th>Actual 2014-15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Staffing Level (number)</td>
<td>13</td>
</tr>
</tbody>
</table>
## Annex 4

### Requirements for annual reports

<table>
<thead>
<tr>
<th>Description</th>
<th>Requirement</th>
<th>Part of Report</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Letter of transmittal</td>
<td>Mandatory</td>
<td>Preliminary</td>
<td>i</td>
</tr>
<tr>
<td>Table of contents</td>
<td>Mandatory</td>
<td>Preliminary</td>
<td>ii–iii</td>
</tr>
<tr>
<td>Index</td>
<td>Mandatory</td>
<td>Annex</td>
<td>88</td>
</tr>
<tr>
<td>Glossary</td>
<td>Mandatory</td>
<td>Preliminary</td>
<td>iv</td>
</tr>
<tr>
<td>Contact officer(s)</td>
<td>Mandatory</td>
<td>Preliminary</td>
<td>inside front cover</td>
</tr>
<tr>
<td>Internet home page address and internet address for report</td>
<td>Mandatory</td>
<td>Preliminary</td>
<td>inside front cover</td>
</tr>
<tr>
<td>Review by agency head</td>
<td>Mandatory</td>
<td>Overview</td>
<td>1–7</td>
</tr>
<tr>
<td>Summary of significant issues and developments</td>
<td>Suggested</td>
<td>Overview</td>
<td>3–7</td>
</tr>
<tr>
<td>Overview of agency’s performance and financial results</td>
<td>Suggested</td>
<td>Overview</td>
<td>3–7, 40–41</td>
</tr>
<tr>
<td>Outlook for following year</td>
<td>Suggested</td>
<td>Overview</td>
<td>3–4</td>
</tr>
<tr>
<td>Significant issues and developments – portfolio</td>
<td>Portfolio departments – suggested</td>
<td>Overview</td>
<td>N/A</td>
</tr>
<tr>
<td>Role and functions</td>
<td>Mandatory</td>
<td>Overview</td>
<td>1, 4–6</td>
</tr>
<tr>
<td>Organisational structure</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>42</td>
</tr>
<tr>
<td>Outcome and programme structure</td>
<td>Mandatory</td>
<td>Performance</td>
<td>8</td>
</tr>
<tr>
<td>Where outcome and programme structures differ from PB Statements/PAES or other portfolio statements accompanying any other additional appropriation bills (other portfolio statements), details of variation and reasons for change</td>
<td>Mandatory</td>
<td>Performance</td>
<td>N/A</td>
</tr>
<tr>
<td>Portfolio structure</td>
<td>Portfolio departments – mandatory</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Review of performance during the year in relation to programmes and contribution to outcomes</td>
<td>Mandatory</td>
<td>Performance</td>
<td>8–41</td>
</tr>
<tr>
<td>Actual performance in relation to deliverables and KPIs set out in PB Statements/PAES or other portfolio statements</td>
<td>Mandatory</td>
<td>Performance</td>
<td>8–41</td>
</tr>
<tr>
<td>Description</td>
<td>Requirement</td>
<td>Part of Report</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>-------------</td>
<td>----------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Where performance targets differ from the PBS/PAES, details of both former and new targets, and reasons for the change</td>
<td>Mandatory</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Narrative discussion and analysis of performance</td>
<td>Mandatory</td>
<td>Performance</td>
<td>8–41</td>
</tr>
<tr>
<td>Trend information</td>
<td>Mandatory</td>
<td>Performance</td>
<td>10, 12, 18–19, 40–41</td>
</tr>
<tr>
<td>Significant changes in nature of principal functions/services</td>
<td>Suggested</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Performance of purchaser/provider arrangements</td>
<td>If applicable, suggested</td>
<td>Management &amp; Accountability</td>
<td>45</td>
</tr>
<tr>
<td>Factors, events or trends influencing agency performance</td>
<td>Suggested</td>
<td>Overview</td>
<td>1, 3–7</td>
</tr>
<tr>
<td>Contribution of risk management in achieving objectives</td>
<td>Suggested</td>
<td>Management &amp; Accountability</td>
<td>42, 43, 44</td>
</tr>
<tr>
<td>Performance against service charter customer service standards, complaints data, and the department's response to complaints</td>
<td>If applicable – mandatory</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Discussion and analysis of the department's financial performance</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>40–41</td>
</tr>
<tr>
<td>Discussion of any significant changes in financial results from the prior year, from budget or anticipated to have a significant impact on future operations</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>3, 40–41</td>
</tr>
<tr>
<td>Agency resource statement and summary resource tables by outcomes</td>
<td>Mandatory</td>
<td>Annex</td>
<td>82–83</td>
</tr>
<tr>
<td>Agency heads are required to certify their agency’s actions in dealing with fraud</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>i</td>
</tr>
<tr>
<td>Statement of the main corporate governance practices in place</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>42–43</td>
</tr>
<tr>
<td>Names of the senior executive and their responsibilities</td>
<td>Suggested</td>
<td>Management &amp; Accountability</td>
<td>42</td>
</tr>
<tr>
<td>Senior management committees and their roles</td>
<td>Suggested</td>
<td>Management &amp; Accountability</td>
<td>42</td>
</tr>
<tr>
<td>Corporate and operational plans and associated performance reporting and review</td>
<td>Suggested</td>
<td>Management &amp; Accountability</td>
<td>42</td>
</tr>
<tr>
<td>Internal audit arrangements including approach adopted to identifying areas of significant financial or operational risk and arrangements to manage those risks</td>
<td>Suggested</td>
<td>Management &amp; Accountability</td>
<td>44</td>
</tr>
<tr>
<td>Policy and practices on the establishment and maintenance of appropriate ethical standards</td>
<td>Suggested</td>
<td>Management &amp; Accountability</td>
<td>43</td>
</tr>
<tr>
<td>How nature and amount of remuneration for SES officers is determined</td>
<td>Suggested</td>
<td>Management &amp; Accountability</td>
<td>43</td>
</tr>
<tr>
<td>Description</td>
<td>Requirement</td>
<td>Part of Report</td>
<td>Page</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
<td>---------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Significant developments in external scrutiny</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>43</td>
</tr>
<tr>
<td>Judicial decisions and decisions of administrative tribunals and by the Australian Information Commissioner</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>19, 43</td>
</tr>
<tr>
<td>Reports by the Auditor-General, a Parliamentary Committee, the Commonwealth Ombudsman or an agency capability review</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>6-7, 43</td>
</tr>
<tr>
<td>Assessment of effectiveness in managing and developing human resources to achieve departmental objectives</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>3, 44–45</td>
</tr>
<tr>
<td>Workforce planning, staff turnover and retention</td>
<td>Suggested</td>
<td>Management &amp; Accountability</td>
<td>44–45</td>
</tr>
<tr>
<td>Impact and features of enterprise or collective agreements, individual flexibility arrangements (IFAs), determinations, common law contracts and Australian Workplace Agreements (AWAs)</td>
<td>Suggested</td>
<td>Management &amp; Accountability</td>
<td>44–45</td>
</tr>
<tr>
<td>Training and development undertaken and its impact</td>
<td>Suggested</td>
<td>Management &amp; Accountability</td>
<td>3, 45</td>
</tr>
<tr>
<td>Work health and safety performance</td>
<td>Suggested</td>
<td>Management &amp; Accountability</td>
<td>46</td>
</tr>
<tr>
<td>Productivity gains</td>
<td>Suggested</td>
<td>Management &amp; Accountability</td>
<td>3, 18–19, 20</td>
</tr>
<tr>
<td>Statistics on staffing</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>44</td>
</tr>
<tr>
<td>Statistics on employees who identify as Indigenous</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>44</td>
</tr>
<tr>
<td>Enterprise or collective agreements, IFAs, determinations, common law contracts and AWAs</td>
<td>Mandatory</td>
<td>Management &amp; Accountability; Annex 2 Salary ranges</td>
<td>44–45</td>
</tr>
<tr>
<td>Performance pay</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>45</td>
</tr>
<tr>
<td>Assessment of effectiveness of assets management</td>
<td>If applicable, mandatory</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Assessment of purchasing against core policies and principles</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>45</td>
</tr>
<tr>
<td>Description</td>
<td>Requirement</td>
<td>Part of Report</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
<td>-----------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Summary statement detailing the number of new consultancy services let during the year; the total actual expenditure on all new consultancy contracts let during the year (inclusive of GST); the number of ongoing consultancy contracts that were active in the reporting year; and the total actual expenditure in the reporting year on the ongoing consultancy contracts (inclusive of GST). A statement noting that information on contracts and consultancies is available through the AusTender website.</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>45</td>
</tr>
<tr>
<td>Absence of provisions in contracts allowing access by the Auditor-General</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>45</td>
</tr>
<tr>
<td>Contracts exempted from publication in AusTender</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>45</td>
</tr>
<tr>
<td>Procurement initiatives to support small business</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>45</td>
</tr>
<tr>
<td>Financial Statements</td>
<td>Mandatory</td>
<td>Financial Statements</td>
<td>46-77</td>
</tr>
<tr>
<td>Work health and safety (Schedule 2, Part 4 of the Work Health and Safety Act 2011)</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>46</td>
</tr>
<tr>
<td>Advertising and Market Research (section 311A of the Commonwealth Electoral Act 1918) and statement on advertising campaigns</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>46</td>
</tr>
<tr>
<td>Compliance with the agency’s obligations under the Carer Recognition Act 2010</td>
<td>If applicable, mandatory</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Grant programmes</td>
<td>Mandatory</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Disability reporting – explicit and transparent reference to agency-level information available through other reporting mechanisms</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>46</td>
</tr>
<tr>
<td>Information Publication Scheme statement</td>
<td>Mandatory</td>
<td>Management &amp; Accountability</td>
<td>45</td>
</tr>
<tr>
<td>Correction of material errors in previous annual report</td>
<td>If applicable – mandatory</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Agency Resource Statements and Resources for Outcomes</td>
<td>Mandatory</td>
<td>Annex 5</td>
<td>84-87</td>
</tr>
</tbody>
</table>
A

address and contact details, inside front cover
administrative tribunals, 19, 43
adverse security assessments, 12, 26–7 see also visa
security assessment processes
advertising and market research, 46
agency resource statements, 82–3
analytic independence inquiry of 2012–13,
implementation of recommendations, 28–9
ANAO see Australian National Audit Office
Anti-Money Laundering and Counter Terrorism
Financing Act 2006, 39, 40
Archives Act 1983, IGIS role, 1, 19, 29
Assistant Inspector-General of Intelligence and
Security, 9, 17, 42, 43
assumed identities, 39
Attorney-General
ASIO submissions to, 4, 23, 26, 28
emergency ministerial authorisations, 36–7
IGIS statement on AUSTRAC use, 39
reporting on warrants to, 4, 6, 23
responsibilities, 2, 6, 24, 26
and Special Intelligence Operations, 24–5
warrant authorisations, 21, 22, 23
Attorney-General’s Department, 5, 12, 23, 30
Attorney-General’s Guidelines under ASIO Act, 2, 5,
21, 24–5, 29, 30
Audit Committee, 42, 43, 44
Auditor-General, 43, 45 see also Australian National
Audit Office
audits
ANAO report on financial statements, 40, 43
internal audit, 44
AUSCHECK, 15
AusTender, 45
AUSTRAC information access and use, 39–40
Australian Defence Force
ASD support for an ADF activity, 36
ASIS assistance to and cooperation with, 5–6,
33
Australian Geospatial-Intelligence Organisation
(AGO)
authorisations to collect intelligence, 31, 36,
37–8
complaints, 79
inspections of, 37–8
intelligence collected over Australian territory,
31, 38
privacy rules, 31–2
recordkeeping, 38
role and functions, 3, 30
Australian Human Rights Commission (AHRC)
referrals to OIGIS, 18
Australian Imagery and Geospatial Organisation
(AGO)
authorisations to collect intelligence, 5–6, 30–1
reporting and notification requirements, 6
Australian Intelligence Community see intelligence
agencies
Australian National Audit Office
access clauses, 45
and accountability of AIC agencies, 1
audit report, 40, 43
Australian National University National Security College, 9

**Australian Passports Act 2005**, 28

Australian persons
- assessed to be in or intending to travel to Syria or Iraq, 26, 28
- intelligence collection on, 4, 32–3, 35–6
- intelligence retention and communication on, 4, 25–6 *see also* privacy rules compliance

Australian Public Service Commission, 46

Australian Secret Intelligence Service (ASIS), 4
- assistance to/cooperation with ADF, 5–6, 33
- assumed identities, 39
- AUSTRAC information access and use, 39, 40
- authorisations to collect intelligence, 5–6, 30–1, 32
- complaints, 12
- cooperation with ASIO, 4, 5, 32
- cooperation with foreign liaisons, 33, 34
- Director-General, 34, 39
- IGIS briefings for ASIS officers, 9
- inquiries relating to, 4, 10, 79
- inspections of, 32–5, 38–9, 40
- intelligence on Australian persons, 4, 32–3
- life insurance for staff, 38
- misconduct investigation, 14
- new powers, 4
- privacy rules, 31–2, 33
- procedural changes as a result of IGIS recommendations, 20
- recordkeeping, 34
- reporting and notification requirements, 5, 6
- ‘request for information’ processes, 25–6
- review of operational files, 34
- role and functions, 2, 30
- training, 32
- weapons use and issues, 4, 10, 18, 20, 34–5

Australian Security Intelligence Organisation (ASIO)
- analytic independence inquiry of 2012–13, implementation of recommendations, 28–9
- assumed identities, 39
- AUSTRAC information access and use, 39–40
- Canberra premises, complaints concerning, 14
- complaints (non visa-related), 12, 14–15, 18, 79
- complaints (visa security assessment-related), 10–12, 19, 79
- cooperation with ASIS, 4, 5, 32
- Director-General of Security, 5, 22, 25, 26, 28, 30, 39
- employment related matters, 4, 18
- foreign intelligence collection warrants, 23
- foreign liaisons information exchange, 26
- human rights and discrimination matters, 18, 26
- information sharing, 28
- inspections of, 21–30, 38–40
- intelligence on Australian persons, 25–6, 32
- internal approval process project, 29
- investigations of issues-motivated groups, 27
- life insurance for staff, 38
- management of information on persons no longer relevant, 5
- new powers, 4, 5, 21, 22, 23, 24
- Preservation Notices (stored telecommunications data), 25
- procedural changes as a result of IGIS recommendations, 23, 28–9
- questioning and detention warrants, 23
- recordkeeping, 21, 27, 29–30
- reporting and notification requirements, 4, 6, 23
reporting/submissions to Attorney-General, 4, 23, 26, 28
'request for information' processes, 25–6
role and functions, 2, 4, 21
Special Intelligence Operations, 4, 24
taxation information access, 25
telecommunications data and interceptions, 6, 21–3, 24–5
use of force, 4, 23–4
warrant operations, 4, 5, 13, 21–4, 29

Australian Security Intelligence Organisation Act 1979, 2
amendments, 4–5, 21, 23
Attorney-General’s Guidelines, 2, 5, 21, 24–5, 29, 30
breaches of, 22
recordkeeping provisions, 29–30
s35P inquiry submission, 4

Australian Signals Directorate (ASD)
authorisations to collect intelligence, 5–6, 30–1, 35–7, 38
complaints, 12, 15, 79
inquiries relating to, 4, 10, 79
inspections of, 35–7
intelligence on Australian persons, 35–7
privacy rules, 31–2, 37
reporting and notification requirements, 6, 36
'request for information' processes, 25–6
role and functions, 3, 30
support for an ADF activity, 36
TIA Act compliance, 37

Australian Taxation Office (ATO), 25

Australian territory
AGO intelligence collection activities, 31, 38

Australians see Australian persons
authorisations to collect intelligence, 5–6, 30–7
average staffing level (OIGIS), 83

Aviation Security Identification Cards, 12, 15

B
Blight, Jake, 9, 42, 43
B-party warrants, 22–3

C
changes in agency procedures see procedural changes as a result of IGIS recommendations
coercive powers, 9
Commissioner of Taxation, 25
committees, 42
Commonwealth Disability Strategy, 46
Commonwealth Ombudsman, 14, 15, 17, 43
Commonwealth Risk Management Policy, 43
Compensation for Detriment Caused by Defective Administration, 14
complaints handling, 10–19
complaints handled administratively, 15, 18, 79
employment-related matters, 12, 15
human rights and discrimination matters, 18
non-visa related, 12, 14–15
numbers and trends, 10, 11
OIGIS engagement with other agencies, 9, 17
role of IGIS, 10
timeliness, 12, 14, 18–19
visa-related, 10–12
see also inquiries
consultants, 45
contact details, inside front cover
contract service providers to Dept of Defence
employment related matters, 15
contracts (OIGIS), 45

corporate and operational planning, 42

corporate governance, 42–3

Counter-Terrorism Legislation Amendment Act (No. 1) 2014, 5, 34

Counter-Terrorism Legislation Amendment (No. 1) Bill 2014, Inquiry into, 7

Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014, 5

Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014, Inquiry into, 6

court decisions, 19, 43

Crimes Act 1914, 39

cross-agency inspections, 38–40 see also inspections

D

Defence Imagery and Geospatial Organisation (DIGO) see Australian Geospatial-Intelligence Organisation (AGO)

Defence intelligence agencies, 3

Defence Intelligence Organisation (DIO)

complaints, 79

privacy guidelines compliance, 38

role, 3

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

deliverables (OIGIS), 8

Department of Defence

Senior Intelligence Managers’ Course, 9

service provider employment matters, 15

see also Minister for Defence

Department of Finance, 14

Department of Immigration and Border Protection, 11, 17, 26

Department of the Prime Minister and Cabinet, 1, 43, 46

detention warrants see questioning and detention warrants

Director-General of ASIS, 34, 39

Director-General of Security (ASIO), 5, 22, 25, 26, 28, 30, 39

disability reporting, 46

E

ecologically sustainable development, 46

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

efficiency dividend exemption, 3

emergency authorisations, 5–6, 31, 34, 36–7

employment (OIGIS), 3, 40, 43, 44–5

employment-related grievances within intelligence agencies, 12, 15

energy conservation, 46

engagement of IGIS with intelligence agencies, 9, 17, 33

enterprise agreements, 44–5

environmental performance, 46

ethical standards, 43

exchange of information see information sharing

exempt contracts, 45

expert evidence provision, 1

external scrutiny, 43

F

Fernandes and National Archives of Australia [2014] AATA 180 (2 April 2014), 19

financial intelligence information, 39

financial performance

agency resource statements, 82–3

summary, 40–1

financial statements, 47–77

firearms see weapons use and issues

force, use of, 4, 23–4
foreign agencies, exchange of information with, 26, 33, 34
foreign conflicts, Australians involved in, 5, 26, 28
foreign fighters legislation, 5
foreign intelligence collection warrants, 23
foreign liaisons, exchange of information with, 26, 33, 34
foreign relations interests, 30
fraud control, 43
freedom of information
IGIS role in FOI and Archives matters, 1, 19
OIGIS as exempt agency (FOI Act), 46
functions see roles and functions
funding, 3

G
geospatial intelligence agency see Australian Geospatial-Intelligence Organisation (AGO)
glossary, iv
Gyngell, Allan, 29

H
harassment allegations (intelligence agency), 16–17
highlights of year, 3–4
human resources management, 44–5 see also staff
human rights and discrimination matters, 18, 26
human source operations
ASIO, 6, 21
ASIS, 34

I
identified person warrants, 21–2
identities, assumed, 39
imagery intelligence see Defence Imagery and Geospatial Organisation (DIGO)
Immigration see Department of Immigration and Border Protection
immigration detention, persons in, 11, 26
Independent National Security Legislation Monitor, 7
Independent Reviewer of Adverse Security Assessments, 12, 26–7
Information Commissioner, 19, 43
Information Publication Scheme, 45
information sharing
with foreign liaisons, 26, 33, 34
Immigration/ASIO/ AFP , 2
inquiries
completed, 4, 10
employment of persons for a particular inquiry, 43
implementation of recommendations see procedural changes as a result of IGIS recommendations
inquiry function and powers, 1, 9–10
numbers and trends, 79
timeliness, 18
workload, 20
inquiries by parliamentary committees
parliamentary oversight of OIGIS, 43
submissions by IGIS, 6–7
inspections
agencies subject to ISA Act, 30–8
AGO activities, 37–8
ASD activities, 35–7
ASIO activities, 21–30, 38–40
ASIS activities, 32–5, 38–9, 40
AUSTRAC access and use, 39–40
cross-agency inspections, 38–40
DIO privacy guideline adherence, 38
forward plan, 42
ONA privacy guideline adherence, 38
overview of activities, 19–20
role of IGIS, 1, 19–20
Inspector-General of Intelligence and Security, 42
appointments, 1
briefings by, 6, 9, 20
reports on status of implementation of recommendations, 20
responsibilities under public interest disclosure scheme, 16
review of year, 3–4
role and functions, 1, 4–6, 19–20, 25
submissions to inquiries and reviews, 6–7
Inspector-General of Intelligence and Security Act 1986, 1, 9, 43
intelligence agencies, 2–4
ASIO requests for information relating to Australian persons, 25–6, 32
AUSTRAC information access and use, 39–40
complaints against agencies see complaints handling; inquiries
cross-agency inspections, 38–40 see also inspections
employment-related grievances, 12, 15, 18
financial intelligence information access, 39
IGIS engagement with, 9, 17, 33
inspection of, 4, 19–38
legislative changes, 3, 4–6, 21, 23
limits to functions, 30
new powers, 4–6
procedural changes as a result of IGIS recommendations, 19, 20, 23, 28–9
public interest disclosure scheme, 16–17
recordkeeping, 16
regular points of contact (officers), 9
reporting and notification requirements, 4, 5–6
roles and powers, 2–3, 4–6
training in weapons use and/or self-defence, 4, 23–4, 34–5
see also names of agencies
Intelligence Services Act 2001, 2, 4
agencies subject to ISA Act, 2 see also intelligence agencies
amendments, 4, 5
ASIS functions under s6, 40
breaches of, 33, 36
limits on intelligence agencies’ functions, 30
privacy rules, 31–2, 33
intelligence-related information, protection of, 4
internal audit, 44
International Intelligence Review Agency Conference, 9th, London 2014, 3
Internet home page, inside front cover
Iraq, 28
issues-motivated groups, 27
J
journalists’ sources, 6
judicial decisions, 19, 43
L
leadership groups addressed by Inspector-General, 9
legislation (enabling Act), 1
legislative changes, 3, 4–6, 21, 23
letter of transmittal, i
life insurance (ASIO and ASIS staff), 38
light cover, agency use of, 38
M
management and accountability (OIGIS), 42–6
Maritime Security Identification Cards, 12, 15
market research, 46
media strategies, 3
memoranda of understanding, 17, 25, 39
Minister for Defence, 3, 6, 35, 37
Minister for Foreign Affairs, 2, 20, 32, 33, 34, 39
ministerial and other authorisations to collect intelligence, 5–6, 30–7
ministers’ roles in respect of IGIS, 1
misconduct allegations and investigations, 14, 16–17

N
National Archives of Australia – ASIO Records Authority, 29
National Capital Authority, 14
National Disability Strategy, 46
national security, 3, 30 see also intelligence agencies
National Security – additional counter-terrorism funding measure, 3
National Security Committee of Cabinet, 30
National Security Legislation Amendment Act (No. 1) 2014, 3, 4–5, 21, 34
National Security Legislation Amendment Bill (No. 1) 2014, Inquiry by PJCIS, 5, 6, 23
nationality, presumption of, 31–2, 33, 37
non-salary benefits, 45
notifiable incidents (WHS), 46

O
offences, 4
Office of National Assessments (ONA) complaints, 79
privacy guidelines compliance, 38
role, 2
Ombudsman, 14, 15, 17, 43
operational files (ASIS), review of, 34
operational planning (OIGIS), 42
oral emergency authorisations, 5–6, 36–7
organisational structure, 42
outcome and program, 8
financial performance summary, 40–1
performance report, 8–41
resources for outcome, 82–3
outreach program, 9
overview by Inspector-General, 1–7

P
Parliamentary Joint Committee on Intelligence and Security, 1, 3
review of National Security Legislation Amendment Bill (No. 1) 2014, 5, 6, 23
submissions to, 6–7
parliamentary oversight of OIGIS, 6–7, 43
passport cancellation or suspension, 5, 28
people under 18 years of age, 21
performance indicators, 8
performance pay, 45
performance report, 8–41
personal security see protective security planning (OIGIS), 42
Portfolio Budget Statements, 8
portfolio relationship, 1
powers
IGIS, 1, 9–10
intelligence agencies, 2–3, 4–6
see also roles and functions
presentations and outreach, 9
Preservation Notices (stored telecommunications data), 25
presumption of nationality, 31–2, 33, 37
Prime Minister, 1, 2
prioritisation of work (OIGIS), risk-based approach, 20
privacy rules compliance, 31–2, 33, 37, 38
procedural changes as a result of IGIS recommendations, 19
   ASIO, 23, 28–9
   ASIS, 20
procurement, 45
program, 8
protective security, 42
Public Governance, Performance and Accountability Act 2013, 43
Public Interest Disclosure scheme, 16–17
Public Service Act 1999 section 24(1) determinations, 43, 45
purchasing, 45
Q
questioning and detention warrants, 23
R
recordkeeping, 16
   AGO, 38
   ASIO, 21, 27, 29–30
   ASIS, 34
recruitment, 3, 40
recycling, 46
remuneration
   APS employees, 80–1
   non-salary benefits, 45
   SES, 43, 80
‘request for information’ processes, 25–6
resources for outcome, 82–3
Review of Administration and Expenditure No. 13 (2014–15) Australian Intelligence Agencies, 7
risk management, 42, 43, 44
risk-based approach to prioritising work, 20
roles and functions
   intelligence agencies, 2–3, 30
   OIGIS, 1, 4–6, 19–20, 25
   S
Safeguarding Australia 2015 Conference, 9
salary ranges, 80–1
search warrants, 12, 13 see also warrant operations by ASIO
section 24(1) determinations, 43, 45
security
   clearances for OIGIS staff, 45
   definition in ASIO Act, 2, 5
   protective security, 42
   visa applicant checks see visa security assessment processes
self-defence training, 4, 23–4, 34–5
Senate Continuing Order No 10 (Harradine Order), 45
Senate Standing Committee on Finance and Public Administration, 6
senior executive, 42
Senior Executive Service (SES) officers, 43, 45, 80
senior management committees, 42
signals intelligence and information security authority see Australian Signals Directorate (ASD)
Special Intelligence Operations, 4, 24
staff
   average staffing level, 83
   employment of persons for a particular inquiry, 43
   non-salary benefits, 45
   recruitment, 3, 40
   remuneration, 43, 80–1
   staff numbers and profile, 44
   training and development, 3, 45
Stone, Margaret, 1
strategies, 8
structure (organisational), 42
study assistance, 45
submissions to inquiries and reviews, 6–7
Syria, 26, 28

T
Taxation Administration Act 1953 (TAA), 25
taxation information, 25
Telecommunications (Interception and Access) Act 1979 (TIA Act)
ASD compliance, 37
ASIO compliance, 21–2, 25
breaches of, 22
and recordkeeping, 29–30
Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015, 6, 24
Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, Inquiry into, 7
telecommunications data, 6, 24–5
telecommunications interception warrants, 21–3
tendering see purchasing
Thom, Vivienne, 1, 42 see also Inspector-General of Intelligence and Security
timeliness
ASIC and MSIC card delays, 15
complaints handling, 12, 14, 18–19
inquiries, 18
training and development (OIGIS), 3, 45
training in weapons use and/or self-defence, 4, 23–4, 34–5
transparency and public credibility, 3–4
trends
finances, 40–1
inquiries and complaints, 10, 12, 18–19
tribunal decisions, 43

V
visa cancellation, 5, 28
visa security assessment processes
adverse security assessments, review of, 12, 26–7
complaints handling, 10–12, 17, 18–19
complaints numbers and trends, 10, 11

W
warrant operations by ASIO, 4, 5, 13, 21–4, 29
weapons use and issues
ASIS management of weapons in a particular location, inquiry into, 10, 18, 20, 35
ASIS training in weapons use and self-defence, 4, 34–5
website address, *inside front cover*
welfare payments cancellation, 5, 28
whistleblower protection scheme see Public Interest Disclosure scheme
Work Health and Safety Act 2011, 46
work health and safety (OIGIS), 46
workload, 20
workplace bullying and harassment allegations (intelligence agency), 16–17

Y
year in review, 3–4
young people, 21