

ANNUAL REPORT 2011–12

THOUSAND AND TWELVE ■ NINETEEN EIGHTY SEVEN TO TWO THOUSAND AND TWELVE

25

NINETEEN E

ANNUAL REPORT

2011–12

THOUSAND AND TWELVE ■ NINETEEN EIGHTY SEVEN TO TWO THOUSAND AND TWELVE

25

IGIS Contact Information

LOCATION

One National Circuit
BARTON ACT 2600

WRITTEN INQUIRIES

Inspector-General of
Intelligence and Security
PO Box 6181
KINGSTON ACT 2604

PARLIAMENTARY AND MEDIA LIAISON

Ms Maryanne Gates
Phone: (02) 6271 5692
Fax: (02) 6271 5696

GENERAL INQUIRIES

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

INTERNET

Homepage:
www.igis.gov.au

Annual report:
www.igis.gov.au/annual_report/index.cfm

ISSN: 1030-4657

© Commonwealth of Australia 2012

This work is copyright. Apart from any use permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Attorney-General's Department, National Circuit, BARTON ACT 2600 or posted at www.ag.gov.au/cca.

Design and typesetting by Spectrum Graphics [sg.com.au]

Printed by New Millennium Print



www.igis.gov.au

2012/575

File Ref: 2012/24

The Hon Gary Gray AO MP
Minister for the Public Service and Integrity
Parliament House
CANBERRA ACT 2600

Dear Minister

I present herewith my annual report for the period between 1 July 2011 and 30 June 2012.

The report has been prepared in compliance with the *Requirements for Annual Reports* issued by the Department of the Prime Minister and Cabinet in June 2012.

The preparation of an annual report by this office is required by section 35 of the *Inspector-General of Intelligence and Security Act 1986*.

Each of the 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 the Parliament.

Yours sincerely

Vivienne Thom
Inspector-General

10 September 2012

Contents

Glossary	vi
PART ONE: OVERVIEW	1
The role of the Inspector-General of Intelligence and Security	1
The agencies of the Australian intelligence community	2
The year in review	3
Twenty five years of the Inspector-General of Intelligence and Security	5
Legislative changes	6
Privacy rules	7
Parliamentary oversight	7
PART TWO: PERFORMANCE	8
Outcomes and outputs	8
Performance indicators	8
Agency engagement	9
Inquiries	9
Effecting change in agencies	12
Complaints and contacts	15
Numbers and trends	18
Timeliness	18
Overview of inspection activities	18

Inspection activities specific to ASIO	22
Inspection activities specific to ASIS	25
Inspection activities specific to DSD	26
Inspection activities specific to DIGO	27
PART THREE: MANAGEMENT AND ACCOUNTABILITY	28
Corporate governance	28
External scrutiny	30
Management of human resources	31
Summary of financial performance and resources for outcomes	34
PART FOUR: FINANCIAL STATEMENTS	36
PART FIVE: ANNEXURES	72
Annex 1 Summary of inquiries and complaints	72
Annex 2 Salary ranges for APS employees in OIGIS in 2011-12	73
Annex 3 Agency resource statements	74
Annex 4 Inquiry into ASIO's security assessments for community detention determinations	76
Annex 5 DSA Inquiry	80
Annex 6 Habib Inquiry	83
Annex 7 Requirements for annual reports	88
Index	92

Glossary

AAT	Administrative Appeals Tribunal
AFP	Australian Federal Police
AGD	Attorney-General's Department
AGSVA	Australian Government Security Vetting Agency
AIC	Australian Intelligence Community
AML/CTF Act	<i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i>
ANAO	Australian National Audit Office
APS	Australian Public Service
APSC	Australian Public Service Commission
ASIO	Australian Security Intelligence Organisation
ASIO Act	<i>Australian Security Intelligence Organisation Act 1979</i>
ASIS	Australian Secret Intelligence Service
AUSTRAC	Australian Transaction Reports and Analysis Centre
DFAT	Department of Foreign Affairs and Trade
DIGO	Defence Imagery and Geospatial Organisation
DIAC	Department of Immigration and Citizenship
DIO	Defence Intelligence Organisation
DIR	data inquiry request
DSA	Defence Security Authority
DSD	Defence Signals Directorate
GST	goods and services tax
IGIS	Inspector-General of Intelligence and Security
IGIS Act	<i>Inspector-General of Intelligence and Security Act 1986</i>
IMA	irregular maritime arrival
ISA	<i>Intelligence Services Act 2001</i>
MA	ministerial authorisation
MOU	memorandum of understanding
OHS Act	<i>Occupational Health and Safety Act 1991</i>
OIGIS	Office of the Inspector-General of Intelligence and Security
ONA	Office of National Assessments
ONA Act	<i>Office of National Assessments Act 1977</i>
PM&C	Department of the Prime Minister and Cabinet
SES	Senior executive service
TIA Act	<i>Telecommunications (Interception and Access) Act 1979</i>
WHS Act	<i>Work Health and Safety Act 2011</i>

PART ONE: OVERVIEW

The role of the Inspector-General of Intelligence and Security

The Inspector-General of Intelligence and Security (IGIS) is an independent statutory office established by the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) which commenced on 1 February 1987. I was appointed as Inspector-General for a term of five years from 19 July 2010.

The Office of the IGIS (OIGIS) is situated within the Prime Minister's portfolio and reports to the Minister for the Public Service and Integrity for administrative purposes.

As an independent statutory office holder, the IGIS is not subject to general direction from the Prime Minister, the Minister for the Public Service and Integrity, 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 the oversight and review of the legality and propriety of the activities of the Australian Intelligence Community (AIC) agencies; 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.

The IGIS Act provides the legal basis for regular inspections of the AIC agencies so as to identify



*Dr Vivienne Thom,
Inspector-General*

issues, including about the governance and control frameworks within agencies, before there is a requirement for major remedial action.

The inspection role of the IGIS 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 also investigate complaints, including complaints by members of the public, about an action taken by an intelligence agency.

The role and functions of the IGIS are an important part of the overall accountability framework to which the AIC agencies are subject. While the focus of the IGIS is on the operational activities of the AIC agencies, the agencies are also subject to review by the Parliamentary Joint Committee on Intelligence and Security as well as the Australian National Audit Office.

The agencies of the Australian Intelligence Community

Australian Security Intelligence Organisation (ASIO)

ASIO's role is to collect and assess intelligence on threats to security, both in Australia and overseas, and to provide advice to protect Australia, its people and its interests.

ASIO's functions are set out in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). It 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 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, through authorised liaison relationships, and from published sources.

The Attorney-General is responsible for ASIO.

Australian Secret Intelligence Service (ASIS)

ASIS's primary function is to obtain and distribute intelligence information which is not readily available by other means, about the capabilities, intentions and activities of individuals or organisations outside Australia. Its functions are set out in the *Intelligence Services Act 2001* (ISA) and include communicating secret intelligence in accordance with government requirements, conducting counter-intelligence activities and liaising with foreign intelligence or security services.

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

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

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. Its sources for reporting are other intelligence and government agencies, diplomatic reporting and open sources including the media.

The ONA Act charges ONA with responsibility for coordinating and reviewing Australia's foreign intelligence activities and issues of common interest among Australia's foreign intelligence agencies. ONA is also responsible for evaluating the effectiveness of Australia's foreign intelligence effort and the adequacy of its resourcing.

The Prime Minister is responsible for ONA.

Defence intelligence agencies

Three of the six intelligence agencies which comprise the AIC are administered by the Department of Defence (Defence), namely, the Defence Intelligence Organisation (DIO), the Defence Imagery and Geospatial Organisation (DIGO) and the Defence Signals Directorate (DSD). These three agencies sit within the Intelligence and Security Group in Defence. DSD's and DIGO's functions 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)

The functions of DIO are to provide intelligence assessment and advice on the strategic posture, policy and intent and the military capabilities of countries relevant to Australia's security. It provides advice to the Government, the Australian Defence Force and senior Defence officials, policy makers and planners on weapons of mass destruction, military capabilities, defence economics and global military trends.

Defence Signals Directorate (DSD)

DSD is Australia's national authority for signals intelligence and for information security. DSD collects foreign signals intelligence and produces and disseminates reports based on the intelligence information it collects. These reports are provided to key policy makers and select government agencies with a clear and established need to know the information.

Defence Imagery and Geospatial Organisation (DIGO)

DIGO provides imagery and geospatial intelligence to support Australia's defence and national interests. It also provides a range of geospatial services (including mapping).

The Minister for Defence is responsible for these Defence agencies.

The year in review

Highlights

The Office of the Inspector-General of Intelligence and Security started the reporting period with two major inquiries underway, the Habib inquiry and the Defence Security Authority inquiry, each of which was conducted as a result of a request by the Prime Minister. Although both of these inquiries were completed by the end of 2011, the level of activity did not drop off as a further three inquiries commenced. All inquiries were finalised by the end of the reporting period.

A key performance indicator of the office is 'the extent to which there has been change within the agencies as a result of the activities of the office'.

The Habib inquiry resulted in significant changes to agency policies and the Defence Security Authority inquiry led to a substantial overhaul of the Australian Government Security Vetting Agency. In addition, a wide range of inspection activities and discussions with agencies have brought about smaller but still significant changes to agency policies and procedures.

Overall, I would assess that the staff in the AIC agencies are highly professional with a strong compliance culture. My office has a strong relationship with each office and I have found informal communication channels throughout the year have worked particularly well to alert me to any sensitive operational matters.

A review of the performance of the office including interviews with AIC agency heads concluded that 'the office has established trust and confidence in its capabilities, at the same time maintaining diligent exercise of its responsibilities'.

The significant level of inquiry activity placed pressures on resources: we needed to be flexible and continually prioritise our inspection and complaint-handling work. I am grateful to staff for demonstrating this flexibility and to agencies for accommodating our changing requirements.

Although the overall staffing level did not change, our increasing requirement for high-level legal advice resulted in the recruitment of an SES officer. Assistant Inspector-General, Mr Jake Blight, joined the office in January 2012.

Staff turnover has remained low. A staff survey was conducted for the first time in the office – overall the results showed a high level of staff satisfaction but indicated some areas for improvement.

A new function of the office has proved to be particularly challenging. My role in providing expert evidence to the Administrative Appeals Tribunal in Freedom of Information and Archives Act matters relating to national security used a significant amount of senior-level resources in the second half of the reporting period. This function will have to be managed carefully so as not to compromise the other work of the office.

25th anniversary

The highlight of the office's 25th anniversary celebration was a seminar *Balancing National Security and Individual Rights* hosted by the Institute of Public Administration of Australia on 28 March 2012. I spoke at the seminar together with Mr David Irvine, Director-General of Security, and Dr Rufus Black, theologian, ethicist and management consultant. The seminar was well-attended and was later broadcast on ABC television's *Big Ideas* program.



Dr Vivienne Thom with Dr Rufus Black and Mr David Irvine

International Intelligence Review Agency Conference

The 8th International Intelligence Review Agency Conference was held in Ottawa, Canada, in May 2012. Delegates from oversight bodies and parliamentarians from ten countries attended the conference. I spoke at the conference as did Mr Jake Blight, Assistant Inspector-General. Four members of the Parliamentary Joint Committee on Intelligence and Security also attended. The conference takes place every two years and is invaluable for sharing information about oversight and review activities.

Looking ahead

Although we have not carried over any significant inquiries into 2012-13, I expect the pace of work to remain high. Our budget is adequate but limited, so we need to ensure that we focus our efforts on areas of key risk in the agencies. In June 2012 we conducted a priorities-setting exercise to map out key inquiries and projects for the next twelve months: our challenge will be to manage this program, as well as remaining flexible enough to meet any emerging issues.

At the end of the reporting period the Attorney-General referred an inquiry into potential reforms of national security legislation to the Parliamentary Joint Committee on Intelligence and Security. The reform proposals are wide-ranging and, if accepted, could lead to extra responsibilities for this office to ensure that agencies continue to exercise their functions lawfully, with propriety and consistent with human rights.

Twenty five years of the Inspector-General of Intelligence and Security

The creation of the position of Inspector-General of Intelligence and Security was a recommendation of the second Hope Royal Commission in 1984 and reflected concerns that the intelligence and security agencies were not sufficiently under ministerial control, nor subject to enough scrutiny, and were being improperly caught up in domestic politics.

The Government of the day brought forward enabling legislation for the creation of an IGIS in May 1986 and the office was formally established on 1 February 1987.

In the second reading speech, the then Attorney-General, the Hon Lionel Bowen, briefly encapsulated the Government's vision for the office:

We believe that the legislation establishes an Office which will ... provide an independent oversight of the agencies' activities, give the public a greater assurance that those activities are proper ones, and clear the agencies, or bring them to task, as the case may be, if allegations of improper conduct are made against them.

As the functions and powers of the agencies have expanded since that time so has the role of the IGIS. In fact, almost any time there are changes suggested to the powers of intelligence and security agencies the office is called upon to provide the appropriate checks and balances demonstrating the value of the role:

- When ASIO's questioning and detention warrants were introduced in 2003 – perhaps the most controversial of new powers for ASIO in recent years – a legislated safeguard was that the IGIS can attend questioning sessions and any concern raised must be considered.
- In 2004 the legislative provisions relating to the use of weapons by ASIS staff required the IGIS to be given copies of their guidelines and to be notified by way of a written report if the weapon is discharged.

- In 2005, following the 2004 Flood Inquiry, the IGIS Act was amended to allow the IGIS to conduct periodic reviews of the statutory independence of the Office of National Assessment to provide assurance that they are free from political interference.
- When Freedom of Information conclusive certificates were abolished in 2009, the IGIS was given a new role in providing expert evidence to the AAT and Information Commissioner about national security exemptions.
- In 2010 the IGIS Act was amended again, to allow the IGIS, at the request of the Prime Minister, to inquire into an intelligence or security matter relating to any Commonwealth agency reflecting the value of oversight over the broader intelligence community.

In his second reading speech Mr Bowen also said that '... the maintenance of trust and good communications between all parties will be essential to the effective operation of the Office of the Inspector-General'. In the 25 years since, the office has grown from an embryonic body with an untested mandate that was viewed with some suspicion by the intelligence community into an agency which, through a sound record of achievement over many years, now enjoys the trust of current and former Ministers of all political persuasions, and the respect and cooperation of the six intelligence agencies.

The success of the office rests entirely on its reputation, credibility and ability to influence. It is therefore appropriate to acknowledge the former Inspectors-General for their excellent stewardship of the office:

Mr Neil McInnes AM (February 1987 – September 1989)
 Mr Roger Holdich AM (September 1989 – April 1995)
 Mr Ron McLeod AM (April 1995 – February 1998)
 Mr Bill Blick PSM AM (February 1998 – March 2004)
 Mr Ian Carnell AM (March 2004 – April 2010).

It is also appropriate to acknowledge and thank the dedicated and professional current and former staff of the office.

Legislative Changes

Inspector-General of Intelligence and Security Amendment Act 2011

The *Inspector-General of Intelligence and Security Amendment Act 2011* commenced on 15 October 2011. The Act made a number of changes to the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) including:

- updating the objectives section to expressly recognise the role of the IGIS in assisting the government to provide assurances about the legality and propriety of AIC activities to the Parliament and the public
- providing the IGIS with a capability to undertake own-motion preliminary inquiries
- allowing the IGIS to undertake own-motion inquiries into the effectiveness and appropriateness of the procedures of all AIC agencies (previously allowed in relation to ASIO, ONA and DIO but not ASIS, DIGO or DSD)
- providing a capacity for the IGIS to delegate the powers of the Office, subject to Ministerial approval
- enabling the IGIS to provide information to any prescribed Royal Commission
- ensuring that the Prime Minister can be provided with a copy of the final report of any inquiry conducted by IGIS
- updating and modernising a number of provisions, without changing their application.

Intelligence Services Legislation Amendment Act 2011

The *Intelligence Services Legislation Amendment Act 2011* commenced on 26 July 2011. The Act amended the ASIO Act so that:

- the definition of 'foreign intelligence' is consistent with the way the term is used in the *Intelligence Services Act 2001* (ISA) and the *Telecommunications (Interception and Access) Act 1979* (TIA Act)

- the conditions for the Attorney-General to authorise foreign intelligence collection are consistent with the ISA in that the Attorney must be satisfied, on the basis of advice received from the relevant Minister, that the collection of foreign intelligence relating to the matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being
- ASIO can provide a security assessment in relation to the engagement of a person as a staff member within the AIC without enlivening an employee or prospective employee's appeal rights in the Administrative Appeals Tribunal
- computer access warrants allow access to data held in a computer at any time while the warrant is in force.

The Act also made some changes to the ISA including:

- clarifying that privacy rules made under s. 15 of the ISA, in relation to DSD, DIGO and ASIS, are not legislative instruments
- adding an additional ground for obtaining ministerial authorisations to collect intelligence about an Australian person who is, or is likely to be, involved in activities related to a contravention, or an alleged contravention, of a United Nations sanction enforcement law (as defined in the *Charter of the United Nations Act 1945*)
- clarifying the DIGO function of assisting the Australian Defence Force
- inserting a new provision to clarify that the immunity in s. 14 of the ISA is intended to have effect unless another law expressly overrides it.

Privacy Rules

Section 15 of the ISA requires that the relevant Ministers make rules for ASIS, DSD and DIGO regulating the communication and retention of intelligence information concerning Australian persons. Before changing those rules the ISA relevantly requires that the Minister consult with the IGIS. I was consulted on proposed changes for the rules relating to ASIS, DSD and DIGO during 2011-12. If the relevant Ministers decide to make new rules in the coming year I will provide advice on the effect of those changes to the Parliamentary Joint Committee on Intelligence and Security as required by the ISA.

Parliamentary oversight

On 22 November 2011 I appeared before the Joint Select Committee on Australia's Immigration Detention Network inquiry.

On 31 January 2012 I made a submission to the Parliamentary Joint Committee on Intelligence and Security to the *Review of Expenditure No. 10 (2010-11) – Australian Intelligence Agencies*.

I appeared before the Senate Standing Committee on Finance and Public Administration on 13 February 2012 during the 2011-12 Additional Budget Estimates hearings, and on 22 May 2012 during the 2012-13 Budget Estimates hearings.



PART TWO: PERFORMANCE

Outcomes and outputs

In 2011-12 the Office of the Inspector-General of Intelligence and Security (OIGIS) had one specified outcome for program budgeting purposes.

That outcome was to:

provide 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 strategies employed to achieve this outcome were for OIGIS to:

- continue inspection work to monitor and review the activities of the AIC agencies
- respond to requests from Ministers to conduct inquiries and, where appropriate, initiate inquiries and investigate complaints about the activities of the AIC agencies.

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

The average staffing level of OIGIS, excluding the IGIS, remained at thirteen in 2011-12.

Performance indicators

The effectiveness of the office is assessed against several key performance indicators. The following measures take into account the unique role and functions of the OIGIS as a specialised review body for the six agencies that comprise the AIC:

- the breadth and depth of inspection work undertaken
- the timeliness of completion of inquiries and 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.

Evaluation of performance

In early 2012 I engaged the services of a consultant, Ms Meryl Stanton, to undertake an evaluation of the performance of OIGIS. Ms Stanton conducted this review using structured interviews with the heads of AIC agencies as well as with the Secretary of the Department of the Prime Minister and Cabinet and the National Security Adviser.

Ms Stanton assessed our performance against our key performance indicators as well as against customer-focussed regulatory criteria.

Overall it was found that we not only meet our formal performance criteria, but achieve good practice in terms of those principles which should guide regulators and similar bodies. Her report concludes that 'the office has established trust and confidence in its capabilities, at the same time maintaining diligent exercise of its responsibilities'.

The report also notes a number of challenges for the office in the future as the security agencies work more closely together and notes that 'the office will require carefully targeted strategies, based on an intelligence-led approach to risk management, in order to fulfil its responsibilities with the same efficiency and effectiveness found by this evaluation'.

The results of this review informed planning for 2012-13 to ensure that resources are allocated appropriately to monitoring the higher-risk activities of the AIC agencies.

Agency engagement

I meet regularly with AIC agency heads and their senior staff to discuss current issues or concerns, and to highlight issues arising from our inspection activities. These discussions are typically used by the agencies to brief me on emerging trends or potential concerns and how they plan to respond to these challenges.

These discussions provide me with good awareness of the operational environment of each AIC agency and also provide a forum to resolve issues informally where appropriate without the need for extended, time consuming or unnecessary correspondence.

Each agency has also identified regular points of contact to facilitate our visits and to coordinate our various requirements, while, within OIGIS, we have designated lead officers to handle interactions

with each AIC agency. The designation of these coordination points does not limit my capacity to speak to whoever I need to, and indeed goes a long way to ensuring that our requirements are met in a full and prompt manner. I would like to express my appreciation to our regular points of contact for assisting the work of this office during the 2011-12 reporting period.

During the reporting period my staff and I delivered several presentations to staff in AIC agencies. These presentations provide a good opportunity to explain the role and functions of our office and our expectations of agency staff on matters of professionalism and ethical conduct. My staff also attended courses run by AIC agencies.

I regularly meet with ASIS heads of station before they are posted to remind them of the functions of the office and explore any particular challenges they anticipate depending upon the particular locations and operations at their post. I have recently started to meet with ASIO officers prior to their overseas postings as well.

Inquiries

Preliminary inquiries provide an avenue to write to an AIC agency head in order to formally raise a matter of concern and request relevant information. Preliminary inquiries assist in resolving:

- whether a particular matter is within jurisdiction
- whether the agency can demonstrate that it acted lawfully and properly in respect of the matter raised or, if the concern was substantiated, whether the agency has already taken remedial action
- whether sufficient issues of concern remain to justify a more comprehensive inquiry.

Full inquiries can arise from complaint matters, of my own motion, or in response to a ministerial referral. During such inquiries the IGIS Act provides for the use of strong coercive powers, immunities and protections. These powers include the power to compulsorily obtain information and documents, to enter premises occupied or used by a Commonwealth agency, to issue notices to persons to attend before me to answer questions relevant to the matter under inquiry, and to administer an oath or affirmation when taking such evidence.

In instances when I use these coercive powers, the IGIS Act provides protections to a person who has given me information. That is, the person will not be subject to any penalty under the provision of any law of the Commonwealth or a Territory by reason only of giving information to me or answering a question put by me, where I have required them to do so.

An agency's responsible Minister is advised when I commence a full inquiry and is also advised of any conclusions or recommendations that I may make at the completion of the inquiry. I also provide opportunities for Ministers and agency heads to comment during the course of an inquiry.

Full inquiries

At the conclusion of the 2010-11 reporting period, two full inquiries remained open and were carried into 2011-12. The first concerned the actions of certain Australian government agencies in relation to the arrest and detention overseas of Mr Mamdouh Habib from 2001 to 2005 (Habib inquiry). The other was into allegations of inappropriate vetting practices in the Defence Security Authority (DSA Inquiry). I conducted these inquiries at the request of the Prime Minister, and concluded both in December 2011.

Inquiry into allegations of inappropriate vetting practices in the Defence Security Authority and related matters

On 29 May 2011, the Prime Minister requested that I conduct an inquiry into allegations of inappropriate vetting practices in the Defence Security Authority (DSA). The inquiry was finalised on 23 December 2011 and the executive summary and recommendations can be found at Annex Five.

The inquiry was notable for being the second referred by the Prime Minister into a non-AIC agency under newly-introduced provisions of the IGIS Act and for demonstrating the impact that disclosure of poor administration can have on organisational reform.

The power of the IGIS to inquire beyond the six AIC agencies at the request of the Prime Minister was introduced in November 2010 and at the time was anticipated to be required sparingly. In the six months following its introduction, the Prime Minister referred two inquiries under the provision, the other being the Habib inquiry (Annex Six).

The referrals underscore the importance of the new provision and the unique and important role of the office in providing independent assurance to Government on matters that cannot normally be aired in public due to security reasons.

The fact the complainants felt their only recourse was to take their concerns to the media emphasises the need for management to appropriately address the concerns of current and former employees in a timely manner and for organisations to create and promote effective mechanisms for dealing with internal disclosures.

Once the complainants' concerns had been publicly aired, the role of an independent review body that could provide appropriate protections became important. The complainants' cooperation with any inquiry was contingent on assurances that their participation would not invite any legal sanctions. The protections provided under the IGIS Act provided the complainants those assurances.

While it is unfortunate that the inaction of the Department of Defence led the three complainants to take their concerns to the media, the subsequent reforms introduced to vetting practices in the DSA following the inquiry demonstrate the valuable role that disclosures can have in exposing poor administration in government agencies.

DSA has advised me that at 30 June 2012, four of the thirteen recommendations have been fully implemented and work continues on the remaining nine. DSA expects that all remediation activities will be finalised by the end of 2013.

During 2011-12, I commenced three full inquiries. One of these concerned ASIO, one ASIS, and the third concerned the Defence intelligence agencies – DSD, DIO and DIGO. These comprised:

- an inquiry into the process by which ASIO conducts security assessments to provide advice to the Minister for Immigration and Citizenship for a
- decision about eligibility for community detention
- an inquiry into ASIS recruitment and vetting practices arising from a complaint by an individual who was unsuccessful in a recruitment process
- an inquiry into Defence intelligence agencies' management of personnel security risk.

Community detention security assessment inquiry

In late 2011 I commenced an inquiry into the process by which ASIO conducts security assessments which are used by the Minister for Immigration and Citizenship when deciding whether an individual is eligible to be transferred to a community detention arrangement.

The number of requests for these assessments has increased rapidly since a new approach to community detention was adopted in 2010. The outcome of such an assessment has a profound effect on a detainee: under Government policy an adverse recommendation means that a person cannot be transferred to a community detention arrangement and must remain in an immigration detention centre.

I finalised the report and provided it to the Attorney-General in late June 2012. An unclassified abridgement of the final report is at Annex Four.

Concerns about coordination and information-flow between DIAC and ASIO arose in several of the cases examined. I recommended that in cases where ASIO issues an adverse security assessment for community detention but where DIAC has identified significant health, welfare or other exceptional issues, ASIO should engage in a dialogue with DIAC so the Minister for Immigration and Citizenship can be advised on possible risk mitigation strategies and conditions with which a person allowed community detention might be required to comply.

While ASIO has not formally accepted this recommendation, the Acting Director-General indicated that they were 'open to dialogue with DIAC should the department wish to pursue this proposal with us'.

I made two further recommendations in respect of record-keeping and training which have been accepted by ASIO.

Publication of inquiry reports

At the end of the reporting period, all five full inquiries had been finalised and I had provided reports to the relevant Ministers and agency heads. Inquiries into the Australian intelligence community often deal with very sensitive information in terms of national security and this affects what can be published. Longstanding practice is that the relevant Minister decides what is released into the public domain and the timing of any release.

In general I think that it is important for the reports of inquiries conducted by oversight agencies to be made public wherever possible:

- it is important for the accountability and transparency of government that where there is a strong public interest in an inquiry the findings are made public
- the credibility of oversight bodies including the IGIS depends upon public reporting
- there are often lessons for public administration that arise out of administrative inquiries that can apply in a more general way to government agencies.

The Prime Minister agreed to the release of my full report on the DSA Inquiry, and an abridged version of my report on the Habib Inquiry. Sections of these reports containing my executive summaries, findings and recommendations can be found at Annex 5 and Annex 6. All inquiry reports that have been publicly released since the commencement of this office can be read online at www.igis.gov.au/inquiries.

Personnel security risk management inquiry

In late 2011, at the request of the Minister for Defence, I commenced an inquiry into the mechanisms and processes for managing risk in the Defence intelligence agencies in circumstances where a staff member is identified as being an actual or potential security concern. The Minister also requested me to compare the activities of the Defence intelligence agencies with the mechanisms and processes being used by the other agencies of the Australian intelligence community.

I completed the inquiry and provided the report to the Minister for Defence and the relevant agency heads in June 2012. I found overall that the systems which operate across the AIC for managing staff risk meet the minimum mandatory requirements of the Australian Government Protective Security Policy Framework. By examining policies and processes across the AIC as well as actual case studies, I identified better practice principles which, if adopted, would serve to strengthen existing arrangements within and across the AIC agencies. I also made a number of recommendations in respect of Defence intelligence agencies. The inquiry report is classified because it contains sensitive material about protective security.

Although ASIO, ASIS and ONA were not within the scope of the inquiry, I provided these agencies with a copy of the full report and letters setting out my views on their compliance with the better practice principles articulated in my report.

Effecting change in agencies

In those inquiries where I made recommendations, I also sought a response indicating whether they were accepted, and if so, advice of their implementation. I am pleased with the agencies'

high level of acceptance and implementation of my recommendations. The sections on the Habib inquiry on page 13 and the ASIS recruitment and vetting inquiry on page 14 demonstrate how recommendations can lead to agency improvements on sensitive matters such as the passage of information to foreign authorities, and recruitment.

Inquiry into the actions of Australian government agencies in relation to the arrest and detention overseas of Mr Mamdouh Habib from 2001 to 2005

In January 2011, at the request of the Prime Minister, I initiated an inquiry into the actions of relevant Australian government agencies in relation to the arrest and detention overseas of Mr Mamdouh Habib from 2001 to 2005. I provided the inquiry report to the Prime Minister on 19 December 2011. Given the highly classified nature of the report, its distribution was strictly limited, however the Prime Minister agreed to release an abridged version of the report which was made public on 23 March 2012 and is available at www.igis.gov.au. The full text of my key findings and recommendations from the abridged report can be found at Annex Six.

Recommendation 1 proposed that government agencies prepare an apology to Mrs Maha Habib for failing to keep her properly informed of Mr Habib's welfare and circumstances. This recommendation was not accepted by Government.

The Government did accept the remaining five recommendations which related to consular responsibilities, the passage of information to foreign authorities, and policies relating to the prohibition on the use of, or involvement in, torture or other cruel, inhuman or degrading treatment. At the end of this reporting period, I sought an update from ASIO, DFAT and the AFP to assess progress of implementation of these recommendations.

The revisions made by DFAT to its *Consular Handbook (Operations), Arrest, Detention and Imprisonment* take into account the findings relevant to DFAT in the inquiry, and fully implement recommendation 2. The Secretary of DFAT has written to the heads of ASIO, ASIS, AFP, Defence, DIAC, Austrade and AGD alerting them to DFAT's updated policy, including its mandatory procedures for Australian government officials visiting Australians detained overseas.

In response to recommendations 3 and 5, ASIO has made several changes to existing internal policies and procedures in relation to custodial interviewing overseas and in the management of their communications with foreign liaison organisations. These changes reflect a strengthening of ASIO's risk management strategies aimed at ensuring that considerations of legality and propriety are taken into account at each step of the process and appropriately documented. I consider ASIO to have fully implemented my recommendations.

The AFP has recently developed a new *AFP National Guideline on offshore situations involving potential torture or cruel, inhuman or degrading treatment or punishment*. The guideline codifies the AFP's policy position on AFP officers' involvement in the custodial interviewing of certain persons detained overseas, and sets out the procedures and reporting requirements in circumstances where the AFP is considering passing information concerning an Australian to a foreign authority, or becomes aware an Australian detained offshore has been or is likely to be subject to inappropriate treatment. The AFP has advised that the guideline will be promulgated widely across the agency.

Inquiry into ASIS recruitment and vetting practices

An individual complained that the recruitment and security vetting process of ASIS did not meet relevant standards. The complainant also alleged that they were not afforded procedural fairness, that they had been provided with incorrect information and subjected to inappropriate questioning during the process.

While ASIS is not subject to the recruitment standards which apply to the general Australian Public Service, the agency endeavours to adhere to those standards insofar as its unique security environment allows.

In the course of the inquiry I interviewed several officers, under oath or affirmation, about the actions they had taken in relation to the matters raised by the complainant.

I determined that the agency's normal business practices were sound, but parts of this recruitment action had not been carried out properly and had caused the complainant considerable inconvenience. However, I found that the applicant had not been denied appropriate procedural fairness and that the questioning was not inappropriate.

At the conclusion of my inquiry I made a number of recommendations about policies, procedures and training for staff involved in the agency's recruitment activities, including changes to referral programmes, improved communication between various recruitment teams and establishing firm guidelines for interactions between recruitment teams and employment candidates. These recommendations have been accepted by ASIS and improvements have been made to its policies and procedures.

I also recommended that the agency apologise to the complainant for the inconvenience caused in this instance. ASIS has since sent a letter of apology to the applicant.

Finally, I recommended that ASIS reconsider the extent to which the agency could provide limited feedback to those candidates who, having proceeded through interview to the vetting process, are then found to be unsuitable. ASIS has informed me that they have considered the recommendation, and determined that the agency will only provide feedback to candidates progressing beyond interview in exceptional cases. I will continue to monitor this.

Preliminary inquiries

I commenced four preliminary inquiries into matters raised in complaints. These comprised:

- an ASIS recruitment and vetting practices matter. I closed this preliminary inquiry after deciding that the matter could be more appropriately considered under the powers and protections of a full inquiry.
- a request for a review of internal administrative decisions taken by ASIO prior to the termination of the complainant's employment. I closed this preliminary inquiry when I concluded that ASIO's processes and decisions were not inappropriate in the circumstances.
- a request for a review of ASIO's internal handling of a complaint matter. I closed this preliminary inquiry when I concluded that ASIO's processes were not inappropriate and the conclusions were not unreasonable. The case highlighted concerns about the timeliness of ASIO's internal investigations. Following discussions with ASIO on options for improving the timeliness of internal investigations, ASIO has advised they are making several changes to their internal policies and practices to address this aspect of the issues raised in the complaint.
- an allegation of improper conduct by ASIO officers towards an individual who was subject of a visa security assessment.

Preliminary inquiry into ASIO's management of a visa security assessment case

An off-shore unsuccessful visa applicant complained about ASIO's treatment of him over several years. He claimed that after receiving an adverse security assessment, he participated in a number of ASIO intelligence collection interviews on the understanding that ASIO would review the adverse assessment. He believed that ASIO took advantage of his willingness to disclose information as ultimately, his security assessment did not change.

I conducted an extensive review of files relating to ASIO's management of the case and concluded there were no issues of concern relating to the legality of ASIO's conduct. However, based on ASIO's records, I concluded that ASIO was aware at the time that the complainant had misinterpreted the purpose and likely outcome of his interaction with ASIO, and that ASIO did not correct the complainant's understanding during discussions when there was a clear opportunity to do so.

In response to my views, ASIO accepted that it may not have managed the complainant's expectations effectively, but did not agree that ASIO officers contributed to his misunderstanding. ASIO has committed to putting in place appropriate measures to manage risks where it is communicating with persons who may have an expectation of a particular outcome occurring as a result of their engagement with ASIO. I will continue to monitor ASIO's management of similar cases.

Employment related matters

Three of the four preliminary inquiries listed above commenced following concerns raised by current and prospective AIC employees. Sections 8(5) and 8(7) of the IGIS Act limit the capacity of the IGIS to investigate what might be regarded as individual employment-related grievances within the six AIC agencies – essentially those relating to promotion, transfer or reduction, termination, discipline, remuneration or other terms and conditions of service.

When a complaint to the office relates to this type of grievance, our general practice is to refer the matter (at least in the first instance) back to the agency concerned to be addressed through its internal grievance mechanisms or through procedures for reporting alleged breaches of the relevant Code of Conduct (where this is applicable).

The Code of Conduct provisions under the *Public Service Act 1999* apply to employees of DIGO, DIO, DSD and ONA, while similar arrangements are separately established by determinations made under the ASIO Act and the ISA for employees of ASIO and ASIS respectively.

The IGIS does have some flexibility in regard to situations where the complainant has exhausted avenues of internal redress and there are related policy or procedural matters that I can usefully pursue, or where a complainant is a prospective or

former employee rather than a current employee. This flexibility is particularly important to former employees because their ongoing secrecy obligations usually mean that they cannot approach any other complaint handling body.

Complaints and contacts

The complaints functions of my office are set out in ss. 10 to 14 of the IGIS Act. Complaints can be made orally or in writing, on matters that relate to the functions laid down in s. 8 of the IGIS Act. Broadly speaking, complaints are limited to matters that relate to the activities of AIC agencies.

Each contact made to my office is assessed to determine whether it falls within the functions of my 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.

Matters handled administratively

An administrative inquiry is the most efficient means of handling straightforward concerns. It reduces the procedural burden of a preliminary or full inquiry when a simple discussion with an agency can resolve the matter. An administrative inquiry can provide information that helps decide whether to pursue more formal inquiries into a complaint, and

generally allows for a timely response to be provided to the complainant.

When it is clear that a complaint has raised complex issues or serious concerns, I may decide to escalate the matter from the outset by initiating a preliminary or full inquiry under the IGIS Act.

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

Matters raised with my office during 2011-2012 were grouped within three broad categories:

- security assessments for visa applicants
- credible allegations of illegality or impropriety within the AIC
- matters falling outside the functions of my office or lacking credibility.

Complaints relating to visa security assessments

We do not assess the merits of any particular security assessment. Nor do we 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, I examine ASIO's processes.

In the reporting period we received 430 complaints about visa security assessment cases, most concerned with delays. Where the application was made more than 12 months previously, we made administrative inquiries of ASIO as to whether or not they had been asked to undertake security assessments, and if so, details of 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 that they have or have not been the subject of a security assessment by ASIO, unless this has already been confirmed to them by an external agency, or we found a significant issue of concern involving ASIO which would justify this office doing so. Where I am satisfied that there is no evidence of error by ASIO, we advise complainants to seek an update on the progress of their case from the Department of Immigration and Citizenship (DIAC), the agency with overall responsibility for the administration of

applications for Australian visas. Where we do find an error for which it is responsible, we suggest ASIO rectify the matter, as seen in the following case study.

Administrative delays in visa security assessments

An individual complained about excessive delay in the processing of a visa application. We contacted ASIO and ascertained that a handling error resulted in the visa security assessment referral being inadvertently cancelled.

As a result of our inquiry, ASIO finalised the security assessment and referred the results to DIAC for completion of the visa application processing.

ASIO also agreed to our request that it send a formal letter of apology to the complainant.

In respect of ASIO's security assessments for visa applicants, the work of this office complements the work of the Commonwealth Ombudsman who has jurisdiction to investigate matters relating to DIAC. I was pleased that in August 2011 Mr David Irvine, Director-General of Security, and senior ASIO staff, offered to give me a joint briefing with Mr Allan Asher, then Commonwealth Ombudsman. The comprehensive briefing covered the process by which DIAC refers requests for security assessments to ASIO as well as sensitive information about the conduct of the assessments and the challenges faced by ASIO.

While the incidence of error which we have identified in visa security assessments in the reporting period has been low, any undue delay in ASIO's completion of security assessments is of serious concern.

An individual who was referred to me by the Commonwealth Ombudsman complained about delays in his visa security assessment. We made inquiries of ASIO and determined that this case was one which pre-dated the DIAC-ASIO electronic referral system that was introduced in 2009. In its search for information about this case, ASIO identified a number of other incomplete security assessments from the same period. ASIO has taken steps to finalise these cases and I will seek regular feedback to ensure they are not subject to further delays.

In April 2012 ASIO staff informed me that they had found 43 referrals for visa security assessments that DIAC sent to an incorrect ASIO electronic mailbox. Five of these referrals were more than twelve months old. ASIO immediately took action to prioritise these cases and implement technical and procedural changes to minimise the risk of recurrence. I will continue to monitor the progress of these cases to ensure there are no further delays.

Last year I flagged my intention to conduct regular inspections of ASIO's case management and quality control processes in order to identify any underlying systemic issues requiring attention. I delayed this work because of the announcement by the Australian National Audit Office (ANAO) of an audit of ASIO's security assessment processes. I did commence a full inquiry into ASIO's community detention security assessments. Details of this inquiry can be found in the 'Inquiries' section of this chapter, and in Annex 4.

Credible allegations of illegality or impropriety

An approach from a member of the public was registered as a complaint if it involved a credible allegation about illegality or impropriety by a member of the AIC. That is, there was a reasonable basis for the person believing that an intelligence agency or one of its employees had done something wrong.

I received twelve complaints alleging illegality or impropriety in the actions of AIC agencies. Eight of these complaints were handled administratively.

Four complaints to my office led to preliminary inquiries, and one of these led me to conduct a full inquiry. This compares to five preliminary inquiries arising from complaints in 2010-11 and twelve in 2009-10. Details of this year's inquiries can be found in this chapter under 'Inquiries'.

Other contacts with the office

My office generally receives several calls each day requesting information or assistance about visa matters that we do not follow up further. These include calls relating to matters that we have already considered, matters that are outside jurisdiction, and concerns about security assessments where the visa application was lodged less than 12 months previously. The office provides general information to the caller and, where appropriate, suggests they contact DIAC.

In addition, my office was contacted more than three hundred times – via telephone, email, online complaint form, letter and fax – by 125 individuals who were seeking advice or expressing concern about matters affecting them that were assessed to be outside the jurisdiction of my office or as lacking credibility.

We provided information by telephone to 59 of the 125 individuals, and wrote to 58. Twenty-three were redirected elsewhere, including to other complaint-handling bodies, the police or the National Security Hotline. In cases where there had been previous contact with my office about matters that had already been assessed, or where insufficient contact details were provided, my office took no further action.

The right to legal representation at an ASIO interview

A state legal aid commission complained that its client was denied the right to legal representation during an ASIO visa security assessment interview.

After making inquiries, we established that ASIO had believed the representative to be a migration agent, rather than a solicitor. This misunderstanding by the ASIO interviewing officers meant the client was denied the presence of a legal representative and ASIO terminated the interview.

As many individuals representing visa applicants are both solicitors and migration agents, this complaint highlights ASIO's responsibility to clarify the role of any support person, particularly where there is some doubt.

Statistics on matters raised with my office can be found at Annex 1 – Summary of inquiries and complaints.

Numbers and trends

Overall, the total number of matters raised with the office reduced during 2011-2012. While we continued to receive a number of complaints about visa security assessments in the first six months of the 2011-12 period, there was a noticeable decrease in the number of complaints in the second half of the reporting period. In particular, complaints about visa security assessments fell by approximately sixty per cent from 1111 in 2010-11 to 430 in 2011-12.

This decline in complaints about visa security assessments may be due to a number of factors. In October 2010 the Federal Government announced it would be allowing greater access to community detention for certain groups of vulnerable irregular maritime arrivals (IMAs). Since that announcement, changes to government policy have resulted in a substantial increase in the number of individuals being eligible for community detention. Additionally, changes within ASIO and the introduction of a triaging system in the previous financial year have enabled ASIO to reduce the number of outstanding IMA security assessments.

Of the remaining complaints handled administratively, those raising credible allegations of illegality or impropriety in the AIC increased from four in 2010-11 to nine in 2011-12. Three of these were employment issues raised by current, former and prospective employees.

The number of inquiries actioned in 2011-12 stayed roughly constant at nine (compared to eight in 2010-11). Full inquiries increased from three to five, while preliminary inquiries decreased from five in 2010-11 to four in the reporting period.

Overall the decrease in workload due to the decrease in complaint numbers was more than offset by the increase in inquiry workload.

Timeliness

All complaints to the office were assessed promptly and decisions about any action required were made

within two weeks of receipt. Most administrative inquiries were completed within two weeks of the complaint being received.

Nine inquiries were completed during the year. The complexity of the subject matter and the individual circumstances of each inquiry were factors affecting timeliness, which ranged from 16 days for a sensitive personnel matter to 349 days for an inquiry into the actions of ten agencies over a number of years.

Overview of inspection activities

The office conducts inspection activities by examining selected agency records to ensure that the activities of the AIC agencies comply with the relevant legislative and policy frameworks and to identify issues before there is a need for major remedial action. An outline of the functions of the AIC agencies and their legislative frameworks is set out on page 2.

ASIO, ASIS, DSD and DIGO each have access to intrusive powers and investigative techniques which can only be used when specifically approved by their responsible Minister.

ASIO can access a range of telecommunications interception capabilities and special powers following the issue of warrants for these purposes by the Attorney-General. The authority for these warrants derives from the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Telecommunication (Interception and Access) Act 1979* (TIA).

The use of particularly intrusive intelligence collection techniques by Australia's foreign intelligence collection agencies (the ISA agencies) is subject to specific ministerial authorisation (MA) by the Minister for Foreign Affairs (for ASIS) and the Minister for Defence (DSD and DIGO). In DIGO's case, any intelligence collected over Australian territory requires authorisation by the head of the agency. The use of these powers is approved at senior levels because their use is sensitive and they may be used on Australian persons, and in activities which could expose Australia's national interests to significant levels of risk. Overall, we found that the agencies had provided sufficient information for the responsible Ministers to make their decisions.

ASIO warrants

During the 2011-12 reporting period we reviewed all of ASIO's warrant operations. We normally review these warrants and authorisations following their revocation or expiry. This retrospective focus is appropriate, as it is not the role of the IGIS to direct or manage the use of these special powers and investigative techniques.

During 2011-12 we noted a relatively small number of cases where errors had occurred either by ASIO or by the relevant telecommunications carrier, in the execution of ASIO warrants. Most of these errors occurred with respect to telecommunications interception warrants (which especially rely on the use of precise and up to date information). Errors of this kind included:

- the inclusion of already disconnected services in warrant renewal requests put to the Attorney-General (which poses the risk that interception might occur if the number is reallocated during the period the warrant is active)
- the provision of an incorrect expiry date in advice to a telecommunications carrier in relation to a supplementary warrant (meaning that coverage was maintained on this service for several days beyond the period actually authorised by the warrant)
- clerical mistakes such as the transposition of digits, letters or symbols when identifying which services are to be intercepted (meaning that the services of persons with very similar phone numbers or email addresses but with no connection to a security related matter could be intercepted)
- technical or software problems leading to the incorrect delivery of intercepted product.

In all of the above instances, we either noted the detailed explanations provided on file, or asked for additional information on what went wrong and how the error had been fixed. In several cases we also sought detailed face to face briefings in order to obtain a deeper understanding of the issues. I was satisfied in each case that prompt and appropriate remedial action was taken.

During the reporting period we noted several instances where collection under a telecommunications interception warrant had been switched off because there had been a change to the grounds upon which the warrant had been issued but the warrant itself had not been formally revoked for some time after, or had been allowed to continue until it expired.

ASIO is in the process of implementing procedural changes to ensure prompt revocation when intercept ceases.

ASIO also advised us that they identified a small number of instances in 2010 where, due to an administrative oversight, it had failed to provide certified copies of warrants to relevant telecommunications carriers, to support their request to intercept certain services.¹

As it was the usual practice of ASIO to notify the carrier when a warrant has been signed and then to separately forward a certified copy of the warrant, collection in each case occurred in a timely manner.

Based on our inspection activities I am satisfied that while the requirement to provide certified copies of warrants was overlooked in a small number of cases, the interception activities which took place occurred within the terms set out in the warrant.

ASIO has reviewed its records and has not identified any other instances where a certified copy of a warrant was not provided to the relevant carrier.

In addition to these issues, we also raised a small number of administrative concerns affecting a variety of warrant types. In each of these cases, we received detailed written explanations or briefings, as appropriate, from relevant areas within ASIO, addressing our concerns.

The incidence of error across the full range of warrant categories is low compared to the overall number of warrants issued to ASIO. We will, however, continue to closely monitor use of ASIO's powers, given the significant consequences which can flow from mistakes.

---

¹ Section 15(1) of the TIA requires that ASIO provide a certified copy of each warrant to the relevant carrier, as soon as practicable after they are issued.

ISA agencies

We inspected every MA issued to DSD, DIGO and ASIS. Overall, we found that the reasons put forward to obtain MAs were clearly articulated and relevant to their respective functions.

We identified several minor administrative errors (for example, the incorrect citation of a subsection number, incorrect or non-dating of instruments, and some template errors) but we were satisfied that none of these defects were such as to bring into question the validity of the authorisations in question.

We noted an increased use of joint submissions by DSD and DIGO when seeking authorisation to conduct collection activities against a common subject.

In all cases where ASIS, DSD or DIGO seek to produce intelligence information on an Australian person on the ground that the person poses a possible threat to Australia's security, the endorsement of the Attorney-General is also required. We identified no instances where an MA was issued on security grounds without the agreement of the Attorney-General.

While the agencies generally work closely together problems can sometimes occur where a new target emerges unexpectedly, or when the endorsement of the Attorney-General is unexpectedly delayed in respect of time critical cases. The agencies are aware of these issues and ensure that all legal requirements are satisfied.

Reports of warrants and MAs

The legal authorities under which warrants and MAs are issued each require that a report be provided to the responsible Minister expressly detailing how useful the warrant or authority was in achieving its objective. In almost all cases where a renewal of an existing warrant or authorisation was sought, the report on the usefulness of the warrant or authorisation is presented as a part of the renewal request package. This can inform the decision of the responsible Minister on whether a renewal can be justified.

These reports must usually be provided to the responsible Minister within three months of the expiry, revocation, or exhaustion, of the relevant approval. We identified no instances where requisite reporting was

not provided within statutory timeframes. The reports provided the relevant Minister with a balanced appraisal.

In summary, I was satisfied that each warrant and MA that was sought during the 2011-2012 reporting period was supported by an intelligence case and fulfilled the legal requirements for their issue.

Review of Foreign Intelligence Collection warrants

In March 2012 I conducted an ad hoc inspection of all Foreign Intelligence Collection warrants issued between September 2011 and February 2012.

Foreign Intelligence Collection warrants are issued by the Attorney-General on the basis of advice from either the Minister for Foreign Affairs or the Minister for Defence that the collection of the foreign intelligence is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well being. The warrants can authorise telecommunications interception and the use of ASIO 'special powers', including listening devices, search powers and computer access. The warrants cannot be issued for the purpose of producing intelligence concerning an Australian citizen or permanent resident.

These operations involve close co-ordination between ASIS, DSD and ASIO, so in reviewing this class of warrants, I had regard to the full range of material from across these agencies.

My review considered the timeliness and comprehensiveness of the advice to the relevant Ministers. Generally the processes were sound although there was some variation between agencies.

Although I was satisfied that no unlawful collection occurred, I did note that in some instances where the grounds for certain warrants had ceased to exist, ASIO's notification to the Attorney-General that it had ceased interception was not provided 'forthwith' as required by legislation. ASIO has accepted my finding in this regard, and has undertaken to revise its processes.

Protecting the privacy of Australian persons

The activities of AIC agencies should not intrude unreasonably into the privacy of Australian persons, or where such intrusions are unavoidable, the distribution of this information should be limited to persons or agencies with a demonstrable 'need to know'.

The extent to which ASIO can intrude into the private affairs of Australian persons is governed by the ASIO Act and the Attorney-General's Guidelines. 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.

Our ASIO inspection teams are tasked to constantly consider whether or not ASIO is acting in accordance with its statutory functions, and the Attorney-General's Guidelines.

The ISA agencies (ASIS, DSD and DIGO) are each subject to privacy rules authorised by the responsible Minister which set out the limited circumstances in which intelligence information on or about Australian persons can be disclosed.

My office proactively reviews files from DSD (monthly) and DIGO (bi-monthly) to determine that reporting is in accordance with privacy rules. My office also meets with ASIS bi-monthly to discuss privacy rules issues.

The intelligence assessment agencies (DIO and ONA) are not subject to the ISA but as they each draw upon intelligence information obtained by the intelligence collection agencies in producing their assessments, they have in place administrative privacy guidelines which have a similar effect to the privacy rules.

Each of the AIC agencies subject to privacy rules or guidelines is required to generate privacy compliance records every time they pass information which references an Australian person. These records must be made available to IGIS upon request.

The ISA agencies are also required to alert me if they identify they may have acted in breach of their privacy rules or guidelines, or where they ascertain that an individual who has been previously referred

to in their communications is later regarded as an Australian person.

For the most part, the AIC agencies complied with their privacy obligations and ensured that their privacy rules or guidelines were well understood by staff and applied in a consistent manner.

We became aware of several instances throughout 2011-12, where an agency had established that an individual was, or was not, an Australian person, and this information was not known to other members of the AIC. During the period, a review was conducted into how ISA agencies share this information with each other, and this problem has now been largely addressed.

Other common issues which arose related to distinguishing whether something was public knowledge (and could be freely reported) or contained intelligence information (which could be reported if there was sufficient justification), and ascertaining whether particular entities were Australian persons for the purpose of applying the privacy rules or guidelines.

Some privacy issues are peculiar to individual agencies. An example of this is that while the privacy rules can usually be easily applied to written intelligence reports or documents, they are more difficult to apply to imagery products, or discussions, in which intelligence information about Australian persons has been shared.

As a part of its functions DIGO produces a range of imagery intelligence products which sometimes include Australian interests and Australian persons. While DIGO may not have formulated an intention to produce intelligence on the Australian persons or interests, it is nonetheless obliged to minimise any potential adverse privacy impacts.

During the reporting period I noted some inconsistencies in the application of the DIGO privacy rules by DIGO analysts which suggested that they continued to experience challenges in the application of the rules. My staff engaged closely with DIGO to work through and overcome these concerns.

Our review of the application by DSD of their privacy rules during 2011-12 identified a low number of incidents where the privacy rules were not applied appropriately. On each occasion where a privacy related concern arose, DSD compliance officers investigated the issue and provided me with a report.

Similarly, ASIS has also proactively reported on privacy rules issues or concerns. Most have been issues regarding a presumption of nationality (that has later been found to be incorrect) or minor administrative error.

Overall I am satisfied that each AIC agency understands and accepts their privacy obligations and has put appropriate measures in place to ensure that they are met.

Access to sensitive financial intelligence information

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 AIC agencies and OIGIS are designated agencies for the purposes of the AML/CTF Act.

This office is party to a memorandum of understanding (MOU) with AUSTRAC which sets out an agreed understanding of the Inspector-General's role in monitoring agencies' access to, and use of, AUSTRAC information.

We conduct inspections to ensure searches undertaken in the AUSTRAC database by AIC staff are for a clear intelligence related purpose, are suitably focussed, and do not abuse the privileged access to these sensitive records through accessing records not related to the prescribed functions of AIC agencies. We also review AIC agencies' sharing of AUSTRAC information within Australia and with their foreign intelligence counterparts.

During 2011-12 OIGIS staff conducted a significant number of inspections of ASIO's access to, and use of, AUSTRAC information. These inspections included checks conducted for intelligence and security vetting purposes and the passage of AUSTRAC information to and from ASIO. We conducted fewer checks in ASIS and DIGO due to their less frequent access to, and use of, AUSTRAC information.

During 2010-11 only ASIO and ASIS accessed AUSTRAC data. I advised the Attorney-General and the Minister for Foreign Affairs in December 2011 that, based on monitoring activities undertaken by this office in 2010-11, I was satisfied that ASIO and ASIS were compliant with their obligations under the AML/CTF Act and the terms of their respective MOUs with AUSTRAC.

The AUSTRAC-IGIS MOU is currently being updated to reflect the need for my office to provide assurance to each Minister responsible for an AIC agency.

Inspection activities specific to ASIO

Approvals for investigations and reviews of investigations

ASIO is empowered under the ASIO Act to obtain, correlate and evaluate intelligence information relevant to security. The circumstances and manner in which ASIO can collect personal information and conduct investigations into persons of possible security interest are detailed in the Attorney-General's Guidelines and in internal policies and procedures.

During 2011-12 my staff regularly inspected documents and files detailing how and why ASIO investigations were initiated and the results of these investigations. We considered whether the investigations were properly justified and lawful, had achievable objectives, were conducted in an appropriate manner, and were subjected to appropriate periodic review.

At each inspection, we selected a representative sample of cases and focussed on particular themes or issues that we assessed to have potential for a higher level of risk.

The documentation associated with most of the investigations reviewed in 2011-12 indicated compliance with the relevant legislation, guidelines and internal policy.

In a small number of cases where the authorisation complied with policy requirements but was poorly expressed, or did not provide sufficient detail, we provided informal feedback to relevant line managers to encourage continuing improvement in standards and consistency of approach across the agency.

In the many requests for approval to conduct an investigation which we examined, the proposed investigation's connection to security was always clearly articulated. As has been the case in previous years, we continued to focus closely on the comments and guidance provided by senior ASIO officers when approving investigations. In particular we looked for evidence that the authorising officers had considered the particular circumstances of the case and provided specific and relevant guidance.

As a result of our inspections I am satisfied that the process for initiating, conducting and reviewing security related investigations is rigorous.

Data inquiry requests

Data inquiry requests (DIRs) are 'one off' inquiries which enable telecommunications related data (but not content) and financial data to be accessed. DIRs are designed to limit the intrusiveness of ASIO activities while providing extra information to assist in assessing the need to use more intrusive investigative methods at a later stage.

During 2011-12 OIGIS staff reviewed a representative sample of DIRs to check whether:

- the objective of the inquiry was relevant to ASIO's statutory functions
- there was sufficient background to explain how the subject came to ASIO attention, the specific data set required, and the objectives of the inquiry
- the request complied with limits placed on inquiries of this kind, and
- the inquiry request was appropriately authorised.

The inspections undertaken by OIGIS staff in 2011-12 revealed that most DIRs which we examined were properly made and authorised at the appropriate level within ASIO. Where errors were made these were mostly administrative in nature.

One recurring issue identified was the failure of some staff to clearly record a decision about the relevance of returned data to the security matter which had prompted the request. My office provided regular feedback to ASIO on this issue and we will continue to monitor ASIO's use of this method of inquiry to ensure that such judgements are made and regularly recorded.

Access to telecommunications locational information or subscriber data

The TIA Act provides legal authority for a specified group of ASIO senior managers to authorise collection of historical and prospective telecommunications data from telecommunications carriers or carriage service providers. Authorisations for prospective telecommunications data allow the collection of near real-time location and other subscriber information

that comes into existence during the period that an authorisation is in force. A request for prospective telecommunications data may only be made when other less intrusive collection methods have been considered and determined to be insufficient. A prospective authorisation operates for the period of time defined in the authorisation, which cannot exceed 90 days in duration.

We review ASIO's requests for access to prospective telecommunications data because of the intrusive nature of the collection activity, which is approved outside the warrant process. Our inspection of these activities is similar to our inspection of telecommunications interception warrants. We also check ASIO's interception management systems to review whether collection took place within the terms of the authority, and where errors have been made, that any resulting product has been deleted from ASIO's systems.

During the reporting period we reviewed every request to renew (that is, continue) prospective telecommunication data collection to provide assurance that these authorities were renewed only where exceptional circumstances exist. I was satisfied that renewed requests for prospective telecommunications data were limited to those cases where reasonable alternatives did not exist.

The inspections undertaken by OIGIS staff in 2011-12 revealed that all requests for prospective telecommunications data were endorsed at an appropriately senior level within ASIO. In the few instances where errors were made, these errors had been already identified by ASIO and appropriate and timely remedial action taken. In circumstances where the reasons for the granting of the authorisation ceased to exist prior to the expiry of the authorisation, I found that ASIO consistently revoked the authorisations in a timely manner.

Overall, we were satisfied that ASIO is using this method of inquiry in a suitable manner and that internal controls are well-developed and appropriate.

Access to taxation information

Section 355-70 of Schedule 1 to the *Taxation Administration Act 1953* (TAA) provides for a taxation officer authorised by the Commissioner or delegate of

the Commissioner to disclose protected information² to an authorised ASIO officer if the Commissioner, a Second Commissioner or an SES employee or acting SES employee of the Australian Taxation Officer (ATO), is satisfied the information is relevant to the performance of ASIO's functions under s. 17(1) of the ASIO Act.

ASIO's access to protected information is the subject of a formal MOU between the Director-General of Security and the Commissioner of Taxation. The Attorney-General's Guidelines generally, and ASIO's internal guidelines and procedures specifically, dictate that a request for taxation information can only be made when less intrusive means have not yielded the required information

ASIO is also able to pass protected information to a law enforcement agency for the purpose of, or in connection with: investigating a serious offence; or enforcing a law, the contravention of which is a serious offence; or the making, or proposed making, of a proceeds of crime order.

ASIO accesses protected information infrequently due to the particular sensitivities associated with information of this kind. OIGIS is committed to reviewing all requests made by ASIO to the ATO, spontaneous disseminations of information from the ATO and passage of information by ASIO to a law enforcement agency. In 2011-12 my office did not identify any matters of significant concern.

We were advised late in the 2011-12 reporting period that ASIO had accessed sensitive tax information relating to one individual in the previous 12 months. We did not have the opportunity to review this material before the end of the reporting period. Any issues arising from our subsequent review of this information will be provided in our next annual report.

Exchange of information with foreign liaisons

ASIO maintains a small network of out-posted liaison officers in a range of overseas locations,

with the knowledge and consent of the host countries, in order to obtain, correlate, evaluate and communicate intelligence information that is relevant to Australia's security interests.

ASIO can lawfully exchange information about Australian and foreign persons with a large number of foreign authorities that have been approved by the Attorney-General as being capable of assisting ASIO in the performance of its functions. The approved foreign authorities includes government agencies that perform functions relating to intelligence and security, law enforcement, immigration and border control, and whole of government coordination.

The focus of our inspections is ordinarily on instances where exchanges of information have occurred with respect to Australian persons or interests, but we also examine cases where information is exchanged on non-Australian persons.

Following recommendations made in my inquiry report relating the arrest and detention of Mr Mamdouh Habib, ASIO revised its guidelines on exchanging of information with foreign liaisons. This is discussed further at page 13. ASIO is required to ensure that liaison officers and decision makers within the agency are informed of their obligations. As part of this process, I addressed the annual conference of ASIO's overseas based liaison officers.

During 2011-12 my office inspected documentation and correspondence logs on ASIO's dealings with approved authorities in fourteen countries. These inspections identified no issues of significant concern.

Use of assumed identities

Section 15LE of the *Crimes Act 1914* requires ASIO, to as soon as practicable after 30 June each year, provide me with a report which details the number of instances in which formal alternative identity documentation has been obtained, and a general description of the activities undertaken by approved persons when using their assumed identities.

The Director-General of Security provided me with such a report, covering ASIO's assumed identity arrangements between 1 July 2010 and 30 June 2011, in September 2011. There was nothing in this report which caused me any concern.

2 Protected information is defined under 355-30, Schedule 1 of the TAA. Protected information means information that was disclosed or obtained under or for the purposes of a law that was a taxation law; relates to the affairs of an entity; and identifies or is reasonably capable of being used to identify the entity.

Engagement with law enforcement agencies

ASIO regularly engages with the Australian Federal Police and with state and territory police services. This is because there is sometimes overlap between persons who are of security interest, and persons who are engaged in criminal activities. The exchange of information between ASIO and these law enforcement bodies is required to be limited to lawful disclosures and is regulated by statutory requirements, MOUs and internal policy requirements.

Cooperation is also necessary in order to plan effectively for major events where Australia has obligations such as those with respect to the protection of visiting foreign dignitaries, such as the forthcoming G20 Leaders meeting to be held in Brisbane in 2014.

During 2011-12 we reviewed a number of files in ASIO's regional offices which detailed their interactions with locally based law enforcement agencies. These exchanges showed that the passage of intelligence information from ASIO to these agencies was conducted in accordance with statutory and policy requirements.

We noted one instance in particular where vital criminal intelligence which was incidentally obtained by ASIO during a security intelligence investigation was promptly, and appropriately, passed to local authorities to facilitate the arrest of an individual on serious criminal charges.

Questioning and detention warrants

The only warrants which the Attorney-General cannot directly authorise relate to requests by ASIO for either a questioning warrant, or a questioning and detention warrant. Requests for such warrants can only be issued by a relevant issuing authority (that is, a federal magistrate, or a federal judge) and can only proceed if they have the prior consent of the Attorney-General.

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

Inspection activities specific to ASIS

Review of operational files

Several senior members of my staff regularly visited ASIS during 2011-2012 to review ASIS's operational case files. This is an on-going inspection activity. It is publicly known that ASIS activities involve the use of human sources and ASIS officers are deployed in many countries to support a wide range of activities including counter-terrorism, efforts against people smuggling and support to military operations. These activities are often high-risk and sensitive. During the reporting period we reviewed files relating to ASIS's operational activities in a diverse range of countries where ASIS has a presence.

I regard this review activity as being important as it provides a deeper than usual insight into the operational environment in which field staff operate, the extent to which staff in ASIS headquarters evaluate risk and guide sensitive activities, and often also reflects on the health of inter-agency relations.

While the sensitive nature of ASIS's operational activities means that I cannot specifically detail the nature and range of issues arising from these inspections in a public report, I can advise that these reviews are thorough and rigorous and something in which I take a keen personal interest.

Authorisations relating to the use of weapons

During 2011-12 my staff conducted several inspections of records relating to the provision by ASIS of training their staff in the use of self-defence techniques and weapons. These reviews had regard to new guidelines on this subject matter, which were issued by the Director-General of ASIS on 10 June 2011 (as detailed in last year's annual report).

These reviews, combined with the requirement that all incidents where weapons have been discharged (other than in training) must be reported to me, my regular meetings with ASIS officers travelling overseas, and our regular review of ministerial submissions from ASIS to the Minister for Foreign Affairs, provides me with good visibility of weapons related incidents and issues.

I am 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. I am also satisfied that appropriate and thorough training is provided by qualified instructors, and that appropriate controls are in place to limit the circumstances in which weapons may be used.

Use of assumed identities

Section 15LE of the *Crimes Act 1914* requires ASIS, to as soon as practicable after 30 June each year, provide me with a report which details the number of instances in which formal alternative identity documentation has been obtained, and a general description of the activities undertaken by approved persons when using their assumed identities.

The Director-General of ASIS provided me with such a report in September 2011 covering the preceding reporting period. There was nothing in this report which caused me any concern.

Inspection activities specific to DSD

Oversight of collection capabilities

Throughout 2011-12, my office continued to monitor DSD's databases, including collection systems, for compliance with the ISA and DSD policy. These checks were conducted both as part of routine inspection activities, as well as via targeted inspection projects. I noted no incidences of unauthorised collection during the reporting period.

Inspection projects

To supplement our regular review of DSD activities, we also conducted a number of ad hoc inspection projects, including:

- an in-depth review of activities conducted under a specified series of ministerial authorisations
- an in-depth inspection of the activities of one of DSD's collection and reporting sections
- a focussed examination of attachments to reporting.

While no significant concerns were identified, feedback was provided to DSD on several administrative or procedural issues where improvements could be made.

DSD compliance incidents

DSD informs my office every time it conducts an internal compliance investigation and concludes that its processes or systems should be improved. Six instances were reported to me during the year.

I was satisfied with the remedial actions taken by DSD in respect of the compliance investigation reports completed in 2011-12, and the risk mitigation strategies that were applied.

Collection team compliance inspection project

In February 2012 I initiated an inspection project into one of DSD's collection teams. This project was initiated in response to activities highlighted in DSD's 2010-11 classified annual report.

The project entailed inspection and analysis of:

- interaction between the collection team and DSD's Compliance team
- reporting produced by the collection team
- interaction between the collection team and other agencies
- DSD's collection systems
- the collection team's application of privacy rules
- the collection team's record-keeping processes.

In general we found that the team's processes and record-keeping were sound, and that the team appeared to have a well established compliance culture. Issues were identified relating to the retention and transfer of information within the team. In addition, the inspection project identified potential gaps in DSD's compliance oversight due to technical issues.

Feedback was provided to DSD regarding the findings of the inspection, and DSD identified and implemented strategies to ameliorate these risks.

Inspection activities specific to DIGO

Director authorisations

The Minister for Defence has delegated the authority to approve the collection of imagery intelligence of Australian territory by DIGO to the Director of DIGO. A director's authorisation cannot be approved for more than 12 months. In addition to reviewing all ministerial authorisations issued to DIGO, we also examined all imagery related tasking and collection activities which were authorised by the Director DIGO during 2011-12.

DIGO's compliance framework

During the reporting period, I conducted a review of DIGO's compliance framework using the Australian Standard for Compliance Programs, AS 3806-2006, as a benchmark. The aim of the review was twofold; firstly to assess whether the DIGO compliance framework reasonably meets relevant key principles of the standard and secondly to identify any areas of concern where further inquiry is warranted.

The specifics of the review remain classified, but I can report that DIGO's compliance framework demonstrates strong support for the standard. Overall the review proved to be a useful exercise and resulted in some constructive suggestions to strengthen DIGO's internal compliance framework.

IGIS role in Freedom of Information and Archives matters

The *Archives Act 1983* and the *Freedom of Information Act 1982* were amended in late 2009 to enable the IGIS to give evidence in cases involving review of national security, defence or international relations exemptions and confidential foreign government communications exemptions. The first cases under the new provisions occurred in this reporting period.

The amendments require the Information Commissioner or the Administrative Appeals Tribunal (AAT) to call on the expertise of the IGIS in relation to those documents that the Commissioner or the Tribunal is not otherwise satisfied on the basis of the evidence of the parties ought to be exempt. With such an approach the IGIS would

be involved only at the final stage of the decision making process and only in those cases where the Commissioner or the Tribunal was inclined to release a document. It was anticipated that the IGIS would not be called often and as such no additional resources were provided for this new function.

The IGIS and the Information Commissioner agreed a memorandum of understanding in May 2012 that sets out a process to be followed which accords with the original policy intent. The IGIS has not been called by the Commissioner to provide evidence on any cases in 2011-12.

In the first case under the new provisions in the AAT the Tribunal decided it would require that the IGIS prepare evidence on all documents over which a claim for exemption had been made, before the Tribunal had itself heard the evidence of the parties and formed a preliminary view on the exemption claims. As a consequence in that case considerable IGIS resources were devoted to examining documents and preparing evidence. The matter was heard just after the reporting period and the Tribunal did not ultimately call the IGIS to give evidence.

If this approach continues it may result in the IGIS becoming a 'bottleneck' in the review system and significant IGIS resources being diverted into preparing evidence which is not ultimately used by the Tribunal. This will impact on IGIS oversight of intelligence and security agencies particularly in respect of more complex inquiry work. We are working together with the AAT and other government agencies to make the procedure more efficient.

PART THREE: MANAGEMENT AND ACCOUNTABILITY

Corporate governance

Organisational structure

Senior positions occupied during 2011-12 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 (from 3 January 2012)

Principal Review and Investigations Officers (EL 2)

Mr Neville Bryan PSM

Ms Sharon Dean

Ms Maryanne Gates

The full staffing complement for 2011-12 was fourteen including six EL 1/APS 6 Review and Investigations Officers, one Office Accountant, one Personal Assistant to the Inspector-General and one Administration Officer.

Senior management committees

The OIGIS Audit Committee is the sole 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.



Dr Vivienne Thom and staff

The office addresses these matters through:

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

Internal audit and risk management

The OIGIS Audit Committee Charter was updated in June 2012 to reflect changes recommended in the 2011 ANAO *Better Practice Guide – Public Sector Audit Committees*. This included a restructure of the Audit Committee so the Chair is an external member. The current Audit Committee consists of Mr Matthew King (Treasury) as Chair and Mr Trevor Kennedy (Attorney General's Department) and Mr Jake Blight (OIGIS) as members. The Inspector-General now attends OIGIS Audit Committee meetings as an observer only.

The Audit Committee meets on a periodic basis to consider corporate governance issues including financial compliance, internal and external audit findings, fraud and risk management, occupational health and safety, and significant financial issues.

The Committee reviews the Risk Management Plan on an annual basis and makes amendments as required. The Committee also reviews the office's risk performance over the previous twelve months.

The Risk Management Plan includes controls designed to mitigate risks including in the following risk categories:

- personnel related
  - » departure or absence of key staff with little notice (for example, through illness or injury)
  - » 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 six categories listed above.

Protective Security Policy Framework

Due to the nature of the activities of my office, we hold a broad range of information originating from the AIC agencies. I regard the protection of that information as being of the utmost importance.

To that end, my office maintains the highest standards of security awareness and procedures to protect that information.

In 2010 the Commonwealth Government introduced the Protective Security Policy Framework (PSPF). The PSPF provides the appropriate security controls for the Australian Government to protect its people, information and assets through a series of mandatory requirements. Agencies must report compliance with the mandatory requirements annually. In order to ensure compliance with the PSPF, my office undertook a comprehensive review of security policy, processes and practices during 2011-12.

Ethical standards and fraud control

While the Risk Management Plan is comprehensive in that it includes fraud prevention, detection and management, the office also maintains a separate Fraud Control Plan which explores in greater detail risks of that type and how they are dealt with. This is updated annually.

Fraud control

I can certify that my office has undertaken a fraud risk assessment and has a fraud control plan, both of which are reviewed periodically. I can further certify that appropriate fraud prevention, detection, investigation and reporting procedures are in place which comply with the Commonwealth Fraud Control Guidelines, and that the office has responded to the annual survey for fraud control data.

Employment of SES Officers

A temporary SES cap of one officer had previously been approved for a nine month period commencing on 10 January 2011 to assist in the conduct of the Habib Inquiry. This position was filled by Ms Diane Merryfull on secondment from the Office of the Commonwealth Ombudsman and expired in October 2011.

In light of recent increases in the scope and complexity of the work of the office, in August 2011 the Special Minister of State for the Public Service and Integrity approved an increase in the SES cap of the office for

the role of Assistant-Inspector General of Intelligence and Security. No additional resources were sought for the position, which is funded from within the existing budget and offset by savings in the requirement for external legal advice and consultants.

The position was filled by Mr Jake Blight, who commenced on 3 January 2012. The terms and conditions of Mr Blight's employment, including salary, are set out in a Section 24(1) determination and 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.

External Scrutiny

Decisions by the judiciary or tribunals

The only decision made by the Judiciary or a Tribunal that had a direct impact on the office in 2011-12 was the decision of the Administrative Appeals Tribunal (AAT) in *Corby v Australian Federal Police* [2011] AATA 861 (29 November 2011). Prior to that decision it was the understanding of the IGIS that the AAT would only call on the IGIS to give evidence in Freedom of Information cases once the AAT had considered the evidence of the parties and formed a preliminary view that a document was not exempt. In *Corby* the Tribunal decided that it was able to require the IGIS to prepare evidence at any time, including before the Tribunal had heard the evidence of the parties. This approach has significant resource implications for the office. Further details on this can be found on page 27 in the Performance chapter, under 'IGIS role in Freedom of Information and archives matters'.

The High Court heard the case of *M47/2012 v Director-General of Security & Others* in June 2012. The decision has been reserved and is expected to be handed down in late 2012. The case concerns the ongoing detention of a person who has been found to be a refugee but who has been given an adverse security assessment by ASIO. The issues in the case

include whether ASIO provided procedural fairness when making the adverse assessment and whether the relevant part of the Migration Regulations 1994 (public interest criteria 4002 in Schedule 2) is valid. The outcome of the case may have an effect on how the office oversees ASIO security assessments, and in particular the lawfulness, in terms of procedural fairness, of ASIO security assessment decisions.

Reports by the Auditor General, Parliamentary Committees and the Commonwealth Ombudsman

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.

Management of human resources

Workforce planning, staff retention and turnover

During the reporting period, the office maintained an average staffing level of 13 employees due to:

- the resignation of one employee
- the recruitment of one new ongoing part time SES employee.

Two of the 13 staff employed by my office are on temporary transfer from another Commonwealth agency.

In light of current efficiency dividends, I do not anticipate that I will run a recruitment exercise in 2012-13.

Staff survey

In late 2011 the Australian Public Service Commission conducted a staff survey for micro-agencies and provided this office with an agency-specific benchmarking report. This was the first staff survey carried out in the 25 years history of the

office and the one hundred per cent participation rate indicates that staff were pleased to have the opportunity to note their views.

As would be expected for such a small agency, satisfaction with agency management, leadership and job satisfaction were well above APS averages as well as being significantly above the average for other micro-agencies. Areas that we will need to address in the future include satisfaction with access to learning and development and career progression but these are again fairly typical of the challenges that small agencies face. One area that does require attention is the low level of satisfaction with the quality of coaching and mentoring and this will be an area of focus in the next reporting period.

Overall this survey was a valuable tool for assessing staff attitudes and we are grateful to the APSC for conducting it. I hope that it will be repeated in the future.

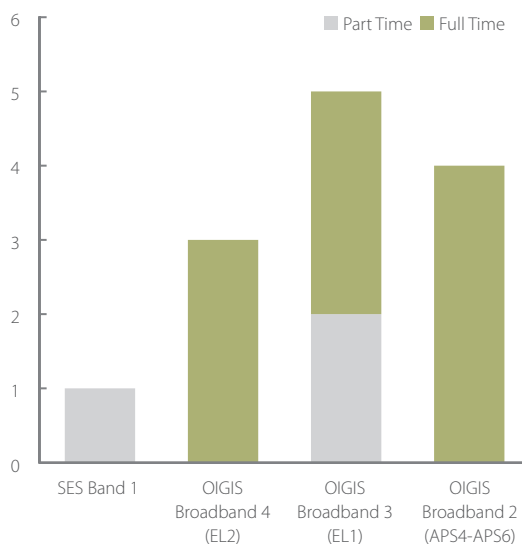
Organisational profile

At the end of the 2011-12 reporting period, the office had 13 ongoing APS employees located in the Australian Capital Territory.

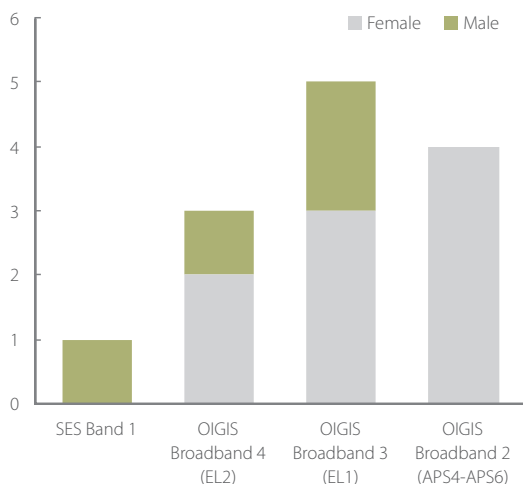
This compares to 13 ongoing APS employees located in the Australian Capital Territory at the end of 2010-11.

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

**Organisation Profile as at 30 June 2012
(employment level and status)**



Gender Balance as at 30 June 2012 (by employment level)



Employment frameworks

At 1 July 2011, all non-SES staff were employed under OIGIS Enterprise Agreement 2011 – 2014, which came into effect on 10 June 2011. One SES staff member was employed under a Section 24(1) determination, with effect 3 January 2012.

The salary range available to APS employees in OIGIS throughout 2011-12 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 Top Secret Positive Vet clearance, as well as other restrictions placed on employees as a result of reviewing the activities of the AIC. The annual allowance was \$1,030 per annum as at 30 June 2012.

Training and staff development

OIGIS introduced an ongoing structured internal training program 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 2012 included:

- What is 'intelligence information' for the purpose of the privacy rules?
- Propriety – what is it?
- When does an agency require a ministerial authorisation to 'produce intelligence'?

- Responding to complainants
- Human rights (presented by staff from the Australian Human Rights Commission).

Staff were provided with regular opportunities throughout 2011-12 to attend other training courses and seminars relevant to their roles. A studies assistance scheme is also 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 Guidelines.

Consultants

Generally a small number of consultants are engaged each year by the office on an 'as-required' basis. Consultants are used where short term resources are inadequate or specialist expertise is required. The security requirements of the office and the specialist nature of the consultancy work often means that consultants are directly sourced.

Where the work is more general in nature the office will, where possible, access consultants selected by PM&C through an open tender or panel selection process.

The decision to engage a consultant is made in accordance with the *Financial Management and Accountability Act 1997* and related regulations including the Commonwealth Procurement Guidelines and relevant internal guidelines.

Total actual expenditure on consultancy contracts for 2011-12 was \$35 934.45 (GST inclusive). This comprised:

- \$16 000.00 (GST inclusive) for one new consultancy contract, which was completed during the reporting period.

There were two ongoing contracts from the previous financial year.

This compares to consultancy expenditure of \$161 248.63 (GST inclusive) in 2010-11, and \$191 467 (GST inclusive) in 2009-10.

Annual reports contain information about actual expenditure on contracts for consultancies. Information on the value of contracts and consultancies is available on the AusTender website www.tenders.gov.au.

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.

Legal services

Expenditure on legal services has previously fluctuated from year to year and is largely dependent upon the nature of the inquiries undertaken. The recruitment in January 2012 of a legally qualified SES Band 1 to fill the role of Assistant Inspector-General of Intelligence and Security is expected to largely reduce future expenditure on legal services.

In 2011-12 legal advice was obtained from:

- Dr Melissa A Perry QC, to a total cost of \$19 886.00 (GST inclusive). This comprised \$19 886.00 (GST inclusive) in respect of tied work pursuant to the Commonwealth Legal Services Directions. The total expenditure compares to \$88 343.15 (GST inclusive) in 2010-11.
- Demir Legal, to a total cost of \$48.45 (GST inclusive). This comprised \$48.45 (GST inclusive) for general legal services and represents an adjustment to invoices received in the previous financial year. The total expenditure compares to \$8 277.00 (GST inclusive) in 2010-11.

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 a new National Disability Strategy which sets out a ten year national policy framework for improving life for Australians with disability, their families and carers. A high level report to track progress for people with disability at a national level will be produced by the Standing Council on Community, Housing and Disability Services to the Council of Australian Governments and will be available at www.fahcsia.gov.au.

The Social Inclusion Measurement and Reporting Strategy agreed by the Government in December 2009 will also include some reporting on disability matters in its regular *How Australia is Faring* report and, if appropriate, in strategic change indicators in agency Annual Reports. More detail on social inclusion matters can be found at www.socialinclusion.gov.au.

Work health and safety

The office's Health and Safety Management Arrangements were updated in February 2012 to incorporate changes resulting from the new *Work Health and Safety Act 2011* (WHS Act), which took effect on 1 January 2012.

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 or dangerous incidents resulting from undertakings carried out by the office that would require reporting under either the WHS Act, or previously under the *Occupational Health and Safety Act 1991* (OHS 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 or previously the OHS Act.

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.

A total of \$443.29 (GST inclusive) was paid for recruitment advertising.

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 I am directly responsible in which I take into account the environmental impact and act accordingly to minimise it. These include:

- recycled paper was used for 94.5 per cent of the office's photocopying, facsimile reports and document printing in 2011-12
- 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
- where there is no operational impact, office equipment is 'shut-down' overnight, rather than being placed on 'stand-by'.

Summary of financial performance and resources for outcomes

OIGIS received an unqualified audit report from the Australian National Audit Office for its 2011-12 financial statements.

The office operated within available resources in 2011-12 and ended the year with a surplus of \$189 903 compared to a budgeted break even position.

In relation to expenditure the most significant budget variance consisted of \$101 000 overspend on employee expenses which related to changes in the government bond rate and the resulting impact on accrued leave liabilities. Other significant variances included a \$27 000 underspend on legal expenses and \$18 000 underspend on training expenses (both of which are demand driven).

Appropriation funding increased from \$2 095 000 in 2010-11 to \$2 241 000 in 2011-12. This increase represents funding related to the new whistleblower protection scheme.

Net equity increased from \$1 165 561 in 2010-11 to \$1 364 464. Movements in net equity included a \$189 903 increase in retained surplus and a \$9 000 increase in contributed equity via the departmental capital budget.

The following tables can be found in Annex 3:

Table 3.1 – Agency Resource Statement and Resources for Outcomes 2011-12, and

Table 3.2 – Expenses and Resources for Outcome 1.

OIGIS has one outcome and one output.

Trends in finances

Significant changes to the finances of the office during 2011-12 include:

- A \$90 532 increase in Other Gains. The increase represents the value of resources received free of charge from the DSD as part of the secure IT system upgrade during 2011-12.
- A \$168 885 decline in Own Source Revenue, mainly related to the significant s. 31 funding received in 2010-11 to cover inquiry costs.
- A \$48 947 increase in Property Plan and Equipment resulting from the secure IT system upgrade.
- A \$226 502 increase in Employee Provisions due to staff movements and the impact of the change in the Government bond rate on accrued leave liabilities.

	2011-12 OUTCOME 1 \$'000	2010-11 OUTCOME 1 \$'000	Change from previous year
Revenues from government	2 241 000	2 095 000	+7%
Other income	483 199	561 552	-14%
TOTAL INCOME	2 724 199	2 656 552	
Employee expenses	2 041 602	1 973 173	+3.5%
Supplier expenses	450 993	486 403	-7%
Other expenses	41 701	16 607	+250%
TOTAL EXPENSES	2 534 296	2 476 183	
OPERATING RESULT	189 903	180 369	
Financial assets	2 090 096	2 007 141	+4%
Non-financial assets	127 434	77 859	+160%
Liabilities	853 066	919 439	-8%
NET ASSETS = A + B - C	1 364 464	1 165 561	



PART FOUR: FINANCIAL STATEMENTS



INDEPENDENT AUDITOR'S REPORT

To the Special Minister of State

I have audited the accompanying financial statements of Office of the Inspector General of Intelligence and Security for the year ended 30 June 2012, which comprise: a Statement by the Inspector General of Intelligence and Security; Statement of Comprehensive Income; Balance Sheet; Statement of Changes in Equity; Cash Flow Statement; Schedule of Commitments; and Notes to and forming part of the financial statements comprising 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 for the preparation of financial statements that give a true and fair view in accordance with the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, including the Australian Accounting Standards, and for such internal control as is necessary to enable the preparation of the financial statements that give a true and fair view and 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 Office of the Inspector General of Intelligence and Security's preparation of the financial statements that give a true and fair view 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 Office of the Inspector General of Intelligence and Security'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 of the Office of the

GPO Box 707 CANBERRA ACT 2601
19 National Circuit BARTON ACT 2600
Phone (02) 6203 7300 Fax (02) 6203 7777

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

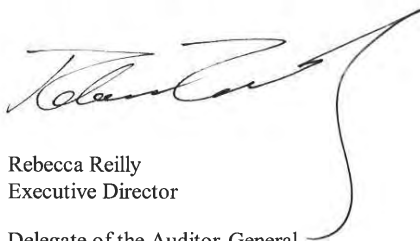
In conducting my audit, I have followed the independence requirements of the Australian National Audit Office, which incorporate the requirements of the Australian accounting profession.

Opinion

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

- (a) have been prepared in accordance with the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, including the Australian Accounting Standards; and
- (b) give a true and fair view of the matters required by the Finance Minister's Orders including the Office of the Inspector General of Intelligence and Security's financial position as at 30 June 2012 and of 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

6 September 2012

STATEMENT BY THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2012 are based on properly maintained financial records and give a true and fair view of the matters required by the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, as amended.



Dr Vivienne Thom
Inspector-General of
Intelligence and Security

6 September 2012

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY
STATEMENT OF COMPREHENSIVE INCOME
for the year ended 30 June 2012

	Notes	2011-12 \$	2010-11 \$
EXPENSES			
Employee benefits	3A	2 041 602	1 973 173
Supplier	3B	450 993	486 403
Depreciation and amortisation	3C	33 799	16 065
Loss on asset disposal	3D	7 902	542
Total Expenses		2 534 296	2 476 183
LESS:			
OWN-SOURCE INCOME			
Own-source revenue			
Other	4A	268 077	436 962
Total own-source revenue		268 077	436 962
Gains			
Other	4B	215 122	124 590
Total gains		215 122	124 590
Total own-source income		483 199	561 552
Net cost of services		2 051 097	1 914 631
Revenue from Government	4C	2 241 000	2 095 000
Surplus attributable to the Australian Government		189 903	180 369
OTHER COMPREHENSIVE INCOME			
Changes in asset revaluation surplus		-	-
Total comprehensive income attributable to the Australian Government		189 903	180 369

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

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

BALANCE SHEET

as at 30 June 2012

Balance Sheet	Notes	2011-12 \$	2010-11 \$
ASSETS			
Financial Assets			
Cash and cash equivalents	5A	197 352	197 325
Trade and other receivables	5B	1 892 744	1 809 816
Total financial assets		2 090 096	2 007 141
Non-Financial assets			
Property, plant and equipment	6A & 6B	126 250	77 303
Intangibles	6C & 6D	-	-
Other	6E	1 184	556
Total non-financial assets		127 434	77 859
Total Assets		2 217 530	2 085 000
LIABILITIES			
Payables			
Suppliers	7A	19 562	139 067
Other	7B	50 281	223 651
Total payables		69 843	362 718
Provisions			
Employee provisions	8A	783 223	556 721
Total provisions		783 223	556 721
Total Liabilities		853 066	919 439
Net Assets		1 364 464	1 165 561
EQUITY			
Parent Entity Interest			
Contributed equity		447 000	438 000
Reserves		6 796	6 796
Retained surplus		910 668	720 765
Total parent entity interest		1 364 464	1 165 561
Total Equity		1 364 464	1 165 561

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 2012

	Retained Earnings		Asset Revaluation Surplus		Contributed Equity/Capital		Total Equity	
	2012 \$	2011 \$	2012 \$	2011 \$	2012 \$	2011 \$	2012 \$	2011 \$
Opening balance								
Balance carried forward from previous period	720 765	540 395	6 796	6 796	438 000	366 000	1 165 561	913 192
Adjusted opening balance	720 765	540 395	6 796	6 796	438 000	366 000	1 165 561	913 192
Comprehensive Income								
Other comprehensive income	-	-	-	-	-	-	-	-
Surplus for the period	189 903	180 369	-	-	-	-	189 903	180 369
Total comprehensive income	189 903	180 369	-	-	-	-	189 903	180 369
of which:								
Attributable to the Australian Government	189 903	180 369	-	-	-	-	189 903	180 369
Transactions with owners								
Contributions by Owners								
Equity Injection - Appropriation	-	-	-	-	-	-	-	-
Departmental Capital Budget	-	-	-	-	9 000	72 000	9 000	72 000
Sub-total transactions with owners	-	-	-	-	9 000	72 000	9 000	72 000
Closing balance as at 30 June	910 668	720 765	6 796	6 796	447 000	438 000	1 364 464	1 165 561
Closing balance attributable to the Australian Government	910 668	720 765	6 796	6 796	447 000	438 000	1 364 464	1 165 561

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

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY
CASH FLOW STATEMENT
for the year ended 30 June 2012

	Notes	2011-12 \$	2010-11 \$
OPERATING ACTIVITIES			
Cash received			
Appropriations		2 154 800	2 097 293
Net GST		35 783	43 805
Other cash received		77 916	686 362
Total cash received		2 268 499	2 827 460
Cash used			
Employees		(1 843 668)	(1 840 006)
Suppliers		(357 037)	(312 405)
Section 31 receipts transferred to OPA		(67 768)	(620 431)
Other		-	-
Total cash used		(2 268 473)	(2 772 842)
Net cash from operating activities	9	26	54 618
INVESTING ACTIVITIES			
Cash received			
Proceeds from sales of property, plant and equipment		-	-
Total cash received		-	-
Cash used			
Purchase of property, plant and equipment		(75 283)	(41 585)
Total cash used		(75 283)	(41 585)
Net cash from (used by) investing activities		(75 283)	(41 585)
FINANCING ACTIVITIES			
Cash received			
Contributed equity		75 283	41 585
Total cash received		75 283	41 585
Net cash from financing activities		75 283	41 585
Net increase in cash held		26	54 618
Cash and cash equivalents at the beginning of the reporting		197 326	142 708
Cash and cash equivalents at the end of the reporting period	9	197 352	197 326

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

SCHEDULE OF COMMITMENTS
as at 30 June 2012

	2012 \$	2011 \$
BY TYPE		
Commitments Receivable		
GST recoverable on commitments	27 471	25 706
Total Commitments Receivable	27 471	25 706
Commitments Payable		
Other Commitments		
Other	272 971	272 971
Operating Leases	24 755	9 798
Total Other Commitments	297 726	282 769
Net Commitments by Type	270 255	257 063
BY MATURITY		
Commitments Receivable		
One year or less	6 146	5 631
From one to five years	21 325	20 075
Over five years	-	-
Total operating lease income	27 471	25 706
Commitments Payable		
Operating Lease Commitments		
One year or less	8 563	7 349
From one to five years	16 192	2 450
Over five years	-	-
Total Operating Lease Commitments	24 755	9 799
Other Commitments Payable		
One year or less	54 594	54 594
From one to five years	218 377	218 376
Over five years	-	-
Total Other Commitments Payable	272 971	272 970
Net Commitments by Maturity	270 255	257 063

Note: Commitments are GST inclusive where relevant.

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

OIGIS in its capacity as a lessee holds two motor vehicle operating leases. The first lease has contracted monthly payments of \$612.43 and expires 19 October 2012. The second lease is expected to commence on 17 September 2012.

OIGIS also 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 the current and following four years.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

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 dependant 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 49 of the *Financial Management and Accountability Act 1997*.

The Financial Statements and notes have been prepared in accordance with:

- Finance Minister's Orders (or FMO) for reporting periods ending on or after 1 July 2011; 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 FMOs, assets and liabilities are recognised in the balance sheet 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 executor contracts are not recognised unless required by an accounting standard. Liabilities and assets that are unrecognised are reported in the schedule of commitments or the contingencies note (refer Note 1.18).

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.

1.4 Correction of Comparatives

The comparatives for Note 3A have been adjusted. In 2010/2011 Note 3A incorrectly showed the expenses relating to Defined Contribution Plans as expenses relating to Defined Benefit Plans and vice versa. There has also been an adjustment to the breakdown between the two expense types with the total expense remaining unchanged.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

1.5 New Australian Accounting Standards

Adoption of New Australian Accounting Standard Requirements

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

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

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.

1.6 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.

1.7 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.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

The main resources received free of charge in 2011-12 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). Other resources received free of charge include auditor remuneration as disclosed in Note 11.

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.

1.8 Transactions with the Government as Owner

Contributed Equity

Amounts appropriated which are designated as 'equity injections' for a year (less any formal reductions) and or Departmental Capital Budgets (DCBs) are recognised directly to contributed equity in that year.

1.9 Employee Benefits

Liabilities for 'short-term employee benefits' (as defined in AASB 119 *Employee Benefits*) and termination benefits due 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 2011-12 FMOs for Financial Reporting as at 30 June 2012. 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 and Deregulation's administered schedules and notes.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

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.

1.10 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.

1.11 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 (2010–11: 30 days).

Impairment of financial assets

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

1.12 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 the year ended 30 June 2012

Other Financial Liabilities

Other financial liabilities, including borrowings, are initially measured at fair value, net of transaction costs.

Other financial liabilities are subsequently measured at amortised cost using the effective interest method, with interest expense recognized on an effective yield basis.

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

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.

1.13 Contingent Liabilities and Contingent Assets

Contingent liabilities and contingent assets are not recognised in the balance sheet 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 2010-11 or in 2011-12.

No contingent rentals exist.

1.14 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.

1.15 Property, Plant and Equipment

Asset Recognition Threshold

Purchases of property, plant and equipment are recognised initially at cost in the balance sheet, 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 2010 by an independent valuer.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

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 – 47 years (2011: 1 – 47 years).

Impairment

All assets were assessed for impairment at 30 June 2012. 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.

1.16 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 (2011: 4 years).

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

1.17 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.

Note 2 – Events after the Balance Sheet Date

There are no significant events occurring after the Balance Sheet date requiring disclosure.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Note 3 – Expenses

	2012	2011
	\$	\$
<u>Note 3A – Employee Benefits</u>		
Wages and salaries	1 453 498	1 448 729
Superannuation:		
Defined benefit plans	210 819	178 271
Defined contribution plans	50 392	36 790
Leave and other entitlements	326 893	309 383
Total employee benefits	2 041 602	1 973 173

	2012	2011
	\$	\$
<u>Note 3B – Suppliers</u>		
Goods and services		
Consultants	16 000	23 464
ICT support	46 000	46 000
Legal expenses	18 122	126 421
Printing non publications	1 394	3 980
Printing publications	16 006	13 215
Resources received free of charge:		
Notional Rent Charge	102 000	102 000
Notional Audit Fees	18 000	18 000
Notional IT Support Costs	79 756	4 590
Stationery	14 956	26 292
Training	17 985	16 234
Travel	59 990	26 228
Other	57 545	76 747
Total goods and services	447 754	483 171
Goods and services are made up of:		
Provision of goods – external entities	28 444	37 633
Rendering of services – related entities	263 631	203 689
Rendering of services – external entities	155 679	241 849
Total goods and services	447 754	483 171
Other supplier expenses		
Workers compensation premiums	3 239	3 232
Total other supplier expenses	3 239	3 232
Total supplier expenses	450 993	486 403

	2012	2011
	\$	\$
<u>Note 3C – Depreciation and Amortisation</u>		
Depreciation – Property, plant and equipment	33 799	16 065
Amortisation – Intangibles	-	-
Total depreciation and amortisation	33 799	16 065

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

	2012 \$	2011 \$
<u>Note 3D – Loss on Disposal of Assets</u>		
Infrastructure, plant and equipment	7 902	542
Total loss on disposal of assets	7 902	542

Note 4 – Income

OWN-SOURCE INCOME

	2012 \$	2011 \$
<u>Note 4A - Other</u>		
Inquiry Funding	183 470	291 367
Leave Liability Transfers	67 768	145 595
Employee FBT Contributions	16 839	-
Total other own-source income	268 077	436 962

GAINS

Note 4B – Other Gains

	2012 \$	2011 \$
Resources Received free of charge:		
Department of Prime Minister & Cabinet	102 000	102 000
Australian National Audit Office	18 000	18 000
Defence Signals Directorate	95 122	4 590
Total other gains	215 122	124 590

REVENUE FROM GOVERNMENT

Note 4C – Revenues from Government

	2012 \$	2011 \$
Appropriations:		
Departmental Appropriation	2 241 000	2 095 000
Total revenue from government	2 241 000	2 095 000

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Note 5 – Financial Assets

	2012	2011
	\$	\$
<u>Note 5A – Cash and cash equivalents</u>		
Cash on hand or on deposit	197 352	197 325
Total cash and cash equivalents	197 352	197 325

	2012	2011
	\$	\$
<u>Note 5B – Trade and other receivables</u>		

Appropriations receivable:		
For existing programs	1 891 659	1 803 973
Total appropriations receivable	1 891 659	1 803 973

Other Receivables:		
GST receivable from the Australian Taxation Office	711	5 842
Other receivables	374	-
Total other receivables	1 085	5 842
Total trade and other receivables (gross)	1 892 744	1 809 816

Less Impairment Allowance Account:		
Other	-	-
Total trade and other receivables (net)	1 892 744	1 809 816

Receivables are aged as follows:		
Not overdue	1 892 744	1 809 816

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

Note 6 – Non-Financial Assets

Note 6A – Property, plant and equipment

	2012	2011
	\$	\$
<u>Property, plant and equipment</u>		
Other property, plant and equipment:		
- Fair value	165 059	93 310
- Accumulated depreciation	38 809	16 007
Total property, plant and equipment	126 250	77 303

All revaluations are independent and are conducted in accordance with the revaluation policy stated at Note 1.16. The most recent revaluation was conducted by the Australian Valuation Office as at 30 June 2010.

All assets were examined for indicators of impairment during the stocktake completed on 30 June 2012 and none were found. No items of property plant and equipment are expected to be sold or disposed of within the next 12 months.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Note 6B – Reconciliation of the Opening and Closing Balances of Property, Plant and Equipment (2011-12)

Item	Other property, plant & equipment \$	Total \$
As at 1 July 2011		
Gross book value	93 310	93 310
Accumulated depreciation and impairment	(16 006)	(16 006)
Net book value as at 1 July 2011	77 304	77 304
Additions		
by purchase	75 283	75 283
resources received free of charge	15 364	15 364
Depreciation expense	(33 799)	(33 799)
Disposals		
Other	(7 902)	(7 902)
Net Book Value 30 June 2012	126 250	126 250
Net Book Value as at 30 June 2012 represented by:		
Gross book value	165 059	165 059
Accumulated depreciation and impairment	(38 809)	(38 809)

Note 6B (cont'd) – Reconciliation of the Opening and Closing Balances of Property, Plant and Equipment (2010-11)

Item	Other property, plant & equipment \$	Total \$
As at 1 July 2010		
Gross book value	52 325	52 325
Accumulated depreciation and impairment	-	-
Net book value as at 1 July 2010	52 325	52 325
Additions		
by purchase	41 585	41 585
Depreciation expense	(16 065)	(16 065)
Disposals		
Other	(541)	(541)
Net Book Value 30 June 2011	77 304	77 304
Net Book Value as at 30 June 2011 represented by:		
Gross book value	93 310	93 310
Accumulated depreciation and impairment	(16 006)	(16 006)

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Note 6C – Intangibles

	2012 \$	2011 \$
Computer software:		
Purchased	-	5 769
Total computer software	-	5 769
Accumulated amortisation	-	(5 769)
Total intangibles	-	-

Note 6D – Reconciliation of the Opening and Closing Balances of Intangibles (2011-12)

Item	Computer Software Purchased \$	Total \$
As at 1 July 2011		
Gross book value	5 769	5 769
Accumulated amortisation & impairment	(5 769)	(5 769)
Net book value as at 1 July 2011	-	-
Additions		
by purchase or internally developed	-	-
Amortisation expense	-	-
Disposals		
Net cost of disposals	-	-
Net Book Value 30 June 2012	-	-
Net Book Value as at 30 June 2012 represented by:		
Gross book value	-	5 769
Accumulated amortisation & impairment	-	(5 769)

The intangible assets were disposed of at nil value during 2011-12.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Note 6D (cont'd) – Reconciliation of the Opening and Closing Balances of Intangibles (2010-11)

Item	Computer Software Purchased \$	Total \$
As at 1 July 2010		
Gross book value	5 769	5 769
Accumulated depreciation	(5 769)	(5 769)
Net book value as at 1 July 2010	-	-
Additions		
by purchase or internally developed	-	-
Depreciation expense	-	-
Disposals		
Net cost of disposals	-	-
Net Book Value 30 June 2011		
Net Book Value as at 30 June 2011 represented by:	-	-
Gross book value		
Accumulated depreciation	5 769	5 769
	(5 769)	(5 769)

2012   2011
\$ \$

Note 6E – Other Non-Financial Assets

Prepayments	1 184	556
Total other non-financial assets	1 184	556

Note 7 – Payables

2012   2011
\$ \$

Note 7A – Suppliers

Trade creditors and accruals	19 562	139 067
Total suppliers	19 562	139 067

Supplier payables expected to be settled within 12 months:

Related entities	8 045	90 613
External parties	11 517	48 454
Total	19 562	139 067

Supplier payables expected to be settled in greater than 12 months:

Related entities	-	-
External parties	-	-
Total	-	-
Total supplier payables	19 562	139 067

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

	2012 \$	2011 \$
<u>Note 7B – Other Payables</u>		
Salaries and wages	43 208	34 616
Superannuation	7 073	5 564
Unearned Revenue	-	183 470
Total other payables	50 281	223 651

Total other payables are expected to be settled in:

No more than 12 months	50 281	223 651
Total other payables	50 281	223 651

Note 8 – Provisions

	2012 \$	2011 \$
<u>Note 8A – Employee Provisions</u>		
Leave	783 223	556 721
Total employee provisions	783 223	556 721

Employee provisions are expected to be settled in:

No more than 12 months	80 220	55 640
More than 12 months	703 003	501 081
Total employee provisions	783 223	556 721

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Note 9 – Cash Flow Reconciliation

	2011-12 \$	2010-11 \$
Reconciliation of Cash and cash equivalents as per Balance Sheet to Cash flow statement		
Report cash and cash equivalents as per:		
Cash Flow Statement	197 352	197 326
Balance Sheet	197 352	197 326
Difference	-	-
Reconciliation of net cost of services to net cash from operating activities:		
Net cost of services	(2 051 097)	(1 914 631)
Add revenue from Government	2 241 000	2 095 000
Less income tax expense		
Adjustments for non-cash items		
Depreciation/amortisation	33 799	16 065
Gain/Loss on disposal of assets	7 902	542
Write-off of assets		-
RRFOC income – offsetting expense capitalised	(15 366)	-
Changes in assets/liabilities		
Increase/(Decrease) in provision for employee liabilities	226 502	126 310
Increase (Decrease) in other payables	(173 370)	193 795
Increase/(Decrease) in supplier trade creditors	(119 504)	89 427
(Increase)/Decrease in appropriations receivables	(153 969)	(554 720)
(Increase)/Decrease in other assets	(374)	2 514
(Increase)/Decrease in other prepayments	(628)	(556)
(Increase)/Decrease in GST receivable	5 131	872
(Increase)/Decrease in transfers to the Official Public Account	-	
Net cash from (used by) operating activities	26	54 618

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Note 10 – Senior Executive Remuneration

Note 10A – Senior Executive Remuneration Expense for the Reporting Period

	2012 \$	2011 \$
Short-term employee benefits:		
Salary	337 395	328 119
Annual leave accrued	<u>25 840</u>	<u>18 360</u>
Total short-term employee benefits	<u>363 235</u>	<u>346 479</u>
Post-employment benefits:		
Superannuation	<u>57 071</u>	48 338
Total post-employment benefits	<u>57 071</u>	<u>48 338</u>
Other long-term benefits:		
Long service leave	<u>47 758</u>	54 636
Total other long-term benefits	<u>47 758</u>	<u>54 636</u>
Termination benefits	<u>468 064</u>	<u>449 453</u>
Total employment benefits	<u>468 064</u>	<u>449 453</u>

Notes:

1. Note 11A was prepared on an accrual basis.
2. Note 11A excludes acting arrangements and part-year service where remuneration expensed for senior executive was less than \$150,000.
3. Note 11A relates to senior executives employed during the year.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Note 10B – Average Annual Reportable Remuneration Paid to Substantive Senior Executives During the Reporting Period

	2012					
	Average annual reportable remuneration ¹	Senior Executives No.	Reportable Salary ² \$	Contributed Superannuation ³ \$	Reportable Allowances ⁴ \$	Bonus Paid ⁵ \$
Total remuneration (including part-time arrangements):						
Less than \$150,000	1		66 968	11 187	0	0
\$390,000 to \$419,999	1		291 219	98 880	666	0
Total	2		358 187	110 067	666	0
						78 155
						390 765
						468 920

	2011					
	Average annual reportable remuneration ¹	Senior Executives No.	Reportable Salary ² \$	Contributed Superannuation ³ \$	Reportable Allowances ⁴ \$	Bonus Paid ⁵ \$
Total remuneration (including part-time arrangements):						
\$200,000 to \$229,999	1		184 402	27 726	0	0
\$360,000 to \$389,999	1		280 811	89 463	751	0
Total	2		465 213	117 189	751	0
						212 128
						371 025
						583 153

Notes:

- This table reports substantive senior executives who received remuneration during the reporting period. Each row is an averaged figure based on headcount for individuals in the band.
- 'Reportable salary' includes the following:
  - gross payments (less any bonuses paid, which are separated out and disclosed in the 'bonus paid' column);
  - reportable fringe benefits (at the net amount prior to 'grossing up' to account for tax benefits); and
  - exempt foreign employment income.
- The 'contributed superannuation' amount is the average actual superannuation contributions paid to senior executives in that reportable superannuation band during the reporting period, including any salary sacrificed amounts.
- 'Reportable allowances' are the average actual allowances paid as per the 'total allowances' line on individuals' payment summaries.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

5. 'Bonus paid' represents average actual bonuses paid during the reporting period in that reportable remuneration band. The 'bonus paid' within a particular band may vary between financial years due to various factors such as individuals commencing with or leaving the entity during the financial year.
6. Various salary sacrificing arrangements were available to senior executives including superannuation, motor vehicle and expense payment fringe benefits. Salary sacrifice benefits are reported in the 'reportable salary' column, excluding salary sacrificed superannuation, which is reported in the 'contributed superannuation' column.
7. The comparative figures have been revised and do not match what was published in the 2010-11 financial statements due to new disclosure requirements.

Note 10C – Other Highly Paid Staff

	Staff No.	2012				Total \$
		Reportable Salary ² \$	Contributed Superannuation ³ \$	Reportable Allowances ⁴ \$	Bonus Paid ⁵ \$	
Average annual reportable remuneration ¹						
time arrangements;						
\$150,000 to \$179,999	2	118 894	32 733	0	0	151 627
Total	2	118 894	32 733	0	0	151 627

	Staff No.	2011				Total \$
		Reportable Salary ² \$	Contributed Superannuation ³ \$	Reportable Allowances ⁴ \$	Bonus Paid ⁵ \$	
Average annual reportable remuneration ¹						
time arrangements;						
\$150,000 or greater	Nil	-	-	-	-	-
Total						

Notes:

1. This table reports staff:
  - a) who were employed by the entity during the reporting period;
  - b) whose reportable remuneration was \$150,000 or more for the financial period; and
  - c) were not required to be disclosed in Tables A, B or director disclosures.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Each row is an averaged figure based on headcount for individuals in the band.

2. 'Reportable salary' includes the following:
  - a) gross payments (less any bonuses paid, which are separated out and disclosed in the 'bonus paid' column);
  - b) reportable fringe benefits (at the net amount prior to 'grossing up' to account for tax benefits); and
  - c) exempt foreign employment income.
3. The 'contributed superannuation' amount is the average actual superannuation contributions paid to staff in that reportable remuneration band during the reporting period, including any salary sacrificed amounts.
4. 'Reportable allowances' are the average actual allowances paid as per the 'total allowances' line on individuals' payment summaries.
5. 'Bonus paid' represents average actual bonuses paid during the reporting period in that reportable remuneration band. The 'bonus paid' within a particular band may vary between financial years due to various factors such as individuals commencing with or leaving the entity during the financial year.
6. Various salary sacrificing arrangements were available to other highly paid staff including superannuation, motor vehicle and expense payment fringe benefits. Salary sacrifice benefits are reported in the 'reportable salary' column, excluding salary sacrificed superannuation, which is reported in the 'contributed superannuation' column.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Note 11 – Remuneration of Auditor

Financial statement audit services were provided free of charge to OIGIS by the Australian National Audit Office (ANAO).

Fair value of the services provided	2011-12	2010-11
Financial statement audit services	\$18 000	\$18 000

No other services were provided by the auditors of the financial statements.

Note 12 – Financial Instruments

Note 12A – Categories of Financial Instruments

Financial Assets	2011-12	2010-11
	\$	\$
Loans and Receivables		
Loans and receivables		
Cash and cash equivalents	197 352	197 325
Trade receivables	374	-
Carrying amount of financial assets	197 726	197 325
Financial Liabilities		
Other liabilities measured at amortised cost		
Payables – Suppliers	19 562	139 067
Carrying amount of financial liabilities	19 562	139 067

Note 12B – Net Income and Expense from Financial Assets

Loans and Receivables	2011-12	2010-11
	\$	\$
Interest Revenue	-	-
Net gain/(loss) from financial assets	-	-

Note 12C – Net Income and Expense from Financial Liabilities

Financial Liabilities – at amortised cost	2011-12	2010-11
Interest Expense	-	-
Net gain/(loss) from financial liabilities	-	-

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Note 12D – Fair Value of Financial Instruments

OIGIS's aggregate net fair values of (identified) financial instruments are the same as their carrying amounts.

Fair value measurements categorised by fair value hierarchy

	Level in the fair value hierarchy	
	2012	2011
Financial assets at fair value		
Cash and cash equivalents	1	1
Trade receivables	2	2
Financial liabilities at fair value		
Payables - Suppliers	2	2

There were no financial instrument transfers between levels during the year.

Note 12E – Credit Risk

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

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

Credit quality of financial instruments not past due or individually determined as impaired

	Not Past Due Nor Impaired 2012	Not Past Due Nor Impaired 2011	Past due or Impaired 2012	Past due or Impaired 2011
Loans & Receivables				
Cash and cash equivalents	197 352	197 325	-	-
Trade receivables	374	-	-	-
Total	197 726	197 325	-	-

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Note 12F – 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 due to appropriation funding and internal policies and procedures put in place to ensure there are appropriate resources to meet its financial obligations.

Maturities for non-derivative financial liabilities 2012					
	On Demand \$	Within 1 year \$	1 to 5 years \$	Greater than 5 years \$	Total \$
Other Liabilities at amortised cost					
Payables – Suppliers		19 562			19 562
Total		19 562			19 562
Maturities for non-derivative financial liabilities 2011					
	On Demand \$	Within 1 year \$	1 to 5 years \$	Greater than 5 years \$	Total \$
Other Liabilities at amortised cost					
Payables – Suppliers		139 067			139 067
Total		139 067			139 067

Note 12G – Market Risk

OIGIS holds only basic financial instruments that do not expose the agency to certain market risks.

Note 13 – Financial Asset Reconciliation

	2012 \$	2011 \$
<u>Financial Assets</u>		
Total financial assets as per balance sheet	2 090 096	2 007 141
Less: non-financial instrument components:		
Appropriations Receivable	1 891 659	1 803 973
GST Receivable	711	5 842
Total non-financial instrument components	1 892 370	1 809 815
Total financial assets as per financial instruments note	197 726	197 325

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

	Appropriation Act		2011 Appropriations				Appropriation applied in 2011 (current and prior years) \$	Variance \$
	Annual Appropriation \$	Appropriations Reduced ¹ \$	AFM ² \$	Section 30 \$	Section 31 \$	Section 32 \$	Total Appropriation \$	
DEPARTMENTAL								
Ordinary Annual Services	2 167 000	-	-	2 513	620 431	-	2 789 944	638 884
Other Services	-	-	-	-	-	-	-	-
Equity	-	-	-	-	-	-	-	-
Loans	-	-	-	-	-	-	-	-
Total Departmental	2 167 000	-	-	2 513	620 431	-	2 789 944	638 884

Notes:

- 1 Appropriations reduced under Appropriations Acts (No. 1, 3 & 5) 2010-11: sections 10, 11 and 12 and under Appropriation Acts (No. 2, 4 & 6) 2010-11: sections 12, 13, and 14. Departmental appropriations do not lapse at financial year-end. However, the responsible Minister may decide that part or all of a departmental appropriation is not required and request the Finance Minister to reduce the appropriation. The reduction in the appropriation is effected by the Finance Minister's determination and is disallowable by Parliament.
- 2 Advance to the Finance Minister (AFM) – Appropriation Acts (No. 1, 3 & 5) 2010-11: section 13 and Appropriation Acts (No. 2, 4 & 6) 2010-11: section 15.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Table B: Departmental Capital Budget ('Recoverable GST exclusive')

	2012 Capital Budget Appropriations				Capital Budget Appropriations applied in 2012 (current and prior years)			
	Appropriation Act		FMA Act		Payments for Non-financial Assets ³	Payments for other Purposes	Total Payments	Variance
	Annual Capital Budget	Appropriations reduced ²	Section 32	Total Capital Budget Appropriations				
Departmental								
Ordinary annual Services – Departmental Capital Budget ¹	9 000	-	-	9 000	20 283	-	20 283	(11 283)
	9 000	-	-	9 000	20 283	-	20 283	(11 283)

Notes:

- 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 Appropriations reduced under Appropriation Acts (No 1, 3, 5) 2011-12: sections 10, 11, 12 and 15 or via a determination by the Finance Minister.
- 3 Payments made for non-financial assets include purchases of assets, expenditure on assets which has been capitalised, costs incurred to make good an asset to its original condition, and the capital repayment of finance leases.

	2011 Capital Budget Appropriations				Capital Budget Appropriations applied in 2011 (current and prior years)			
	Appropriation Act		FMA Act		Payments for Non-financial Assets ³	Payments for other Purposes	Total Payments	Variance
	Annual Capital Budget	Appropriations reduced ²	Section 32	Total Capital Budget Appropriations				
Departmental								
Ordinary annual Services – Departmental Capital Budget ¹	72 000	-	-	72 000	41 585	-	41 585	30 415
	72 000	-	-	72 000	41 585	-	41 585	30 415

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Notes:

- 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 Appropriations reduced under Appropriation Acts (No 1, 3, 5) 2010-11: sections 10, 11, 12 and 15 or via a determination by the Finance Minister.
- 3 Payments made for non-financial assets include purchases of assets, expenditure on assets which has been capitalised, costs incurred to make good an asset to its original condition, and the capital repayment of finance leases.

Table C: Unspent Departmental Annual Appropriations ('Recoverable GST exclusive')

Authority	2012 \$	2011 \$
Appropriation Act (No 1) 2004-05	-	-
Appropriation Act (No 2) 2004-05	53 000	108 000
Appropriation Act (No 2) 2005-06	-	-
Appropriation Act (No 1) 2005-06	40 000	40 000
Appropriation Act (No 3) 2005-06	33 000	33 000
Appropriation Act (No 1) 2006-07	380 800	380 800
Appropriation Act (No 1) 2007-08	261 846	261 846
Appropriation Act (No 1) 2008-09	195 192	195 192
Appropriation Act (No 1) 2009-10	197 707	197 707
Appropriation Act (No 1) 2010-11	567 145	587 428
Appropriation Act (No 1) 2011-12	162 969	197 325
Cash	197 352	-
Total	2 089 011	2 001 298

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Note 15 – Special Accounts

Until 2009 OIGIS previously had two special accounts established under section 20 of the FMA Act. These accounts were:

- *Other Trust Moneys Account* (s20 FMA Act 1997). The purpose of this account was for expenditure of moneys temporarily held on trust or otherwise for the benefit of a person other than the Commonwealth, and
- *Services for Other Governments and Non-Agency Bodies Account* (s20 FMA Act 1997). The purpose of this account was for expenditure in connection with services performed on behalf of other Governments and bodies that are not FMA agencies.

These accounts have never been active. The Services for Other Commonwealth and Non-Agency Bodies Account was abolished on 11 September 2009 by Determination 2009/28 issued by the Minister for Finance and Deregulation. The Other Trust Moneys Account was abolished on 12 October 2010 by Determination 2010/13 issued by the Minister for Finance and Deregulation.

Note 16 – Compensation and Debt Relief

No 'Act of Grace' payments were expensed during the reporting period, (2010-11: nil).

No waivers of amounts owing to the Australian Government were made pursuant to subsection 34(1) of the *Financial Management and Accountability Act 1997* during the reporting period, (2010-11: nil).

No payments were made under the 'Defective Administration Scheme' during the reporting period, (2010-11: nil).

No ex-gratia payments were provided for during the reporting period, (2010-11: nil).

No payments were made under section 73 of the *Public Service Act 1999*, (2010-11: nil).

Note 17 - Reporting of Outcomes

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

Note 17A – Net Cost of Outcome Delivery

	Outcome 1		Total	
	2012	2011	2012	2011
	\$	\$	\$	\$
Departmental				
Expenses	2 534 296	2 476 183	2 534 296	2 476 183
Own-source income	483 199	561 552	483 199	561 552
Net cost/(contribution) of outcome delivery	2 051 097	1 914 631	2 051 097	1 914 631

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2012

Note 18 – Net Cash Appropriation Arrangements

	2012 \$	2011 \$
Total Comprehensive Income (loss) less depreciation/amortisation expenses previously funded through revenue appropriations¹	156 104	164 304
Plus depreciation/amortisation expenses previously funded through revenue appropriation	33 799	16 065
Total comprehensive income (loss) as per the Statement of Comprehensive Income	189 903	180 369

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.

PART FIVE: ANNEXURES

Annex 1: Summary of Inquiries and Complaints

Table 1.1
IGIS Act Inquiries actioned between 1 July 2011 and 30 June 2012

Agency	Source	Date initiated	Type of inquiry	Date finalised	Duration (days)
All AIC agencies, PM&C, DFAT, AGD and AFP	Prime Minister	04/01/11	Full	19/12/11	349
DSA	Prime Minister	01/06/11	Full	23/12/11	206
ASIS	Public	29/08/11	Preliminary	25/10/11	57
ASIO	Employee	25/10/11	Preliminary	10/11/11	16
ASIO	IGIS	01/11/11	Full	29/06/12	242
ASIS	Public	25/10/11	Full	02/04/12	160
DSD/DIGO/DIO	Minister for Defence	28/11/11	Full	14/06/12	199
ASIO	Public	18/01/12	Preliminary	21/05/12	125
ASIO	Employee	05/03/12	Preliminary	06/06/12	94

Table 1.2
Summary of complaints handled administratively by OIGIS between 1 July 2011 and 30 June 2012

Agency	Number of complaints	From public	From AIC employee or ex-employee
ASIO (general)	8	6	2
ASIO (visa security assessments)	430	430	0
ASIS	1	0	1
DSD	0	0	0
DIGO	0	0	0
DIO	0	0	0
ONA	0	0	0
AIC (all)	0	0	0
TOTAL COMPLAINTS	439	436	3

Annex 2: Salary ranges for APS Employees in OIGIS in 2011-12

OIGIS Band	APS Level	Salary Range 1 July 2011 – 30 June 2012 (\$)
SES Band 1	SES Band 1	171 657
OIGIS Band 4	EL2	126 277
		123 288
		120 895
		112 181
		106 102
OIGIS Band 3	EL1	101 621
		98 629
		91 158
OIGIS Band 2	APS6	84 808
		82 193
		79 204
		75 467
		71 732
	APS5	70 236
		68 367
		66 128
		64 633
		62 764
	APS4	61 272
		59 403
	APS3	57 534
		56 040
		54 545
		53 426
OIGIS Band 1	APS2	51 930
		50 437
		48 194
		46 699
		45 580
	APS1	43 711
		42 591
		42 547

Annex 3: Agency resource statements

Table 3.1
Agency Resource Statement and Resources for Outcomes 2011-12

		Actual available appropriation for 2011-12 \$'000 (a)	Payments made 2011-12 \$'000 (b)	Balance remaining 2011-12 (a) – (b)
Ordinary Annual Services				
Departmental Appropriation				
Prior year departmental appropriation		1 893	20	1 873
Departmental appropriation		2 250	2 200	50
S31 Relevant Agency Receipts		113	–	113
Total		4 256	2 220	2 036
Administered expenses		–	–	–
Total		–	–	–
Total ordinary annual services	A	4 256	2 220	2 036
Other services				
Departmental non-operating		108	55	53
Total		108	55	53
Total other services	B	108	55	53
Total available annual appropriations		4 364	2 275	2 089
Special appropriations		–	–	–
Total special appropriations	C	–	–	–
Special accounts		–	–	–
Total special accounts	D	–	–	–
Total resourcing A + B + C + D		4 364	2 275	2 089
Less appropriations drawn from annual or special appropriations above and credited to special accounts and/or CAC Act bodies through annual appropriations		–	–	–
Total net resourcing for agency		4 364	2 275	2 089

Table 3.2
Expenses and Resources for Outcome 1

Outcome 1: Independent assurance for the Prime Minister, senior ministers and Parliament as to whether Australia's intelligence and security agencies act legally and with propriety by inspecting, inquiring into and reporting on their activities	Budget 2011-12 \$'000 (a)	Actual expenses 2011-12 \$'000 (b)	Variation 2011-12 \$'000 (a) – (b)
Program 1.1: Office of the Inspector-General of Intelligence and Security			
Departmental expenses			
Ordinary annual services (Appropriation Bill No.1)	2 241	2 241	–
Revenue from independent sources			
Special appropriations			
Special Accounts			
Expenses not requiring appropriation in the Budget year	245	483	(238)
Total for Program 1.1	2 486	2 724	(238)
Outcome 1 Totals by appropriation type			
Departmental expenses			
Ordinary annual services (Appropriation Bill No.1)	2 241	2 241	–
Revenue from independent sources			
Special appropriations			
Special Accounts			
Expenses not requiring appropriation in the Budget year	245	483	(238)
Total expenses for Outcome 1	2 486	2 724	(238)
	Budget 2011-12	Actual 2011-12	
Average Staffing Level (number)	13	13	–

Annex 4: Inquiry into ASIO's security assessments for community detention determinations

Abridged report

ASIO provides security assessments to the Department of Immigration and Citizenship (DIAC) including recommendations to be provided to the Minister for Immigration and Citizenship about an individual irregular maritime arrival's eligibility for community detention. The number of requests for these assessments has increased rapidly since late 2010. The outcome of such an assessment has a profound effect on a detainee: an adverse recommendation means that a person cannot be transferred to a community detention arrangement and must remain in an immigration detention centre. In late 2011 I decided to inquire into the process by which ASIO conducts these community detention security assessments.

The activities of DIAC do not come under the ordinary jurisdiction of the IGIS, but the nature and extent of interaction between DIAC and ASIO are matters which are relevant to this inquiry.

Issues identified in the inquiry

The issues below arose following consideration of the relevant legal and policy framework and ASIO's procedures and internal policies. The inquiry also examined in detail seven more complex cases where ASIO was required to provide a security assessment for community detention purposes.

Procedural fairness

At the time this inquiry commenced, when ASIO made a decision to recommend that a person not be placed in community detention. ASIO did not first provide any opportunity for the individual to comment on any of the material adverse to them. In my view, this practice was not consistent with good decision making and the requirements of procedural fairness.

In January 2012 following initial discussions with my office, ASIO changed its community detention

security assessment process. An assessment recommending against community detention is now only issued in cases where an adverse security assessment has either already been approved by the Director-General, or where such an assessment is in the final stages of being drafted, and the person concerned has been assessed as posing a direct, or indirect, threat to security.

Given the process for issuing an adverse security assessment in this situation includes a requirement for ensuring that some level of procedural fairness is afforded, this revised process for community detention assessments does not raise the same level of procedural fairness concerns which existed prior to this change.

I make no formal recommendation in respect of procedural fairness considerations but note that, in my view, it is important that in each individual case, prior to making an adverse assessment, ASIO actively consider how much potentially adverse material can be put to the person without prejudicing national security.

There is a risk that ASIO officers may fall into error if they do not recognise that procedural fairness requires that ASIO must put to the individual as much of the potentially adverse material as security permits. Over-reliance on a standard process, for example by only inviting a person to comment on general issues at interview, may mean that insufficient consideration is given to the specific case at hand and the specific security risks associated with disclosing potentially adverse information in that particular case.

I am aware that the High Court has recently heard the case of *M47/2012 v Director-General of Security*. I understand that one aspect of this matter involves the issue of procedural fairness in security assessments. The judgment in this case had not been handed down at the time this inquiry was finalised.

Coordination and communication between DIAC and ASIO

Concerns about coordination and communication between ASIO and DIAC arose in several of the case studies.

Ministerial Guidelines relating to the power of the Minister for Immigration and Citizenship to allow an individual to be transferred to community detention give scope for a range of detention placement options to be utilised. Whereas a visa to live permanently in Australia cannot be issued if a person is assessed to be directly or indirectly a risk to security, the Minister may allow a person to be transferred to community detention if they are satisfied it is in the public interest. When making this decision the Guidelines provide that the Minister will take into account a wide range of factors, including security and welfare issues, and any other exceptional or unique characteristics or circumstances in the particular case. A person who is allowed community detention is obliged to comply with any conditions that are set by the Minister.

The Minister requires DIAC to provide a submission setting out the circumstances of the individual case, the reasons why community detention is considered appropriate, and a risk assessment based on the particular circumstances of the case. The submission to the Minister should also detail conditions that could be applied and proposed accommodation and support arrangements.

In cases where ASIO has assessed someone to be a risk to security, ASIO currently advises DIAC by way of a simple statement recommending that the Minister should not exercise their powers to allow community detention as it would not be 'in the public interest' to do so. No further information is provided. Currently such a case would not routinely be considered by the Minister. Thus the decision is in effect based only on ASIO's security assessment. This process tends to conflict with the Ministerial guidelines which require the balancing of a number of factors in the public interest test, together with the consideration of conditions to address potential risks.

In my view, it would not usually be appropriate for ASIO to consider a person's health, welfare or vulnerability when assessing whether they are a risk to security: the security assessment should be objective.

It is also not ASIO's role to develop arrangements that would balance any health or welfare concerns for individuals that ASIO regards to be a risk to security. However, ASIO has a broader statutory function 'to advise Ministers and authorities of the Commonwealth in respect of matters relating to security, in so far as those matters are relevant to their functions and responsibilities' (s 17(1)(c) of the *Australian Security Intelligence Organisation Act 1979*). I believe it would be consistent with this provision for ASIO to advise DIAC on conditions that might be applied to those individuals and how such conditions might serve to mitigate the risk to security. This would allow DIAC officers to appropriately advise the Minister so that all relevant factors can be considered.

In my view, this requirement would not necessarily be satisfied merely by providing the security assessment and the grounds for the assessment to DIAC. Further dialogue between ASIO and DIAC is required to provide a proper basis for DIAC to devise risk mitigation strategies and conditions.

I understand that this additional function is not currently resourced or funded within ASIO but believe that its application would be limited to those vulnerable detainees where DIAC has significant concerns about their welfare if they were to remain in an immigration detention centre. It is also possible that a whole-of-government approach, including a modest increase in funding to ASIO to fulfil this function, could result in a reduction in detention centre costs as well as contribute to better longer-term health outcomes.

I have been advised by ASIO that this issue is currently the subject of interagency discussions.

Recommendation 1

In cases where ASIO issues an adverse security assessment for community detention but where DIAC has identified significant health, welfare or other exceptional issues, ASIO should engage in a dialogue with DIAC so the Minister for Immigration and Citizenship can be advised on possible risk mitigation strategies and conditions with which a person allowed community detention might be required to comply.

In responding to this recommendation, the Acting Director-General of Security advised the inquiry that ASIO:

... believe[s] there could be unintended consequences in regard to this recommendation as the underpinning commentary appears to propose a new or expanded role for ASIO in which it would become involved in issues relating to conditions for community-based immigration detention.

... [If requested for input by DIAC] ASIO would need to carefully consider the legality appropriateness/competence and resource implications of ASIO assuming authority in this area. There may also be concerns about possible restrictions placed on individuals' civil liberties and questions about whether such conditions can be challenged on appeal.

In response to my draft report ASIO advised further that:

You are aware of ASIO's concern that Recommendation 1 of the report proposes a role for ASIO which might be outside of its current legislative remit ...

ASIO also notes that such advice would likely constitute a further security assessment and the resource implications of this, including responding to any legal challenges, could be significant. I note however that merits review of security assessments does not currently extend to non-citizens.

Notwithstanding the complexity of the issues, ASIO concludes that it is 'open to dialogue with DIAC should the department wish to pursue this proposal with us'. The Acting Secretary of DIAC agreed that the approach suggested might help improve the management of some sensitive cases.

The scope of this inquiry and recommendations is limited to security assessments for community detention. The proposed provision by ASIO of advice on risk mitigation strategies and conditions as recommended above apply only in that context. It is possible, however, that a similar strategy could be explored more broadly in situations where a visa applicant has received an adverse security assessment and is facing an indefinite period in a detention centre.

I understand the implementation of any proposal of this type could be contingent upon the reallocation of resources by Government, but believe that modest funding in this area could significantly benefit a small number of vulnerable individuals who might otherwise be kept in an immigration detention centre for an indefinite period (with all of the financial and other costs attendant upon such an action).

Recordkeeping

I requested that ASIO provide all holdings relating to the decision making around a sample of cases where requests for security assessments for community detention had been received. The inquiry noted some deficiencies in recordkeeping, or circumstances where it was not easy to follow the decision making pathway in respect of individual cases.

For example, in one case study a recommendation against community detention was made because of an administrative error but the error was not identified for two months. In this case the individual may have been kept in an immigration detention centre longer than necessary. If the ASIO assessor had been required to record clear and unambiguous reasons to support the recommendation against community detention, the error might have been identifiable at an earlier stage.

The formal decision should form part of the official record for each individual and state the basis for the recommendation against the individual being placed in community detention. In cases where no security concerns are identified, a simple statement to that effect could suffice.

Recommendation 2

ASIO should ensure that records of decision making in respect of all security assessments are clear and unambiguous, explicitly setting out what decision has been made, by whom, and the basis for the assessment.

I have been advised that ASIO agrees with this recommendation, and continues to focus on clear recording of decision making without imposing unnecessarily burdensome administrative processes.

Policy and training documentation

ASIO provided notes and slide presentations to the inquiry from courses conducted in-house including on mental health and cultural issues. While the training covered some relevant mental health issues, no comprehensive written guidance was provided.

Recommendation 3

ASIO should ensure that its policy and training documents in relation to custodial interviews are consistent, current and relevant, particularly regarding mental health considerations.

I have been advised that ASIO agrees with this recommendation and is reviewing policy and support for staff in respect of security assessment interviews and more generally for interviews of individuals where there may be mental health considerations.

Annex 5: Inquiry into allegations of inappropriate vetting practices in the Defence Security Authority and related matters

Executive summary

On 16 May 2011 three former contractors who had been employed as data-entry operators in Defence Security Authority's (DSA's) Brisbane-based vetting operation made allegations on the ABC *Lateline* program of inappropriate vetting practices. The Prime Minister requested the Inspector-General of Intelligence and Security to inquire into the allegations. The inquiry commenced in June 2011.

The inquiry focussed on the allegations of inappropriate vetting practices rather than the human resource management issues that were also raised. Following the *Lateline* disclosure several former and current staff members came forward with further information. The three complainants were interviewed as well as a number of current and former DSA employees and contractors and the inquiry had regard to a wide range of information including systems audits.

Evidence provided to the inquiry confirmed that the substance of the allegations was true: incorrect data had been inserted in the vetting process. Difficulties in uploading data led to the use by vetting staff of 'workarounds' to address both database incompatibilities and situations where an applicant had not provided all of the data required. This corrupted data had then entered the Australian Security Intelligence Organisation (ASIO) and was used for security assessments. The practice was not confined to the three complainants; most if not all staff used workarounds to some extent. There was a wide variation in the use of incorrect data and little by way of documentation. Further, except in limited circumstances, the use of the modified data had not been agreed by ASIO. There was also no support for the suggestion that this data was used as a place marker to be corrected at a later stage.

In the course of the inquiry other practices and incidents, unrelated to data entry, were also identified which were not consistent with good administrative practice.

While there was no evidence that there had been any attempt to subvert or mislead the security clearance process, the report identifies a number of contributing factors that led to these practices including:

- delayed and inadequate systems upgrades
- inadequate formal documentation and manuals
- inadequate training for contractors and APS staff
- the use of delegates who had not completed formal qualifications
- poor systems and process change management
- inadequate quality assurance
- inadequate management oversight and contractual arrangements
- sustained pressure for output following increases in demand.

The Inspector-General found that the integrity of data in both DSA and ASIO had been undermined if not compromised. Modified data entered the databases and some persists today.

The ASIO security assessment is one part of a broader assessment of a person's suitability to hold a clearance. For high-level clearances the process involves a personal interview, multiple referee checks, intrusive financial checks, police record checks and often a psychological interview. This thorough assessment process is designed to pick up issues of security concern. As the data relating to an individual primary applicant would usually be

accurate and complete and was less likely to have been modified, most of the overall clearance process would not be affected by these changes in data.

It was not possible for the inquiry to determine whether any particular ASIO security assessment had been compromised. The extensive remediation work currently underway in DSA should identify whether any cases exist.

Although lack of management oversight contributed to the problems in DSA, the Inspector-General did not form the opinion that there was sufficient evidence that any person was guilty of a breach of duty or of misconduct to justify referral to the Secretary of the Department of Defence.

The Inspector-General noted that senior executive officers hold leadership positions of special responsibility and accountability. While acknowledging the workload at the time she observed that although it may be appropriate for senior executive officers to rely on the advice of subordinate officers to some extent, this does not diminish the individual personal responsibility or accountability of individual senior executive officers. In particular, senior executive officers cannot rely only on information they receive – they also need to actively assure themselves in whatever way they can that advice is complete and accurate and that they understand its significance.

The Department of Defence has advised that remedial action is underway. The Australian Government Security Vetting Agency (AGSVA) has commenced validation of information required for ASIO security assessments granted since 2009. If validation identifies that information has been changed without justification then the correct information will be obtained from the clearance holder and provided to ASIO under an agreed data remediation strategy. The nature of any data discrepancies may require clearances of concern to be revalidated by AGSVA and ASIO. All vetting documentation is now being reviewed to ensure that it is authorised and fit for purpose, is applied consistently and is readily available to all staff.

On the basis that this remediation work will be conducted expeditiously, the Inspector-General makes no further recommendations relating to remediation of existing security clearances.

Potentially the most significant outstanding issue is that remediation will not resolve all data issues – particularly those relating to the unauthorised and unaudited access to the current electronic vettee pack where it seems likely that it will not be possible to identify the missing or inaccurate information. Defence advises that IT fixes should resolve known problems with transferring data between systems. Defence is also limiting access to a mechanism that potentially allows unaudited changes to vettee information to a very small number of authorised staff.

The Inspector-General also makes no recommendations in relation to a review of management structure noting that this is being considered as part of an internal Defence review.

In the *Lateline* program the complainants alleged that they had raised data integrity issues in previous DSA reviews. Although such issues were raised in reviews focussed on staff management issues, the warning signs were not heeded by senior management.

Defence has accepted all recommendations.

Recommendations

Recommendation 1

The Department of Defence should write to the three *Lateline* complainants and acknowledge that their allegations in respect of data-entry were true.

Recommendation 2

The AGSVA should review the adequacy of its IT systems user controls and audit capability and take appropriate remedial actions where necessary.

Recommendation 3

The Defence Chief Audit Executive should review and report annually on the AGSVA's compliance with all applicable Government security vetting policies, with the first review to be completed by 30 June 2012. The results of the reviews should be reported in Defence's annual report. The need for annual reviews should be reconsidered after three years.

Recommendation 4

All business processes, policies and procedures, including any workarounds, should be appropriately documented and be in accordance with the relevant legislative requirements. Documentation should be formally authorised by DSA management, endorsed by ASIO (where relevant), and subject to version control. Documents should be readily available, and appropriate for their purpose and audience.

Recommendation 5

A comprehensive Training Needs Analysis should be conducted in the AGSVA and a structured training program introduced to cover all aspects of training from induction to ongoing development and education, with a view to professionalising the vetting workforce.

Recommendation 6

All staff involved in vetting in the AGSVA, up to and including EL2 level officers, should be required to hold a recognised qualification in security vetting. Qualifications held by staff should be appropriately confirmed and recorded in the relevant IT systems.

Recommendation 7

The AGSVA should formalise change-management processes for policies, procedures, and systems. Changes should be appropriately communicated, centrally-recorded and adequate resources allocated to training programmes.

Recommendation 8

The AGSVA should implement a Quality Management System to cover the full-range of activities involved in a security clearance process.

Recommendation 9

Defence should review contracting arrangement in the National Coordination Centre with the aim of ensuring that contract personnel can be subject to appropriate APS management oversight and that all staff can be subject to common policies, procedures, training and performance management including being held to the same standard of conduct.

Recommendation 10

Defence should review whether the staffing numbers for the NCC/AGSVA are adequate given the growth in security clearance requirements within the Australian Government in recent years and the failure of systems to deliver projected productivity improvements.

Recommendation 11

The implementation of PSAMS2 should be given a high priority in Defence's ICT program.

Recommendation 12

The AGSVA should work with ASIO as a matter of urgency to resolve the outstanding data transfer compatibility issues and agree and document any appropriate workarounds.

Recommendation 13

When a clearance is due for re-evaluation, the vettee should be explicitly notified that the data may be corrupt and informed of their obligation to correct it.

Annex 6: Inquiry into the actions of Australian government agencies in relation to the arrest and detention overseas of Mr Mamdouh Habib from 2001 to 2005

Executive summary and findings

Mr Mamdouh Ahmed Habib is a dual Australian-Egyptian national who was detained in Pakistan in October 2001. Australian government agencies believe that, after a period of detention in Pakistan, he was transferred to Egypt in November 2001. In April 2002 Mr Habib was transferred to the Afghan city of Bagram en route to the US Naval Base in Guantanamo Bay, Cuba. Mr Habib was held at Guantanamo Bay until his release into the community in Australia in January 2005.

Following his release, Mr Habib initiated Federal Court proceedings against the Commonwealth in relation to the actions of Australian government officials during his period of detention. This action was settled in December 2010.

In December 2010 the Prime Minister requested the Inspector-General of Intelligence and Security to conduct an inquiry into the actions of Australian intelligence agencies in relation to the arrest and detention overseas of Mr Habib from 2001 to 2005. The Prime Minister also requested that the inquiry cover the actions of the Department of Foreign Affairs and Trade (DFAT) and the Australian Federal Police (AFP) relevant to this intelligence and security matter. The Prime Minister requested the inquiry also explore the implications for the involvement of Australian intelligence and law enforcement agencies, as well as for DFAT, in matters relating to Australians detained in foreign countries.

In February 2011, the Prime Minister expanded the scope of the inquiry at the request of the Inspector-General to include the actions of the Attorney-General's Department (AGD) and the Department of the Prime Minister and Cabinet (PM&C).

The inquiry considered many thousands of pages of documents and twenty-four current or former Commonwealth officers were formally interviewed. Mr Habib was also interviewed and given the opportunity to provide information.

The inquiry also considered the adequacy of agencies' policies and practices at the time of Mr Habib's arrest and detention, as well as any changes since that time. The Prime Minister requested that due weight be given to the potential impact of any recommendations on the future effectiveness of the intelligence community in supporting Australia's national security, notably in operations overseas and in relations with foreign agencies.

The Inspector-General makes a number of recommendations in respect of consular responsibilities, the passage of information to foreign authorities, and on the prohibition on the use of, or involvement in, torture or other cruel, inhuman or degrading treatment or punishment.

The report acknowledges that there have been considerable changes in the way that Australian government agencies manage national security matters over the last ten years, including the creation of the role of National Security Adviser. It also notes that an Interdepartmental Committee would be established in future to manage any situation where an Australian citizen is detained overseas on suspicion of terrorism. The Inspector-General considers these arrangements to be satisfactory and therefore makes no recommendations in respect of clarifying whole-of-government responsibilities.

The Inspector-General found that communication to the Habib family in respect of Mr Habib's welfare was not adequate and recommends that an apology be made.

Key findings

The intelligence case against Mr Habib

1. On 13 September 2001 credible information was obtained that Mr Mamdouh Habib may have had prior knowledge of the September 11 terrorist attacks.
2. From that time until approximately April 2002, Australian government agencies and foreign governments considered that there was an urgent need to clarify the extent of Mr Habib's prior knowledge and whether he was involved in planning for future attacks.
3. From April 2002, the Australian Security Intelligence Organisation (ASIO) was of the view that Mr Habib had not been involved in planning for future terrorist attacks. However, this assessment was not sufficient to secure his release from detention in either Afghanistan or Guantanamo Bay.
4. On 5 January 2005, Australia was advised that the US would not lay charges against Mr Habib. The Australian Attorney-General and the Minister for Foreign Affairs noted in a joint media release on 11 January 2005 that 'it remained the strong view of the United States that, based on information available to it, Mr Habib had prior knowledge of the terrorist attacks on or before 11 September 2001. Mr Habib has acknowledged he spent time in Afghanistan, and others there at the time claim he trained with al-Qa'ida'. They noted further that 'Mr Habib remains of interest in a security context because of his former associations and activities'.
5. Australian officials were not involved in making arrangements for Mr Habib's transfer to Egypt and were not present at any time during his forced removal from Pakistan.
6. No Australian official accompanied Mr Habib on an aircraft from Pakistan to Egypt.
7. In Egypt (November 2001 to April 2002):
  - Mr Habib's place of detention was not known by Australian officials for the period of his detention
  - no Australian official attended Mr Habib's place of detention
  - no Australian official was present during interrogations of Mr Habib
  - in particular, Mr Habib was not seen by any officers from the Australian Embassy in Cairo, or persons identified by Mr Habib as ASIO officers named 'Stewart', 'Stuart' or 'David'.
8. ASIO should have made active enquiries about how Mr Habib would be treated in Egypt before providing information which may have been used in his questioning in Egypt.
9. Mr Habib's claim that he was questioned in Egypt about documents obtained during an ASIO search of his home is credible.
10. On arrival in Guantanamo Bay in May 2002, Mr Habib made various allegations about his treatment while in Pakistan and Egypt. It is not apparent that the Australian government agencies made immediate inquiries of the US, Pakistan or Egyptian Governments at that time with respect to Mr Habib's allegations of mistreatment.

Action of Australian officials in relation to Mr Habib's detention in Egypt and Pakistan

5. In Pakistan (October to November 2001), the only Australian officials to see Mr Habib were one ASIO officer and one AFP officer. Neither of these officers:
  - engaged in acts of mistreatment of Mr Habib or had knowledge of any actual or intended mistreatment by others
  - made threats that Mr Habib's Australian citizenship would be rescinded
  - made threats that Mr Habib's family would be harmed
  - made threats that Mr Habib would be sent to Egypt.
12. DFAT's administrative obligation to seek consular access to Mr Habib 'at the earliest possible moment' (in accordance with its consular guidelines) commenced as soon as the possibility of an Australian being detained was first raised. DFAT officials from the Australian High Commission in Islamabad should have demonstrated a greater sense of urgency in formally pursuing proper consular access to Mr Habib in Pakistan.

Consular responsibilities in Pakistan and Egypt

13. The arrangements for providing consular assistance to Mr Habib in Islamabad, including the use of an ASIO officer, were not adequate in Mr Habib's particular circumstances. It was unrealistic to expect that Mr Habib could contact the Australian Consul in Islamabad directly by telephone if he wished to receive consular assistance or that he would be able to independently contact a legal representative.
14. DFAT officials from the Australian Embassy in Cairo were diligent in pursuing confirmation that Mr Habib was in Egypt and in seeking urgent consular access to him, although access was never granted.

Interview of Mr Habib in Guantanamo Bay

15. When Mr Habib arrived in Guantanamo Bay, his first contact with Australian officials was during an interview conducted by DFAT, ASIO and AFP officers in May 2002. The conduct of the interviewing AFP officers is considered to have been not unreasonable in the circumstances. However, the AFP should have more carefully considered how it might have tasked its officers to conduct an appropriate interview, in circumstances where it was known that Australian domestic laws could have been engaged, but the obligations imposed by these laws could not have been met.
16. It would have been preferable for the AFP officers to have advised Mr Habib, specifically, that he was under no obligation to say or do anything; that he was not required to answer any particular question that he may not have wished to answer; and that he was free to terminate the interview at any time.
19. From 31 October 2001 to 10 November 2001, ASIO received increasingly senior representations from foreign governments about a proposal to move Mr Habib from Pakistan to Egypt. The Director-General of Security did not take sufficient action to advise DFAT or responsible ministers that there was an urgent need for the Australian Government to escalate its objections to that proposal.
20. In April 2002 (when Mr Habib was being detained by the US in Afghanistan, but had not yet been sent to Guantanamo Bay) DFAT requested advice from the US about its future intentions regarding Mr Habib. DFAT did not, however, indicate that the Australian Government had a preferred course of action; nor did it indicate that any Australian government agency expected to be consulted prior to the US making a decision about Mr Habib's ongoing detention; nor that the Australian Government had any intention to communicate a preferred course of action to the US at a later stage.
21. A whole-of-government policy position was never developed on the best way to approach the US Government about Mr Habib's detention in Afghanistan and subsequent transfer to Guantanamo Bay, or what Australia's preferred course of action should be.
22. Australian officials were diligent and committed in attempting to secure the best and fairest possible arrangements for military commission trials for Australian detainees, given the stated and clear position of the Australian Government that if Mr Habib could not be prosecuted in Australia, then the US should prosecute him.

Liaison with foreign governments

17. Individual Australian officials gave strong and consistent messages to foreign governments that Australia would not agree to Mr Habib being sent from Pakistan to Egypt.
18. Although ASIO took a lead role in giving these messages, there was no whole-of-government consideration of whether Australia should separately object to the move through other channels, including through diplomatic channels.
23. It was the responsibility of Pakistani, Egyptian and US authorities to decide whether Mr Habib had committed an offence against the laws of their respective countries, which warranted his detention. However, Australian agencies had insufficient regard to the fact that Mr Habib – an Australian citizen – was held without charge and without access to any legal process for a significant period of time. Mr Habib's best interests should have been the subject of more attention and action by Australian government agencies.

Coordination between Australian government agencies

24. At a number of points during Mr Habib's detention overseas there was a lack of effective coordination between Australian government agencies and it was not clear at times which agency was taking the lead role. This led to poor interagency communication and resulted in some agencies acting on incomplete information.
25. From April 2002, ASIO was of the view that Mr Habib had not been involved in planning for future terrorist attacks. This does not seem to have been understood by DFAT or conveyed to the Australian Ambassador to the US or to the Attorney-General prior to their meeting with senior US officials on 6 May 2002.

Mr Habib's welfare

26. There was no evidence that in the period between June 2002 and June 2003 DFAT made further enquiries about Mr Habib's health or sought access to Mr Habib. During this period DFAT appeared to rely on what ASIO shared about the observations of its officers. DFAT should have taken a more proactive approach to pursuing welfare visits to Mr Habib in this period.
27. In light of the constraints placed upon Australian agencies by having to rely upon foreign authorities to conduct and report on any investigations, Australian officials dealt with the allegations of mistreatment of Mr Habib in Guantanamo Bay appropriately in the circumstances. No report of any abuse investigation conducted by US authorities was provided for public release.

Communication with Mrs Habib

28. A letter sent to Mrs Habib from a DFAT official while Mr Habib was detained in Pakistan was inadequate and was not likely to have given Mrs Habib a full understanding of her husband's circumstances while in detention in Pakistan. Further, the letter may have denied Mr Habib's family an opportunity to obtain legal representation in Pakistan.

29. There was no apparent basis for the advice that DFAT gave to Mrs Habib (and to the Minister for Foreign Affairs) that Mr Habib was 'well and being treated well' in February 2002 when he was detained in Egypt.
30. There were inadequate mechanisms in place to ensure that Mrs Habib was kept informed with information Australian government agencies had about her husband's health and welfare while he was in US custody at Guantanamo Bay. The failure to provide Mrs Habib with any information in the period May 2002 to November 2003 is of particular concern.

Recommendations

Recommendation 1

Australian government agencies should prepare an apology to Mrs Maha Habib for failing to keep her properly informed about Mr Mamdouh Habib's welfare and circumstances.

Recommendation 2

DFAT should amend its current 'Arrest and Detention checklist' in the *Consular Handbook* to make explicit that:

- The checklist must be completed by any government official asked to undertake consular duties.
- The checklist must be completed each time a detainee is visited (not only on the first visit as currently required).
- After each visit, the official must provide details of the information they obtain, against the full range of consular functions.
- The official must advise what ability the detainee has to independently communicate with Australian officials or a legal representative – if the detainee has no such ability, this should be immediately drawn to the attention of senior consular officers in Canberra, for a determination of what action might be appropriate.

Recommendation 3

ASIO should amend its policies and procedures, for the avoidance of doubt, to make it clear:

- that before sending questions or other information to another state, in support of a custodial interview overseas, ASIO will first satisfy itself (including by reasonable enquiry where necessary) that the interviewee is not being and is not likely to be subjected to torture or other cruel, inhuman or degrading treatment or punishment
- any officer approving ASIO involvement in custodial questioning overseas must record what factors he or she had regard to in each particular case
- which Commonwealth agencies might be considered 'appropriate' or 'relevant' to advise or consult, in instances when ASIO becomes aware that torture or cruel, inhuman or degrading treatment or punishment has been used.

Recommendation 4

The AFP should develop a formal policy on what AFP officers should do in the event that they become aware torture or cruel, inhuman or degrading treatment or punishment has been, or is likely to be, experienced by an interviewee who is being held in detention overseas. The policy should encompass the sending of questions or information to support the conduct of a custodial interview, as well as circumstances where an AFP officer is physically present at an interview.

Recommendation 5

ASIO should amend its guidelines on the communication of information to foreign authorities to place a positive obligation on approving officers to document the reasons for a decision when any factor of which they had account is not articulated in the request documentation.

Recommendation 6

The AFP should review its *National guidelines on the disclosure of information* to include procedures for the communication of information about Australians to foreign authorities.

Annex 7: Requirements for Annual Reports

Description	Requirement	Part of Report	Page
Letter of transmittal	Mandatory	Preliminary	3
Table of contents	Mandatory	Preliminary	iv–v
Index	Mandatory	Annex	92–98
Glossary	Mandatory	Preliminary	vi
Contact officer(s)	Mandatory	Preliminary	ii
Internet home page address and internet address for report	Mandatory	Preliminary	ii
Review by agency head	Mandatory	Overview	1–7
Summary of significant issues and developments	Suggested	Overview	1–7
Overview of agency's performance and financial results	Suggested	Overview	1–7, 34–5
Outlook for following year	Suggested	Overview	4
Significant issues and developments – portfolio	Portfolio departments – suggested	Overview	N/A
Role and functions	Mandatory	Overview	1, 3, 6, 27
Organisational structure	Mandatory	Management & Accountability	28
Outcome and program structure	Mandatory	Performance	8
Where outcome and program 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	Mandatory	Performance	34–5
Portfolio structure	Portfolio departments – mandatory	N/A	N/A
Review of performance during the year in relation to programs and contribution to outcomes	Mandatory	Performance	8–29
Actual performance in relation to deliverables and KPIs set out in PB Statements/PAES or other portfolio statements	Mandatory	Performance	8–29, 72
Where performance targets differ from the PBS/PAES, details of both former and new targets, and reasons for the change	Mandatory	N/A	N/A
Narrative discussion and analysis of performance	Mandatory	Performance	8–29
Trend information	Mandatory	Performance	18, 35
Significant changes in nature of principal functions/services	Suggested	N/A	N/A

Description	Requirement	Part of Report	Page
Performance of purchaser/provider arrangements	If applicable, suggested	Management & Accountability	N/A
Factors, events or trends influencing agency performance	Suggested	Overview	1–7, 27
Contribution of risk management in achieving objectives	Suggested	Management & Accountability	29, 30
Social inclusion outcomes	If applicable – mandatory	N/A	N/A
Performance against service charter customer service standards, complaints data, and the department's response to complaints	If applicable – mandatory	N/A	N/A
Discussion and analysis of the department's financial performance	Mandatory	Management & Accountability	34–5
Discussion of any significant changes from the prior year, from budget or anticipated to have a significant impact on future operations	Mandatory	Management & Accountability	4, 27, 34–5
Agency resource statement and summary resource tables by outcomes	Mandatory	Annex	74–5
Agency heads are required to certify that their agency comply with the Commonwealth Fraud Control Guidelines	Mandatory	Management & Accountability	30
Statement of the main corporate governance practices in place	Mandatory	Management & Accountability	28–30
Names of the senior executive and their responsibilities	Suggested	Management & Accountability	28, 30
Senior management committees and their roles	Suggested	Management & Accountability	28, 29
Corporate and operational planning and associated performance reporting and review	Suggested	Management & Accountability	28–9
Approach adopted to identifying areas of significant financial or operational risk	Suggested	Management & Accountability	29–30
Policy and practices on the establishment and maintenance of appropriate ethical standards	Suggested	Management & Accountability	30
How nature and amount of remuneration for SES officers is determined	Suggested	Management & Accountability	30
Significant developments in external scrutiny	Mandatory	Management & Accountability	30–1
Judicial decisions and decisions of administrative tribunals	Mandatory	Management & Accountability	30–1
Reports by the Auditor-General, a Parliamentary Committee or the Commonwealth Ombudsman	Mandatory	Management & Accountability	31
Assessment of effectiveness in managing and developing human resources to achieve departmental objectives	Mandatory	Management & Accountability	31–2
Workforce planning, staff turnover and retention	Suggested	Management & Accountability	31

Description	Requirement	Part of Report	Page
Impact and features of enterprise or collective agreements, individual flexibility arrangements (IFAs), determinations, common law contracts and AWAs	Suggested	Management & Accountability	32
Training and development undertaken and its impact	Suggested	Management & Accountability	31, 32
Work health and safety performance	Suggested	Management & Accountability	33–4
Productivity gains	Suggested	Management & Accountability	30, 33
Statistics on staffing	Mandatory	Management & Accountability	28, 31–2
Enterprise or collective agreements, IFAs, determinations, common law contracts and AWAs	Mandatory	Management & Accountability; Annex 2 Salary ranges	32
Performance pay	Mandatory	Management & Accountability	32
Assessment of effectiveness of assets management	If applicable – mandatory	N/A	N/A
Assessment of purchasing against core policies and principles	Mandatory	Management & Accountability	32
Summary statement detailing the number of new and ongoing consultancies, total expenditure on new and ongoing consultancies, and reference to information on the AusTender website, and reporting all consultancies valued at \$10 000 or more (GST incl).	Mandatory	Management & Accountability	32–3
Absence of provisions in contracts allowing access by the Auditor-General	Mandatory	Management & Accountability	33
Contracts exempt from the AusTender	Mandatory	Management & Accountability	33
Financial Statements	Mandatory	Financial Statements	37–71
Work health and safety Schedule 2, Part 4 of the <i>Work Health and Safety Act 2011</i>	Mandatory	Management & Accountability	33–4
Advertising and Market Research (section 311A of the <i>Commonwealth Electoral Act 1918</i>) and statement on advertising campaigns	Mandatory	Management & Accountability	34
Ecologically sustainable development and environmental performance (section 516A of the <i>Environment Protection and Biodiversity Conservation Act 1999</i>)	Mandatory	Management & Accountability	34
Compliance with the agency's obligations under the <i>Carer Recognition Act 2010</i>	If applicable, mandatory	N/A	N/A
Grant programs	Mandatory	N/A	N/A

Description	Requirement	Part of Report	Page
Disability reporting – explicit and transparent reference to agency-level information available through other reporting mechanisms	Mandatory	Management & Accountability	33
Information Publication Scheme statement	Mandatory	N/A	N/A
Correction of material errors in previous annual report	If applicable – mandatory	N/A	N/A
List of requirements	Mandatory	Annex 7	88–91

Index

A

accountability *see* management and accountability

address and contact details, ii

Administrative Appeals Tribunal (AAT)

employee/prospective employee appeal rights
not enlivened, 6

IGIS role in providing expert evidence, 3, 27, 30

advertising and market research, 34

agency resource statements, 74–5

anniversary celebration (25th), 4

*Anti-Money Laundering and Counter Terrorism
Financing Act 2006*, 22

Archives Act 1983

IGIS role in FOI and Archives matters, 3, 27

Asher, Allan, 16

Assistant Inspector-General of Intelligence and
Security, 3, 28, 30, 33

assumed identities, 24, 26

Attorney-General, 2, 4, 6, 18, 20, 22, 24, 25, 84, 86

Attorney-General's Department (AGD), 83

Attorney-General's Guidelines, 21, 22, 24

Audit Committee, 28, 29

Auditor-General, 31, 33 *see also* Australian National
Audit Office

AusTender, 33

Australian Federal Police (AFP), 25

in Habib inquiry, 13, 83–7

Australian government agencies' actions in relation
to arrest and detention overseas of Mamdouh
Habib *see* Habib inquiry

Australian Government Protective Security Policy
Framework, 12, 29–30

Australian Government Security Vetting Agency,
3, 81–2

Australian Intelligence Community, 2–3

complaints against *see* complaints handling;
inquiries

employment related matters raised by current/
prospective AIC employees, 15

engagement with, 9

personnel security risk management, 12

Australian National Audit Office, 1

access clauses, 33

audit of ASIO's security assessment processes, 17
report, 31, 37–8

Australian Public Service Commission, 32, 33

Australian Secret Intelligence Service (ASIS), 2, 9

assumed identities, 26

AUSTRAC information access and use, 22

IGIS briefings for ASIS officers, 9, 25

IGIS inquiries and complaints handled
administratively, 72

inspections of, 25–6

ministerial authorisations to collect intelligence, 20

powers, 18

privacy rules and issues, 6, 21, 22

recruitment and vetting practices (IGIS inquiry),
11, 14

role, 2

weapons use and issues, 25–6

Australian Security Intelligence Organisation (ASIO)

allegations of improper conduct by
ASIO officers, 14

ANAO audit of ASIO's security assessment
processes, 17

assumed identities, 24

AUSTRAC information access and use, 22

community detention security assessment
inquiry, 11, 17, 76–9

complaints relating to ASIO visa security
assessment cases, 15, 16–17

communication with other agencies, 77, 78, 82

data inquiry requests, 23

engagement with law enforcement agencies, 25

exchange of information with foreign liaisons, 13, 24
 exposed to modified/corrupt vetting data, 80–1
 in Habib inquiry, 13, 83–7
 IGIS briefings for ASIO officers, 9, 24
 IGIS inquiries and complaints handled
   administratively, 72
 inspections of, 18–25
 investigations by, 22–3
 legal representation at ASIO interviews, 17
 management of a visa security assessment case
   (preliminary inquiry into), 14
 policy and training documentation, 79
 powers, 18, 22
 preliminary inquiries into, 14–15
 privacy rules and issues, 21
 procedural fairness in security assessments,
   30–1, 76–9
 processes in termination of employment, 14
 questioning and detention warrants, 5, 25
 recordkeeping, 23, 78–9
 role, 2
 security assessments issues, 6, 14, 30–1, 76–9
 taxation information access, 24
 telecommunications data access, 23
 timeliness of processes, 14, 16–17
 warrant operations, 19

Australian Security Intelligence Organisation Act 1979
 (ASIO Act), 2, 6, 18, 21, 77

Australian Taxation Officer (ATO), 24

Australian Transaction Reports and Analysis Centre
 (AUSTRAC), 22

Australians detained in foreign countries, 83–7 *see also* Habib inquiry

B

Balancing National Security and Individual Rights
 seminar, 4

Black, Rufus, 4

Blight, Jake, 3, 28, 30

briefings

  for IGIS by agencies, 9, 16, 19

  by IGIS for agency officers, 9, 24, 25

C

changes in agency policies and procedures as a
 result of IGIS recommendations, 3, 11, 12

  AFP, 13

  ASIO, 11, 13, 15, 16–17, 20, 79

  ASIS, 14

  DFAT, 13

  DSA, 10, 81–2

  DSD, 26

Commonwealth Disability Strategy, 33

Commonwealth Ombudsman, 16, 31

community detention eligibility, 18

community detention security assessment inquiry,
 11, 17, 76–9

complaints handling, 15–18, 72 *see also* inquiries

complaints to media concerning vetting practices
see Defence Security Authority (DSA) Inquiry

computer access warrants, 6

conferences and seminars, 4

consultants, 32–3

contact details, ii

contracting *see* purchasing

Corby v Australian Federal Police [2011] AATA 861
 (29 November 2011), 30

corporate and operational planning, 28–9

corporate governance, 28–30

court decisions, 30–1

Crimes Act 1914, 24, 26

D

data inquiry requests, 23

data integrity, 80–2

Defence Imagery and Geospatial Organisation (DIGO)
 compliance framework, 27
 Director authorisations, 27
 IGIS inquiries and complaints handled
 administratively, 72
 inspections of, 27
 ministerial authorisations to collect intelligence,
 20, 27
 powers, 18
 privacy rules and issues, 6, 20
 role, 2–3
 use of AUSTRAC information, 22

Defence intelligence agencies, 2–3
 personnel security risk management
 (inquiry into), 12

Defence Intelligence Organisation (DIO)
 IGIS inquiries and complaints handled
 administratively, 72
 privacy rules and issues, 21
 role, 2–3

Defence Security Authority (DSA) Inquiry, 3, 10, 72, 80–2

Defence Signals Directorate (DSD)
 collection team compliance inspection project, 26
 IGIS inquiries and complaints handled
 administratively, 72
 inspections of, 26
 internal compliance investigations, 26
 ministerial authorisations to collect intelligence, 20
 powers, 18
 privacy rules and issues, 6, 20
 role, 2–3

Department of Defence, 2, 10, 81 *see also* Minister
 for Defence

Department of Foreign Affairs and Trade (DFAT)
 in Habib inquiry, 13, 83–7
see also Minister for Foreign Affairs

Department of Immigration and Citizenship
 (DIAC), 11, 16, 17, 76, 77, 78 *see also* Minister for
 Immigration and Citizenship

Department of the Prime Minister and Cabinet
 (PM&C), 9, 33, 83 *see also* Prime Minister

Director of DIGO, 27
 Director-General of ASIS, 25, 26
 Director-General of Security, ASIO, 24
 disability reporting, 33

E

ecologically sustainable development, 34

effecting change in agencies *see* changes in
 agency policies and procedures as a result
 of IGIS recommendations

employment (OIGIS)
 frameworks, 32
 of persons for a particular inquiry, 30
 of SES officers, 30, 33
see also human resources management; staff

employment related matters raised by current/
 prospective AIC employees, 15

engagement with AIC agencies, 9 *see also* briefings

environmental performance, 34

ethical standards, 30

exchange of information *see* information sharing

exempt contracts, 33

expert evidence provision, 3, 27, 30

external scrutiny, 30–1

F

financial data
 access (data inquiry requests), 23
 intelligence information (AUSTRAC), 22

Financial Management and Accountability Act 1997, 32

financial performance, 34–5, 74–5

financial statements, 37–71

foreign intelligence collection
 legislative changes, 6
 warrants review, 20

foreign liaisons
 exchange of information with, 24

fraud control, 30

freedom of information

IGIS role in FOI and Archives matters, 3, 5, 27, 30

OIGIS as exempt agency (FOI Act), 34

functions *see* roles and functions (IGIS)

future *see* outlook

G

gender of staff, 32

grievance procedures in employment matters, 15

H

Habib inquiry, 3, 10, 12, 13, 83–7

Health and Safety Management Arrangements, 33–4

High Court, 30–1

human resources management, 31–2 *see also* staff

I

identities, assumed, 24, 26

imagery intelligence *see* Defence Imagery and Geospatial Organisation (DIGO)

immigration detention, 77, 78
see also community detention

immunity provisions of ISA, 6

Information Commissioner, 5, 27

information sharing, 13, 20, 21, 22, 24, 25, 86

inquiries, 1, 3, 9–12

administrative, 15–16, 17, 18, 72

full, 9–11, 17, 18

into non-AIC agencies, 10

number of, 10–11, 18, 72

own-motion, 6

preliminary, 9–10, 14–15, 17, 18

publication of reports, 11, 13

timeliness, 18

Inquiry into actions of Australian government agencies in relation to the arrest and detention overseas of Mamdouh Habib, 3, 10, 12, 13, 83–7

Inquiry into allegations of inappropriate vetting practices, 3, 10, 72, 80–2

Inquiry into ASIO's security assessments for community detention determinations, 11, 17, 76–9

Inquiry into ASIS recruitment and vetting practices, 11, 14

inquiry into Defence intelligence agencies' management of personnel security risk, 12

inspections, 1, 3

agency compliance with privacy rules, 21–2

ASIO activities, 18–25

ASIS activities, 25–6

AUSTRAC use, 22

DIGO activities, 27

DSD activities, 26

MAs issued to DSD, DIGO and ASIS, 20

overview of activities, 18–22

review of Foreign Intelligence Collection warrants, 20

Inspector-General of Intelligence and Security, 28

achievements over 25 years, 5

briefed by agencies, 9, 16, 19

briefings for agencies, 9, 24, 25

consulted on privacy rules, 7

former Inspectors-General, 5

parliamentary committee appearances/
submissions, 7

powers, 1, 6, 9–10

review of year, 1–7

role, 1, 3, 6, 27, 30

Inspector-General of Intelligence and Security Act 1986, 1, 9–10, 30

changes in 2011–12, 6

prior changes, 5

Inspector-General of Intelligence and Security Amendment Act 2011, 6

Institute of Public Administration of Australia, 4

Intelligence Services Act 2001 (ISA), 2

legislative changes, 6

privacy rules, 6, 7, 21

Intelligence Services Legislation Amendment Act 2011, 6

internal audit, 29

International Intelligence Review Agency
Conference, 4

Internet home page, ii

investigative powers *see* powers of IGIS

Irvine, David, 4, 16

J

Joint Select Committee on Australia's Immigration
Detention Network inquiry, 7

judicial decisions, 30–1

K

key performance indicators, 3, 8–9

L

law enforcement agencies, 24, 25, 83
see also Australian Federal Police (AFP)

learning and development, 32

legal representation rights at ASIO interview, 17

legal services, 33

legislative changes

in 2011–12, 6

historical, 5

national security legislation potential reforms, 4

M

M47/2012 v Director-General of Security & Others,
30–1, 76

management and accountability, 28–35

market research, 34

mental health considerations in custodial interviews, 79

Merryfull, Diane, 30

Migration Regulations 1994, 31

Minister for Defence, 3, 12, 18, 20, 27 *see also*
Department of Defence

Minister for Foreign Affairs, 2, 18, 20, 22, 84 *see also*
Department of Foreign Affairs and Trade (DFAT)

Minister for Immigration and Citizenship, 11,
76–9 *see also* Department of Immigration and
Citizenship (DIAC)

Minister for the Public Service and Integrity, 1, 30
ministerial authorisations to collect intelligence,
6, 18, 20, 27

N

National Disability Strategy, 33

National Security Adviser, 9

national security legislation potential reforms, 4

non-salary benefits, 32

O

occupational health and safety *see* work health
and safety

Office of National Assessments (ONA), 2, 5

IGIS inquiries and complaints handled
administratively, 72

privacy rules and issues, 21

role, 2

Office of National Assessments Act 1977 (ONA Act), 2

Ombudsman, 16, 31

organisational structure, 28

outcomes and outputs, 8

outlook, 4

overview by Inspector-General, 1–7

own-motion inquiries, 6

P

Parliamentary Joint Committee on Intelligence
and Security, 1, 4, 7

parliamentary oversight, 7

pay *see* remuneration

performance indicators, 3, 8–9

performance pay, 32

performance report, 8–27

evaluation of performance, 9

highlights, 3–5

personnel security risk management inquiry, 12

policy and training documentation, 79, 82

portfolio relationship, 1

powers of IGIS, 1, 6, 9–10 *see also* roles and functions (IGIS)

Prime Minister, 1, 2, 3, 5, 6, 8

    requests for inquiries, 10, 13, 80, 83

see also Department of the Prime Minister and Cabinet (PM&C)

priorities-setting, 4

privacy rules, 6, 7, 21–2

protected information, 24

protection for complainants/information providers, 10

protection of privacy *see* privacy rules

Protective Security Policy Framework, 12, 29–30

publication of inquiry reports, 11, 13

purchasing, 32, 34

Q

questioning and detention warrants, 25

R

recordkeeping, 21

    by ASIO, 11, 23, 78–9

    by DSD, 26

recruitment (OIGIS), 31, 34

recruitment and vetting practices inquiry, 11

remuneration, 32, 73

reports of inquiries, 11, 13

risk management, 29, 30

roles and functions (AIC agencies), 2–3

roles and functions (IGIS), 1, 3, 6

    changes over 25 years, 5

    in FOI and Archives matters, 3, 27, 30

S

salary, 32, 73

security assessments for visa applicants

    ASIO management of a visa security assessment case (preliminary inquiry into), 14

ASIO procedural fairness (court case), 30–1

    complaints handling, 16–17, 18

security awareness and procedures, 29–30

Senate Standing Committee on Finance and Public Administration, 7

senior executive team, 28, 30

Senior Executive Service (SES) officers, 30

senior management committees, 28

staff

    number, 8, 28

    profile (statistics), 31–2

    recruitment, 3, 31, 34

    remuneration, 32, 73

    retention and turnover, 3, 32

    senior executive, 28, 30

    survey, 3, 31

Stanton, Meryl, 9

structure *see* organisational structure

T

Taxation Administration Act 1953 (TAA), 23–4

taxation information, 23–4

Telecommunications (Interception and Access) Act 1979 (TIA Act), 6, 18, 23

telecommunications data, 23

telecommunications interception warrants, 19

tendering *see* purchasing

Thom, Vivienne *see* Inspector-General of Intelligence and Security

training and development (OIGIS), 31, 32

training in AGSVA, 82

trends, 18, 35

tribunal decisions, 30–1

U

United Nations sanction enforcement law, contravention of, 6

V

- vetting practices Inquiry *see* Defence Security Authority (DSA) Inquiry
- visa applicants *see* security assessments for visa applicants

W

- wages *see* remuneration
- warrant operations by ASIO, 19, 20
- warrants for collection of foreign intelligence, 20
- weapons use and issues, 5, 25–6
- website address, ii
- work health and safety, 33–4
- workforce planning, 31
- workload, 3, 27, 30, 72
- workplace agreements, 32

Inspector-General of
Intelligence and Security
Annual Report 2011-12

TWELVE

NINETEEN EIGHTY SEVEN TO TWO THOUSAND AND TWELVE

■ NINETEEN EIGHTY SEVEN TO TWO