

# Annual Report 2007–2008



# Annual Report 2007–2008



## **IGIS CONTACT INFORMATION**

### **Location**

One National Circuit  
BARTON ACT 2600

### **Written inquiries**

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

### **Parliamentary and media liaison**

Ms Jodie Williams  
Office Manager  
Phone: (02) 6271 5692  
Fax: (02) 6271 5696

### **General inquiries**

Phone: (02) 6271 5692  
Fax: (02) 6271 5696  
E-mail: [info@igis.gov.au](mailto:info@igis.gov.au)

### **Internet Address**

<http://www.igis.gov.au>

ISSN 1030-4657

© Commonwealth of Australia 2008

This work is copyright. Apart from any use as 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, Robert Garran Offices, National Circuit, Barton ACT 2600 or posted at <http://www.ag.gov.au/cca>.

Design and typesetting by ZOO, ACT.

Printed by Goanna Print



2008/744

File Ref: 2007/89

Senator the Hon John Faulkner  
Special Minister of State  
Cabinet Secretary  
Parliament House  
CANBERRA ACT 2600

Dear Senator Faulkner

I present herewith my annual report, as required by section 35 of the *Inspector-General of Intelligence and Security Act 1986*. The report covers the period between 1 July 2007 and 30 June 2008.

The report has been prepared in compliance with the Requirements for Annual Reports, issued by the Department of the Prime Minister and Cabinet on 18 June 2008.

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 or the privacy of individuals. The report is therefore suitable to be laid before each House of the Parliament.

Yours sincerely

Ian Carnell  
Inspector-General of  
Intelligence and Security

22 September 2008

# table of contents

Glossary of acronyms used in this report	7	Inquiry into ASIO's dealings with Mr Izhar Ul-Haque	23
Key points	8	Administrative inquiry into the arrest of Dr Mohamed Haneef	23
Role of the Inspector-General	10	Parliament, legislation and liaison	24
The year in review	11	Overview	24
Federal election and change of government	11	Parliamentary oversight	25
Newly constituted National Security Committee	11	Parliamentary Joint Committee on Intelligence and Security	25
Changed administrative arrangements affecting IGIS	11	Senate Finance and Public Administration Committee	25
New selection arrangements	12	Parliamentary accountability – general	25
Key intelligence and security interests	12	Legislative proposals and developments	26
Continuing growth of the AIC	13	<i>Telecommunications (Interception and Access) Amendment Act 2007</i>	26
Consequential growth of OIGIS	13	<i>Telecommunications (Interception and Access) Amendment Act 2008</i>	26
Acting IGIS	14	Independent Reviewer of <i>Terrorism Laws Bill 2008</i>	27
Secretary of PMC	14	Independent Reviewer of <i>Terrorism Laws Bill 2008 (No.2)</i>	27
OIGIS valedictions	14	<i>Inspector-General of Intelligence and Security Act 1986</i>	27
Retirement of Ms Robyn Kelly	14	ALRC review of the <i>Privacy Act 1988</i>	27
IGIS activities	15	ALRC review of client legal privilege	28
Complaints and inquiries	15	Contributions to public sector governance	28
Processing of complaints by administrative means	16	Membership of the Administrative Review Council	28
Preliminary inquiries	16	Homeland and Border Security Review	28
Full inquiries	16	Providing advice on the outcome of complaints investigations	28
Inspection and visits program	17	Review of Part D of Protective Security Manual	29
Community outreach	18	Liaison with other Commonwealth integrity agencies	29
Training	19	Renewed involvement with CrimTrac	29
International cooperation	19		
IIRA Conference 2008	19		
Significant issues	19		
Review of ONA statutory independence	20		
Inquiry into DIO analytic integrity	20		
Inquiry into Organisational Suitability	20		
Assessment processes	20		
NSW coronial inquiry into Mr Brian Peters' death	21		

Performance	30	Concerns about recruitment experiences	46
Outcomes and outputs	30	Concerns held by former employees	46
Performance indicators	30	Assessment of security equipment	47
Levels of complaint and inquiry	30	Immigration related complaints	47
Timeliness	32	Australian Secret Intelligence Service	49
Acceptance of recommendations	33	What ASIS does	49
Responsiveness to issues raised	33	Significant issues	49
Level of assurance	33	New Minister	49
Summary	34	Growth and expansion	49
Australian Security Intelligence Organisation	35	Special briefings	50
What ASIO does	35	Visits and contact with staff	50
Significant issues	35	Training	50
New Attorney-General's Guidelines	35	Access to AUSTRAC data	50
Ul-Haque inquiry	36	Inspection activities	51
Increase in the number of		Range and scope	51
immigration-related complaints	37	Review of Ministerial Authorisations	51
ASIO's continued growth, litigation and		Ministerial submissions	51
review workload	37	Authorisations related to training in/	
Monthly meetings and special briefings	38	or use of weapons for self-defence	
Training	38	purposes/self-defence techniques	51
Inspection activities	39	Operational file review activities/use	
General scope	39	of former IGIS as a consultant	52
Range of current and new inspection		Privacy rules	52
activities	39	Periodic roundtable meetings	53
Project to review the retention of		Use of assumed identities	53
intelligence information on currently		Complaints and inquiries	53
serving politicians	39	Defence Signals Directorate	54
Warrant operations	39	What DSD does	54
Outcome of warrant inspections	40	Significant issues	54
Unauthorised telecommunications		New Minister	54
interception	41	Ministerial Directions	54
Interception management systems	41	DSD privacy rules	55
Reports of warrant activity	41	Compliance oversight of ADF signals	
Questioning warrants/questioning and		intelligence activities	55
detention warrants	42	Support to military operations	55
Approval to investigate – procedures	42	Support for counter-terrorism activities	56
Approval to investigate – inspection		NSW coronial inquiry into the late	
results	42	Mr Brian Peters	56
ASIO and law enforcement agencies	43	Inspection activities	56
Interoperability issues	43	Ministerial authorisations	56
Information obtained from AUSTRAC	43	Spot checking of databases	56
Access to taxation information	44	Monthly meetings	57
Use of assumed identities	44	Privacy rules – monitoring and	
Exchange of information with foreign		compliance	57
liaisons	44	New collection activities	57
Complaints and inquiries	45	Site visits	57
Operational interactions between		Training	57
ASIO and members of the community	45	Complaints and inquiries	58
Archives related complaints	46	Wider review of OSA policy and	
Release of RCIS papers	46	procedures	58
		Matters handled administratively	58

Defence Imagery and Geospatial Organisation	59	Fraud control	71
What DIGO does	59	Disaster recovery plan/business continuity plan	71
Significant issues	59	Corporate and operational planning	71
New Minister	59	External scrutiny	71
Ministerial Directions and DIGO privacy rules	59	Support from PMC and DSD	71
Inspection activities	60	Human resources	72
Ministerial and Director DIGO authorisations	60	Background	72
DIGO privacy rules	61	Organisation profile	72
Meetings with senior DIGO staff	61	Training and development	73
Training	61	Performance management and pay	73
Visits	61	Workplace agreements	73
Complaints and inquiries	61	Personnel guidelines	73
Wider review of OSA policy and procedures	61	Other information	73
Matters handled administratively	61	Occupational health and safety	73
Defence Intelligence Organisation	62	Disability Strategy	74
What DIO does	62	Freedom of information	74
Analytic Integrity	62	Advertising and market research	74
Privacy guidelines	63	Ecologically sustainable development and environmental performance	74
Training	63	Financial management	74
Complaints and inquiries	63	Purchasing	74
Office of National Assessments	64	Consultancy services	74
What ONA does	64	Contract services	74
Statutory Independence– Inquiry 2007	64	Legal services	75
Privacy guidelines	65	Summary of the office's financial performance and resources for outcomes	75
Training	65	Financial Statements	76
Complaints and inquiries	65	Annex 1 – Complaint and inquiry statistics	102
The year 2008-09 in prospect	66	Annex 2 – Consultancy services let during FY 2007–08 of \$10 000 or more	104
Inspection and review activities involving AIC agencies	66	Annex 3 – Report on the independence and integrity of ONA assessments	105
ASIO	66	Annex 4 – Principles of analytic integrity – DIO	107
ASIS	67	Annex 5 – Inquiry into Organisational Suitability Assessment processes in Defence	108
DSD	67	Annex 6 – IGIS/AUSTRAC memorandum of understanding	110
DIGO	68	Annex 7 – Attorney-General's Guidelines to ASIO	117
DIO	68	Index	124
ONA	68		
Inquiries and complaints	68		
OIGIS staffing and recruitment	68		
Other OIGIS corporate activities	69		
Other matters to be pursued	69		
Corporate governance, human resources and financial management	70		
Corporate Governance	70		
Organisation structure	70		
Internal audit	70		
Risk management	70		

# glossary of acronyms used in this report

ADF	Australian Defence Force
AIC	Australian Intelligence Community
ALRC	Australian Law Reform Commission
AML/CTF Act	<i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i>
APEC	Asia-Pacific Economic Cooperation
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
DIGO	Defence Imagery and Geospatial Organisation
DIAC	Department of Immigration and Citizenship
DIO	Defence Intelligence Organisation
DSD	Defence Signals Directorate
IGIS	Inspector-General of Intelligence and Security
IGIS Act	<i>Inspector-General of Intelligence and Security Act 1986</i>
ISA	<i>Intelligence Services Act 2001</i>
MA	Ministerial authorisation
MOU	Memorandum of understanding
NAA	National Archives of Australia
OIGIS	Office of the Inspector-General of Intelligence and Security
ONA	Office of National Assessments
OSA	Organisational Suitability Assessment
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PMC	Department of the Prime Minister and Cabinet

# key points

- Significant attention was paid in the reporting period (by way of own motion inquiries) to the two assessment agencies, the Office of National Assessments (ONA) and the Defence Intelligence Organisation (DIO). A detailed inquiry into the independence and integrity of ONA assessments in the 12 months to September 2007 was completed in December 2007. I concluded that the culture and processes support independence and integrity, with some minor suggestions for strengthening made. There was no evidence or indication of improper pressure or attempted direction from ministers or their offices in that period. While policy departments very occasionally could press their arguments in a way which bordered on undue pressure, ONA's final judgements did not appear to have been affected in an improper way.
- As a logical follow on from this scrutiny of ONA, I commenced an own motion inquiry into the integrity of DIO assessments. This was still under way at the close of the reporting period, as was an own motion inquiry into the activities of the Australian Security Intelligence Organisation (ASIO) in respect of Mr Izhar UI-Haque and related matters. The latter was triggered by criticism of ASIO in *R v. UI-Haque* [2007] NSWSC 1251 and raised serious allegations about the legality and propriety of certain actions by ASIO officers which occurred in 2003.
- Another inquiry completed in the 2007–08 reporting period concerned the Organisational Suitability Assessment process in the Defence intelligence agencies. I made a number of recommendations for enhancement to the process which were accepted positively and are being implemented.
- Inquiries were also initiated in the reporting period as a result of 15 complaints of various kinds. These ranged across operational interactions between ASIO and members of the community, the handling of archives requests, concerns about recruitment experiences, concerns held by former employees, issues to do with the assessment of security equipment, and a small number of immigration related matters.
- The number of complaints received by the office increased markedly in 2007–08. This was primarily driven by matters pertaining to the timeliness of ASIO's security assessment process for visa purposes. A total of 193 new complaints of this type were received and actioned administratively in the reporting period. This compares to 71 new complaints of this kind being received and actioned administratively in 2006–07 and 26 immigration related complaints processed in this manner in 2005–06.
- There was also some increase in the number of contacts and complaints which my office received from current or former members of the AIC raising personnel management related grievances, and from applicants for positions with AIC agencies expressing concerns about recruitment practices. However, the number is not large relative to the size and growth of the AIC.
- The office's inspection program continued to grow in size due to increased levels of activity by the Australian Intelligence Community (AIC) agencies. I am very appreciative of the efforts of my staff in responding to the increasing tempo and fulfilling the planned program.

- The inspection program paid close attention to ASIO warrants and investigative approvals; AUSTRAC checks by ASIO; the privacy rules and ministerial authorisation requirements for the Australian Secret Intelligence Service (ASIS), Defence Imagery and Geospatial Organisation (DIGO) and Defence Signal Directorate (DSD); the privacy guidelines applicable to DIO and ONA; and sensitive operations by ASIS. Although substantive concerns identified were relatively few in number, I was pleased that each was corrected or addressed suitably by the relevant agency when raised with them. We raised a somewhat greater number of procedural issues, particularly through our inspection activities, and these were also corrected or addressed satisfactorily.
- As in previous years my staff and I also presented at agency seminars and training courses and at common AIC courses, reaching around 1250 staff in approximately 40 sessions. We impress upon agency staff the importance of the rule of law and the need for them to have the trust and confidence of the community through being professional and judicious in the use of powers and capabilities.
- The portfolio arrangements under the new Government elected on 24 November 2007 involve the Cabinet Secretary and Special Minister of State, Senator the Hon John Faulkner having general administrative responsibility for my office, consistent with his responsibility for other accountability and integrity agencies such as the Commonwealth Ombudsman and the Auditor-General.
- We continued to develop our relationships with other accountability and integrity agencies, and pursued targeted outreach activities to the community.
- Despite the recruitment of two new staff during 2007–08, there was no net gain in staff numbers as had been budgeted for, due to two departures. As noted earlier, the planned 2007–08 visits and inspections program was still achieved by dint of the commitment of staff to the work of the office. Further recruitment action was under way at the close of the reporting period.
- The office received an unqualified report on its financial statements for 2007–08 from the Australian National Audit Office (ANAO).



Ian Carnell,  
Inspector-General of Intelligence and Security

# role of the Inspector-General

The IGIS is an independent statutory office holder who reviews the activities of the agencies which collectively comprise the AIC. The IGIS has own motion powers in addition to considering complaints or requests from ministers.

There are currently six intelligence and security agencies which form the AIC, namely:

- Australian Security Intelligence Organisation (ASIO)
- Australian Secret Intelligence Service (ASIS)
- Defence Signals Directorate (DSD)
- Defence Imagery and Geospatial Organisation (DIGO)
- Defence Intelligence Organisation (DIO), and
- Office of National Assessments (ONA).

The office was formally established by the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) and commenced operating on 1 February 1987.

The Office of the Inspector-General of Intelligence and Security (OIGIS) is situated within the Prime Minister's portfolio for administrative purposes, but as an independent statutory office holder, the IGIS is not subject to general direction from the Prime Minister or other Ministers on how the functions under the IGIS Act should be carried out.

The role and functions of the IGIS are set out in sections 8, 9 and 9A of the IGIS Act. These sections provide the legal basis for the IGIS to conduct regular inspections of the AIC agencies and to conduct inquiries, of varying levels of formality, as the need arises.

The overarching purpose of these activities is to ensure that each AIC agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights.

The majority of the resources of the office are directed towards on-going inspection and monitoring activities, so as to identify issues or concerns before they develop into systemic problems which then require major remedial action.

The inspection role of the IGIS is complemented by an inquiry function. In undertaking inquiries the IGIS has very strong investigative powers, akin to those of a Royal Commission.

Inquiries are conducted in private because they almost invariably involve highly classified or sensitive information, and the methods by which it is collected. The public ventilation of this material could be potentially very harmful to those persons involved in its collection, or compromise collection, neither of which would serve the national interest.

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 IGIS focus is the operational activities of the AIC agencies, they are also subject to review by the Parliamentary Joint Committee on Intelligence and Security (PJCS), as well as the Australian National Audit Office (ANAO). Certain ASIO assessments can be appealed to the Administrative Appeals Tribunal (AAT). Proceedings can also be instituted against AIC agencies in the Courts.

# the year in review

## Federal election and change of government

The 41st Parliament of the Commonwealth of Australia was formally prorogued at 1200 hrs on 17 October 2007, and writs were issued for an election for the House of Representatives and half of the Senate, which was conducted on 24 November 2007.

A new government, under the Prime Ministership of the Hon Kevin Rudd MP, was sworn in on 3 December 2007.

With the change of government, those individuals who had held ministries under the Howard Government with oversight and management responsibilities for AIC agencies naturally relinquished those positions.

The Hon Kevin Rudd MP, assumed administrative responsibility for a range of agencies within his portfolio upon being sworn in as Prime Minister. These agencies include ONA and OIGIS.

The incoming Attorney-General, the Hon Robert McClelland MP, replaced the Hon Philip Ruddock MP and in addition to becoming the first law officer of the Commonwealth, also took over executive responsibility for ASIO.

The Minister for Foreign Affairs, the Hon Alexander Downer MP, was replaced in that role by the Hon Stephen Smith MP. In doing so, Mr Smith assumed executive responsibility for ASIS.

The Hon Joel Fitzgibbon MP replaced the Hon Dr Brendan Nelson MP as the Minister for Defence, and in so doing assumed executive responsibility for DSD, DIGO and DIO.

## Newly constituted National Security Committee

Each of the newly appointed Ministers named above are also members of the National Security Committee (NSC), as are the Deputy Prime Minister (the Hon Julia Gillard MP), the Treasurer (the Hon Wayne Swan MP), and the Cabinet Secretary/Special Minister of State (the Hon Senator John Faulkner).

NSC is a standing committee of the Cabinet which meets both regularly and on an ad hoc basis (as necessary), to consider significant issues and make decisions which have, or are likely to have, an impact on Australia's defence, intelligence and security, and international affairs and relationships. Excepting where decisions are referred to a full meeting of the Cabinet, NSC is the peak executive-level political decision making body for the AIC agencies.

## Changed administrative arrangements affecting OIGIS

In April 2008 I was advised of Prime Minister Rudd's intention to rebalance the administrative arrangements within his portfolio entailing, among other things, administrative responsibility for OIGIS being transferred from him to the Cabinet Secretary/Special Minister of State, Senator the Hon John Faulkner.<sup>1</sup> This is consistent with Senator Faulkner's responsibility for other accountability and integrity agencies such as the Commonwealth Ombudsman and the Auditor-General.

<sup>1</sup> My understanding is that when Senator Faulkner is engaged on matters which pertain to the Prime Minister and Cabinet portfolio he is properly titled the Cabinet Secretary, and that when he is engaged in other matters within his remit he is properly titled the Special Minister of State. I will adopt this approach in this report.

In being advised of this proposed change I was reassured that the revised arrangements would not prevent me dealing directly with the Prime Minister if there were a significant matter which I believed the Prime Minister should be alerted to or otherwise personally involved.

The above change and other revised administrative arrangements affecting the Prime Minister and Cabinet portfolio came into effect on 1 May 2008.<sup>2</sup>

## New selection arrangements

The Australian Labor Party made a commitment in the lead up to the 2007 federal election to strengthen transparency and merit based selection when appointing senior statutory office holders and senior public servants. Upon coming to power the Rudd Government sought to give effect to this commitment by introducing new arrangements with effect from 8 February 2008.<sup>3</sup>

In announcing these new arrangements the Cabinet Secretary indicated that, in future, at least 130 prescribed senior public service/statutory office holder positions would be publicly advertised when a vacancy arose or was anticipated, that an assessment process for each position would be conducted on the basis of merit, and that each process would be oversighted by the relevant departmental secretary and the Public Service Commissioner.<sup>4</sup>

While in each case a report and recommendations will be made to the responsible Minister, the decision on appointment or recommendation to the Governor-General will remain with the Minister.

The positions of Director-General of ASIS and Director-General of Security (i.e. the head of ASIO) are excluded from this new arrangement, while the positions of IGIS and Director-General of ONA are specifically included. The heads of the three Defence intelligence agencies are not statutory office holders and are not listed, but are in any case subject to other merit-based processes.

As indicated in my previous annual report, I was reappointed for a second and final term as Inspector-General on 27 April 2007.<sup>5</sup> The instrument of appointment is for a period of four years from that date.

This means that at the conclusion of my appointment on 26 April 2011, or if I were to leave this office prior to then, there is now a requirement for the position of IGIS to be advertised. The statutory requirements for consultation with the Leader of the Opposition before submission of a recommendation to the Governor-General, will remain a part of the process.

## Key intelligence and security interests

Given the complex interweaving of domestic and international affairs, it follows that the focus of the AIC agencies in the period covered by this report was necessarily directed towards a variety of targets and interests.

While it is not appropriate for me in a public document to set out the details and ordering of Australia's national intelligence collection priorities, or the trends and developments in which our assessment agencies have a particular interest, in a very general sense it can be said that these interests include (but are not limited to) the following broad topics:

- the provision of accurate and timely advice to key decision makers, so that they might respond in an informed way to emerging and enduring issues of concern
- the early detection of threats to the interests of Australians at home and abroad
- the disruption of activities which are judged to pose a serious threat to Australia's national interests, where it is possible and desirable to do so
- the provision of support to various ADF deployments overseas (including in hostile operational environments such as Iraq and Afghanistan)

<sup>2</sup> Cabinet Secretary/SMOS media release number 13/2008 dated 1 May 2008, Cabinet Secretary: Additional Responsibilities, refers.

<sup>3</sup> Cabinet Secretary/SMOS media release number 02/2008 dated 5 February 2008, New Arrangements for Merit and Transparency in Senior Public Service Appointments, refers.

<sup>4</sup> *ibid.*

<sup>5</sup> IGIS Annual Report 2006–2007, p.16.

- providing coordinated in-depth planning and support to the security effort associated with Australia's hosting of events of major significance (e.g. the Asia-Pacific Economic Cooperation (APEC) Leaders meeting in September 2007, the Olympic torch relay in April 2008, and the Papal visit and various events associated with World Youth Day in July 2008)
- the sharing of information with AIC and non-AIC agencies, in order to gain a better appreciation of potential threats, and to enhance regional and global security, and
- sharing skills and building capability within our region to deal more effectively with new and emerging threats to Australia's defence, economic, foreign relations and security interests.

## Continuing growth of the AIC

The AIC has experienced a significant increase in size in recent years. This growth has occurred as a consequence of:

- ever-changing global circumstances
- the increased targeting of both western and Australian interests
- the implementation of recommendations contained in various external and internal reviews of the AIC agencies which were commissioned in response to these changing circumstances, and
- the acceptance by government of a variety of new policy and planning proposals put forward by the AIC agencies to enhance their capability to respond to a changing security environment.

Notwithstanding that there was a change of government in late 2007, there are no outwards signs that the funding outlook for the AIC agencies will alter dramatically in the near to medium term.

As an example of this, in October 2005 the then Attorney-General, the Hon Philip Ruddock MP, announced a five-year strategic plan under which he projected that ASIO would grow from an existing establishment of 980 positions to 1860 positions by 30 June 2011.<sup>6</sup>

In the ASIO portfolio budget statement for 2008–09, it is stated that:

*“ASIO remains on track to meet the government-endorsed target of 1860 staff by 2010–11. ASIO currently has around 1470 staff, which is more than double the number at the end of 2002–03 (668). ASIO will continue to recruit around 170 staff in each of 2008–09 and 2009–10.”<sup>7</sup>*

The Rudd Government's first budget was delivered by the Treasurer, the Hon Wayne Swan MP, on 13 May 2008. The passage of relevant budgetary measures announced on that night, namely the Appropriation Bill (No. 1) 2008–09, will have the effect of continuing the growth of ASIO and the other AIC agencies to ceiling levels which were proposed by the former government.

For any agency rapid growth generates some degree of organisational stress, and the AIC agencies are not an exception.

One way in which this may be manifest is a small but increasing number of complaints made to my office about AIC agency selection exercises and recruitment practices, and complaints from current and/or former staff about internal management practices. However, in a relative sense the number of such complaints is not large when compared to the size and growth of the agencies.

## Consequential growth of OIGIS

When I began my first term of appointment as Inspector-General in March 2004, the office comprised myself and four staff.

This staffing level remained static for approximately 12 months before I obtained funding approval to increase the size of the office, in a phased manner, in lock-step with the growth of the AIC.

As at 30 June 2008, OIGIS comprised myself and 9 staff who perform a range of inspection, inquiry, review, complaints handling and corporate functions.

Further details about the resources of the office are provided in the “Corporate Governance, Human Resources and Financial Management” chapter of this report.

<sup>6</sup> The Hon Philip Ruddock MP, Attorney-General Media Release 191/2005 dated 16 October 2005.

<sup>7</sup> ASIO Portfolio Budget Statement 2008–2009, p. 182. This statement can be viewed at <[http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications\\_Budgets\\_Budget2008-2009](http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_Budgets_Budget2008-2009)> (accessed on 4 August 2008).

## Acting IGIS

In my previous annual report, I wrote of how the then Prime Minister, the Hon Mr John Howard AC, had issued a standing instrument of appointment to Professor John McMillan on 28 May 2007, which enables Professor McMillan to serve as the Acting Inspector-General for those periods of time when I am either outside of the country, on an extended period of approved leave, or if I were to be incapacitated for any reason.<sup>8</sup>

Despite the change of government, this instrument has continuing legal effect until such time as it is either revoked or overridden by a subsequent instrument of appointment.

During September–October 2007, I took four weeks leave during most of which time I was overseas. This was the first extended period of annual leave which I have taken since being appointed as Inspector-General in 2004.

I am most grateful to Professor McMillan for the assistance he afforded to this office, as Acting Inspector-General, at that time and on a continuing basis.

## Secretary of PMC

Shortly after the 2007 Federal Election and overseeing the transition to power of the new Rudd Government, the then Secretary of the Department of the Prime Minister and Cabinet (PMC), Dr Peter Shergold AC, formally advised the Prime Minister of his decision not to seek reappointment to that position when his five-year term expired in February 2008.

On 6 February 2008, the Prime Minister announced the appointment of Mr Terry Moran AO, as Dr Shergold's replacement.<sup>9</sup> Mr Moran took up his appointment on 3 March 2008.

At the time of his appointment, Mr Moran was serving as the Secretary of the Victorian Department of Premier and Cabinet, a position which he had held since July 2000.

The position of the Secretary of PMC is a critical appointment for any government, as the holder of that office sits at the centre of the bureaucratic power structure and shares a leadership role for the Australian Public Service with the Australian Public Service Commissioner.

The Secretary of PMC also plays a pivotal role in respect of the AIC, in that he or she provides direct input and support to NSC, and as chair of the Secretaries Committee on National Security (SCNS).

I only had the opportunity for limited dealings with Mr Moran in the period between his commencement as Secretary of PMC and the end of the reporting period, but these dealings were cordial and served to underline the importance he places on accountability bodies such as OIGIS.

## OIGIS valedictions

### Retirement of Ms Robyn Kelly

The occasion of this annual report provides me with the opportunity to put on the public record some comments about a valued member of the OIGIS team, Ms Robyn Kelly, who retired in August 2007, after 14 years of dedicated service to the office.

Ms Kelly has the unique distinction of spending the longest period of any one individual on the OIGIS payroll. In addition to being a diligent and dedicated officer throughout her tenure, Ms Kelly has also left an enduring mark on all who worked with her through her constant championing of environmental and animal welfare issues, as well as bringing *joie de vivre* to the office.

We all miss the special spark which Ms Kelly gifted to the office and wish her the very best in her well deserved retirement.

<sup>8</sup> IGIS Annual Report 2006–2007, *op. cit.* p.16.

<sup>9</sup> Prime Minister of Australia Media Release dated 6 February 2008, *Secretary of Department of the Prime Minister and Cabinet*, refers.

## IGIS activities

### Complaints and inquiries

Section 8 of the IGIS Act provides a legal basis for the Inspector-General to conduct inquiries into the AIC agencies following a referral from a responsible Minister, or upon the Inspector-General's own motion.

Section 8 of the IGIS Act also empowers the Inspector-General to receive and inquire into complaints about the AIC agencies which collect intelligence (i.e. ASIO, ASIS, DSD and DIGO).

There is no specific provision in section 8 of the IGIS Act which directly permits this office to initiate an inquiry on the basis of a complaint which is made about either of the assessment agencies (i.e. DIO and ONA).

The rationale for this delineation between the intelligence collection and intelligence assessment would appear to be that the agencies which undertake only assessment do not have the capacity to infringe the civil liberties of individuals to the degree that the collection agencies might.

For practical purposes this has not been a major impediment to the efficient operation of this office because we have received very few complaints about DIO and ONA since the office was created.

When complaints about DIO or ONA have been received, they have usually been capable of being dealt with administratively (i.e. without need to use the formal powers afforded to the IGIS under the IGIS Act).<sup>10</sup>

Mr Philip Flood considered whether the Inspector-General should have the capacity to directly initiate an inquiry on the basis of a complaint about DIO or ONA, in his *Report of the Inquiry into Australian Intelligence Agencies*, which was presented to government in July 2004.<sup>11</sup>

Mr Flood did not propose a change of this sort but did recommend that the IGIS Act should be amended, to provide the IGIS with the capacity to initiate own motion inquiries into the assessment agencies, at his or her discretion, consistent with the Inspector-General's existing jurisdiction in respect of the collection agencies. Such an amendment was made to the IGIS Act with effect from 2 December 2005.

The net effect of the above is that the IGIS has either clearly defined direct authority, or sufficient flexibility, to handle complaints about all six AIC agencies.

Section 8 also provides guidance on whether or not particular employment related concerns, and a range of other issues, fall inside or outside the remit of the Inspector-General. These provisions are somewhat convoluted.

If my office receives a complaint which I determine falls outside of my jurisdiction, the complainant is promptly informed of this fact and whether or not there are any other avenues available to them for consideration of their concerns.

If a matter of concern or complaint falls within my jurisdiction, a judgement needs to be exercised as to whether or not it should be pursued, and if so, the most appropriate mechanism for taking it forward.

Section 11 of the IGIS Act provides me with wide discretion on whether or not to pursue a complaint. The underlying presumption of the section is that a complaint against an AIC agency will be pursued, so long as it is within jurisdiction, unless:

- the complainant became aware of the action more than 12 months before the complaint was made and did not pursue it at the time
- the complaint is frivolous or vexatious or not made in good faith, or
- having regard to all of the circumstances of the case, an inquiry, or further inquiry, into the action is not warranted.

Additionally, I will not pursue an inquiry where a complainant has exercised or could exercise a right to cause the action to which a complaint relates to be reviewed by a court or tribunal, unless I am of the opinion that there are special reasons for doing so.

Having considered whether or not a complaint is within jurisdiction, and determined whether it should be pursued, I have three options on how next to handle a complaint. These options are to either pursue the matter administratively, as a preliminary inquiry, or as a full inquiry.

<sup>10</sup> P. Flood, *Report of the Inquiry into Australian Intelligence Agencies*, Canberra, July 2004, pp. 59-60.

<sup>11</sup> Section 8 of the IGIS Act was amended to this end via the *Intelligence Services Legislation Amendment Act 2005*, Act No. 128 of 2005.

## Processing of complaints by administrative means

The bulk of complaints made to the office are of such a character that they can be processed administratively.

In the specific instance of complaints about the timeliness or otherwise with which ASIO processes security assessments for visa applicants, this entails oral and written communications between my office and the relevant functional area of ASIO, initially at the desk officer level, to ascertain the facts of the matter, to obtain a progress report and to report back to the complainant or their agent.

The level of contact is escalated, as necessary, depending on the individual circumstances of each case, but is something which can usually be undertaken administratively and at the working level.

On occasion complaints of this kind will be pursued more formally by means of a preliminary inquiry, or as a full inquiry.<sup>12</sup>

Of the remaining complaints which we receive and process administratively, the majority are dealt with without referral back to the AIC agency which is the subject of the complaint. There are a variety of reasons why this is so, including:

- the complainant holds genuine but misconceived ideas about the role and functions of the AIC agencies (e.g. actions are ascribed to AIC agencies which do not correlate to their function)
- the complainant has put forward suggestions which are highly unlikely (e.g. conspiracy theories), or
- the claims made by the complainant are manifestly unlikely or impossible (e.g. purported new mind control or related technologies).

Judgements in such matters are formulated on the basis of all of the material which has been presented by the complainants (i.e. not only new material, but materials which may have been presented previously), as well as our experience in dealing with similarly formulated complaints which we have received from other complainants.

Regardless of whether or not a complaint raises substantive issues, I can assure readers of this report that all complaints are taken seriously and that all complainants to this office are treated with courtesy and respect.

## Preliminary inquiries

The next means by which a complaint can be processed is by way of a preliminary inquiry.

Preliminary inquiries are provided for under section 14 of the IGIS Act and are made by the Inspector-General of the head of the agency which is the subject of complaint.

Preliminary inquiries will usually be pursued if there is a question about the jurisdiction of the IGIS which requires further information before it can be resolved, or in cases where further information is required from the agency in question, in order to form a view as to whether a fuller inquiry is required.

Preliminary inquiries are, as the name suggests, less formal than a full inquiry and will ordinarily be sufficient to address issues raised by a complainant, or any concerns which the Inspector-General might have, without the need to proceed to a full inquiry.

## Full inquiries

The final means of investigating a complaint, responding to a formal request from a responsible Minister for an investigation into a matter within my remit, or for me to pursue a matter on my own motion is by means of an inquiry, as provided for under Division 3 of the IGIS Act.

Inquiries of this kind are more commonly referred to as “full inquiries” in my office, so as to readily distinguish them from “preliminary inquiries”.

Full inquiries are not initiated lightly, as a number of statutory steps need to be complied with, and because I may utilise my full suite of special powers in the course of a full inquiry.

These powers, which are akin to those which are available to a Royal Commission, include the power to compulsorily obtain information and documents, to enter premises occupied or used by an AIC 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.

<sup>12</sup> A fuller description of the handling of such complaints is provided in the “ASIO” chapter of this report.

During 2007–08 I initiated 18 new full or preliminary inquiries. This compares with 13 such new inquiries initiated in the previous reporting period. Of these 18 new inquiries, three were own motion inquiries and 15 were the result of complaints.

Of the 15 complaints which resulted in either full or preliminary inquiries, three were lodged by either current or former AIC employees and relate in some way to their employment, while an additional five were lodged by external applicants for positions which were advertised by AIC agencies who were aggrieved either by the selection process or the manner in which the selection process was administered.

In 2006–07 my office received 65 complaints about AIC agencies which did not relate to the processing of security assessments by ASIO which were handled administratively. In 2007–08 this figure was 75.

Sixteen of the 75 complaints were made by current or former employees of AIC agencies about the agency for which they had worked compared to only five such approaches in the previous year.

In addition to this, seven out of the 75 complaints were received from external applicants for positions which were advertised by AIC agencies, who were aggrieved either by the selection or vetting processes.

During this reporting period my office also received 193 new complaints about alleged delays by ASIO in preparing security assessments on applicants for various visa categories, which I chose to handle administratively.

The receipt of 193 new complaints of this kind represents a very substantial increase on the 71 new immigration related complaints which OIGIS processed administratively during the previous year. There are several reasons why the number of immigration related complaints has increased substantially, but of particular significance is the advice to me that there was a 36% increase in the number of visa security assessments processed by ASIO during the year.

I should note that approximately half of the immigration related complaints received in 2007–08 were not actually “live” for ASIO i.e. they had not been referred by the Department of Immigration and Citizenship (DIAC), or DIAC had been asked for further information, or ASIO had already provided a security assessment to DIAC. Of course, such cases still add to the OIGIS workload.

A more general examination of the overall level of complaints made to this office is explored in the “Performance” chapter of this report.

### **Inspection and visits program**

During 2007–08 approximately two-thirds of the resources of OIGIS (other than those required for corporate matters) were devoted to the on-going inspection and visits program.

I consciously devote such a significant proportion of our resources to these activities because I believe very strongly in the positive effect that our regularly scheduled round-table meetings and targeted inspection activities, supported by occasional special projects, have on influencing normative behaviour within the agencies.

Fuller details of the various visits and inspection activities undertaken by OIGIS during 2007–08 are provided in the individual chapters on each of the agencies, but these activities have included:

- the scheduling of monthly meetings with senior ASIO managers so that we might discuss issues of topical and on-going interest to our respective agencies. (This replicates our long-standing practice of conducting round-table meetings of this kind in each of the other collection agencies)
- continuing to review relevant accountability documents for every request made by ASIO for the use of special powers warrants
- reviewing authorisations issued within ASIO to conduct investigations into persons of security interest
- reviewing a sample of ASIO’s accesses to Australian Transaction Reports and Analysis Centre (AUSTRAC) data

- regularly reviewing the application of privacy rules to products/records generated by ASIS<sup>13</sup>, DSD and DIGO, and the application of the privacy guidelines applicable to ONA and DIO
- reviewing all ministerial authorisations issued to the foreign intelligence collection agencies by their respective ministers
- reviewing ASIS operational files on a regular and targeted basis
- reviewing the application of relevant weapons guidelines and approval processes in respect of ASIS personnel
- regularly speaking to AIC staff at 'in-house' training courses, to promote awareness of the importance of accountability and acting legally and with propriety, and
- regularly visiting AIC offices and sites around Australia.

Even though our existing visits and inspection program is quite expansive, there is scope for this work to be varied, and to add new inspection tasks.

With the recent and proposed growth in the size of OIGIS, I intend to take advantage of this to initiate several pilot projects in 2008-09, within different AIC agencies.

I see these anticipated projects being not only useful exercises in themselves but as an aid to determining if they should become regular on-going inspection activities in the future.

I also plan to deepen my office's knowledge of the agencies for which I have oversight responsibilities so that I and my staff are well informed about the full range of their activities.

### Community outreach

Notwithstanding recent growth OIGIS is presently, and is likely to remain, one of the smallest budget-funded Commonwealth agencies.

Despite our relatively small size, I am keen for the office to be known to as many people as possible, so that those with a genuine grievance or concern about an AIC agency will know where they might turn for reliable information and assistance.

One vehicle through which awareness of the office is promoted is a website which provides details of the role and functions of the office, addresses frequently asked questions, and provides a repository for public versions of past inquiry reports and annual reports.

The website, which is located at < <http://www.igis.gov.au> > also provides guidance on lodging complaints. This guidance is provided in English and in 15 other community languages.

Given the potential for members of the public to be unsure which agency has the jurisdiction to handle complaints about the AIC, we maintain close relations with Commonwealth Ombudsman, and have provided copies of our brochures to the Ombudsman for the information of complainants to that office, whose concerns might be better directed to us.

OIGIS, in turn, also periodically refers complainants to the Ombudsman if the matters which are raised with us are more appropriately dealt with under that jurisdiction.

While it is unlikely that OIGIS will ever have the wherewithal or desire to advertise our existence via the mass-media, I am keen to take up opportunities as they present themselves, to meet with a variety of community groups, media representatives, student groups and academics, to promote a better and more widespread understanding of the activities of this office.

To this end, during 2007-08 I spoke at the following conferences, forums or community events:

- a forum arranged by the Law Faculty, University of Sydney (29 August 2007)
- the 'National Security for a Diverse Community', forum hosted by the Protective Security Coordination Centre in Canberra (24 October 2007)
- the Australian Institute of International Affairs, Canberra (22 November 2007)
- the Pakistan Association of Australia, Sydney (28 November 2007)
- a class of students engaged in intelligence and security related studies at the ANU, Canberra (20 March 2008)

<sup>13</sup> I temporarily suspended some but not all of our privacy review activities with respect to ASIS in April 2008, due to my confidence in the Service's internal compliance systems, but will review this position in the next reporting period.

- the Australian Federation of Islamic Councils, annual congress Sydney (17 May 2008), and
- the 'Above Board Public Accountability Forum', Australian National University, Canberra (24 May 2008).

In addition to the above, I was interviewed by a student/community radio station based in Sydney about the work of the office, and also responded to some queries from several journalists throughout the year on matters of topical interest.

I also met with representatives from policy bodies with an interest in the work of the AIC and this office, as well as visiting academics with an interest in the field.

### Training

As the AIC continues to grow, and more persons become professionally engaged in intelligence related activities, I believe it is essential for new starters and existing staff to have at least a general knowledge of the role and functions of my office, and the range of activities undertaken.

During 2007–08 my staff and I made at least 40 presentations to approximately 1250 staff drawn from across the six AIC agencies. These presentations were primarily delivered in Canberra, but a number were also provided at different locations across Australia.

The presentations are tailored to each agency or audience but all cover the history and activities of this office, the fundamental importance of agencies acting in accordance with the law and staff acting in an ethical manner and the need for the agencies to maintain public confidence by using their special powers and capabilities judiciously and professionally.

I am also occasionally invited to speak to specialist in-house forums hosted by AIC agencies which are also attended by their international counterparts.

In addition to delivering presentations on the role and functions of OIGIS, members of my staff and I have also attended several agency training courses either as participants or observers and I will look to doing so again during the next reporting period.

## International cooperation

During the reporting period, the office again received a number of international visitors. Notable among these were visits from a senior Canadian office holder, as well as senior ranking Japanese officials, who were interested in the manner in which Australia's intelligence and security oversight and review arrangements work.

### IIRA Conference 2008

As indicated in my previous annual report one of my staff and I attended the fifth International Intelligence Review Agencies (IIRA) conference, which was held in Cape Town, South Africa, in October 2006.<sup>14</sup>

The IIRA conferences have occurred approximately every two years on a rotating basis between Australia, Canada, the United Kingdom, the United States of America, South Africa and New Zealand.

The next IIRA conference is to be held in New Zealand in the second quarter of 2008-09, and the subsequent IIRA conference will be hosted by Australia, most likely in the second half of the 2010 calendar year.

I am on the working party which is assisting the New Zealand Inspector-General of Intelligence of Security (NZ IGIS) to plan and prepare for the forthcoming conference. I have been happy to assist the NZ IGIS in this task, as his office is even smaller than mine and he is grateful for our input and support, but also it will assist in planning for when Australia next hosts this event.

## Significant issues

In 2007–08 my office either had a direct involvement in, or monitored, a number of issues of public interest or significance.

A summary of these issues is provided in this section, with a further discussion of some of these matters also provided in relevant chapters elsewhere in this report.

<sup>14</sup> IGIS Annual Report 2007–2008, *ibid*, p.23.

## Review of ONA statutory independence

In the *Report of the Inquiry into Australian Intelligence Agencies* published in July 2004, the report's author, Mr Philip Flood AO, recommended that the Inspector-General should conduct periodic reviews of ONA's statutory independence.<sup>15</sup>

So as to facilitate future inquiries of this kind Mr Flood recommended, and the government of the day accepted, that it would be necessary to amend the IGIS Act, through the insertion of a new subsection, namely subsection 8(3)(c), which provides that, the IGIS may:

*"at the request of the responsible Minister or of the Inspector-General's own motion, ... inquire into any matter in relation to the statutory independence of ONA."*

Section 35(2) of the IGIS Act was amended at the same time so as to require that the IGIS include in his or her annual report, comments on any inquiry conducted in accordance with the new s8(3)(c). The above changes came into effect on 2 December 2005.<sup>16</sup>

As detailed in the IGIS Annual Report 2005–06, I initiated a review of ONA's statutory independence early in 2006.<sup>17</sup> In so doing, I utilised the longer-standing general inspection powers afforded to the IGIS under section 9A of the IGIS Act, rather than relying on the new subsection 8(3)(c). This was a suitable means of scoping and doing a preliminary exploration of the relevant issues. I concluded that inspection activity with the presentation of a report of my findings to the then Prime Minister, the Hon John Howard AC, on 15 December 2006.

I followed up this initial inspection work with a formal own motion inquiry, as provided for under subsection 8(3)(c) of the IGIS Act, initiated on 14 February 2007.

Work on this inquiry continued throughout much of the calendar year, and culminated in the delivery of a report of this inquiry to the incoming Prime Minister, the Hon Kevin Rudd MP, on 5 December 2007.

A fuller description of these processes and a general summary of my findings is provided in the chapter on ONA and at Annex 3.

## Inquiry into DIO analytic integrity

As a logical corollary to my various ONA inspection and inquiry activities, I determined that it would be timely for me to initiate a similarly themed inquiry into the other assessment agency within my remit, namely DIO.

While DIO does not have a statutory basis (unlike ONA), and the provisions of subsection 8(3)(c) of the IGIS Act apply exclusively to ONA, section 8(3)(a)(iii) of the IGIS Act provides that the IGIS may inquire, on his or her own motion, into any matter that relates to:

*"the effectiveness and appropriateness of the procedures of that agency relating to the legality and propriety of the activities of that agency"*

In interpreting the meaning of this section I believe that the concept of "propriety" can be readily construed to encompass within its ambit the notion that DIO assessment processes should be objective and free from improper direction or influence.

This being so, I wrote to the Minister for Defence, the Hon Joel Fitzgibbon MP, on 29 February 2008 to inform him of my intention to conduct an own motion inquiry into the propriety of the assessment activities of DIO.

Additional information about this inquiry is provided in the "DIO" chapter of this report and also at Annex 4.

This inquiry was close to finalisation at the conclusion of 2007–08. I will naturally provide details of our findings in the next IGIS annual report.

## Inquiry into Organisational Suitability Assessment processes

On 5 June 2007 I initiated an own motion inquiry into the Organisational Suitability Assessment (OSA) policies and procedures which are used by DIGO, DIO and DSD as part of determining the suitability of prospective and current employees to work in their respective agencies.<sup>18</sup>

The bulk of the work for this inquiry was conducted during 2007–08 and the inquiry concluded when I provided a report of my findings to the Minister for Defence on 15 February 2008.

<sup>15</sup> Flood, op. cit., p.106 and p. 180.

<sup>16</sup> These amendments were effected via the *Intelligence Services Legislation Amendment Act 2005*, Act No. 128 of 2005.

<sup>17</sup> IGIS Annual Report 2005–06, pp. 52–53.

<sup>18</sup> This inquiry was conducted in accordance with sections 8(2) and 8(3) of the IGIS Act.

My office has had a long standing interest in OSA policies and procedures across the AIC, given that my immediate predecessor as Inspector-General, Mr Bill Blick AM PSM, recommended that each of the AIC agencies should undertake mandatory psychological assessments of all current and prospective employees if they were not already doing so.

Mr Blick's recommendation was accepted by government and the AIC agencies then took action, as necessary, to give it effect.

Given that approximately seven years had passed since Mr Blick had concluded his inquiry, I considered that it was both timely and appropriate for OSA policies and procedures in the Defence intelligence agencies to be subject to review by this office.

The inquiry included consideration of documentation setting out each agency's OSA policies and procedures, an examination of the psychological testing instruments used, and interviews with staff, human resource managers, psychologists and security experts.

To assist me in this task, I engaged Workplace Research Associates to provide expert advice in the interpretation and assessment of the testing instruments, interview techniques and assessment processes. Workplace Research Associates provided expert advice in the fields of clinical psychology and psychometrics.

I am pleased to say that the general picture of the management of the OSA policies, procedures and practices within the Defence intelligence agencies is a positive one. While a small number of cases which were considered in the course of this inquiry raise issues, these would appear to be an unintended consequence of the OSA evolving to serve two distinct purposes. I concluded that opportunities exist to clarify these purposes and provide additional structure and rigour to the OSA process.

The Defence intelligence agencies have accepted my recommendations and have commenced implementation of them. I am quietly optimistic that if the changes I have proposed are fully implemented they will serve to enhance the utility, reliability and validity of OSA processes. A copy of the executive summary of my report is provided at Annex 5 of this annual report.

### **NSW coronial inquiry into Mr Brian Peters' death**

In recent annual reports I have made reference to an inquest which had been initiated by the NSW Coroner into the death of the late Mr Brian Peters, in East Timor, in October 1975.<sup>19</sup>

Mr Peters was one of five newsmen who were killed in the small village of Balibo, who have over time come to be known in media reporting and other commentary as the 'Balibo Five'.

The inquest into Mr Peter's death was conducted by the Deputy NSW Coroner, Magistrate Dorelle Pinch, and concluded when Magistrate Pinch formally brought down her findings on 16 November 2007.

My office had a particular interest in this inquest as my predecessor conducted an extensive investigation in 2000–01 into claims that intelligence information said to have been in the possession of DSD before the killings was not passed on to the government, and that if it had been, the Balibo Five could have averted their fate.

Mr Blick ultimately concluded that intelligence material meeting the above description did not exist, although there was intelligence material relating to journalists in Timor. Mr Blick further concluded that all relevant material held by DSD was passed to government and that DSD did not deliberately withhold a particular item of intelligence.<sup>20</sup>

It would not be appropriate for me to provide commentary on Magistrate Pinch's report, especially as it is readily available to anybody who wishes to read it.<sup>21</sup> I have, however, selected some extracts from the report, which touch on issues of relevance to this office.

<sup>19</sup> IGIS Annual Report 2005–06, pp. 8–9 and IGIS Annual Report 2006–07, pp. 25–26.

<sup>20</sup> An unclassified version of Mr Blick's report was published at Annex 3 to the 2001–02 IGIS Annual Report, pp. 82–90.

<sup>21</sup> This report can be found at the following address, following the links to 'Brian Peters' <[http://www.lawlink.nsw.gov.au/lawlink/coroners\\_court/ll\\_coroners.nsf/pages/coroners\\_findings](http://www.lawlink.nsw.gov.au/lawlink/coroners_court/ll_coroners.nsf/pages/coroners_findings)> (accessed 6 August 2008).

On the question of the level of cooperation received by the inquest from DSD and DSD's efforts to comply with various subpoenas, Magistrate Pinch noted the evidence:

*"... that a taskforce of nine DSD personnel conducted searches of all relevant hard copy files, an exercise which entailed collating literally thousands of documents and reading them ... In total, the number of staff hours devoted to this task was estimated at 2,500. Hence, I am satisfied that the most thorough and comprehensive search has been conducted to ensure compliance with the subpoenae."*<sup>22</sup>

On the question of access to classified and sensitive documentation, and the transparency of proceedings Magistrate Pinch wrote:

*"In recognition of the importance of all of the material to the inquest, the Commonwealth Government agreed that the classified documents could be inspected not only by myself, my Senior and Junior Counsel and their instructing solicitor, but also by Senior Counsel for Ms Tolfree, Mr Stratton S.C. Additionally, those Commonwealth officers – former Government Ministers and Departmental officials – who could give evidence of classified material were provided with the requisite authorizations by the Commonwealth Government under the Crimes Act 1914 and Intelligence Services Act 2001 to speak with my Counsel and instructing solicitor in order to provide Statements."*

*"It is also important to note that about 98% of the inquest was conducted in open session ... I am satisfied that all matters of substance are now in the public domain, even if not the specific detail."*<sup>23</sup>

Returning to the subject of the thoroughness of the searches undertaken by DSD, Magistrate Pinch wrote:

*"As noted previously, given the breadth of the subpoena that I issued, the extensive process of cross-referencing that was undertaken and the sworn evidence of [a senior DSD officer] about the searches undertaken to ensure compliance with the subpoena, I am satisfied that all extant classified material of possible relevance to the inquest was made available to myself and those authorized to view it."*<sup>24</sup>

In respect of allegations which were located at the centre of Mr Blick's inquiry in 2000–01, Magistrate Pinch wrote:

*"I have not seen any Sigint material, received prior to 16 October (1975), in which the Indonesians indicated any knowledge of the presence of either team of the Australian journalists in Balibo. Nor have I seen any intercept in which the Indonesians referred to an intention of killing the journalists."*<sup>25</sup>

Magistrate Pinch's ultimate finding, made in accordance with section 22(1) of the Coroners Act 1980 (NSW) was as follows:

*Brian Raymond Peters, in the company of fellow journalists Gary James Cunningham, Malcolm Harvie Rennie, Gregory John Shackleton and Anthony John Stewart, collectively known as "the Balibo Five", died at Balibo in Timor Leste on 16 October 1975 from wounds sustained when he was shot and/or stabbed deliberately, and not in the heat of battle by members of the Indonesian Special Forces ..."*<sup>26</sup>

I am hopeful that Magistrate Pinch's report and Mr Blick's report, taken in their totality, will serve to end speculation that DSD played any role in the death of the Balibo Five, either directly, or via an act of omission.

---

<sup>22</sup> *ibid*, Inquest report p. 12.

<sup>23</sup> *ibid*, p. 13.

<sup>24</sup> *ibid*, p. 77.

<sup>25</sup> *ibid*, p. 90.

<sup>26</sup> *ibid*, p. 129.

## **Inquiry into ASIO's dealings with Mr Izhar Ul-Haque**

Mr Izhar Ul-Haque is an Australian citizen of Pakistani heritage who, following investigations undertaken by ASIO and the Australian Federal Police, was arrested in April 2004 and charged with the offence of training with a proscribed terrorist organisation.

At the time of his arrest Mr Ul-Haque was a 21 year old medical student.<sup>27</sup>

Mr Ul-Haque's charges were brought in the NSW Supreme Court in October 2007 but were withdrawn on 5 November 2007, after Justice Michael Adams, of the NSW Supreme Court, found certain evidence against Mr Ul-Haque to be inadmissible. Justice Adams reasons for his decision were publicly released several days later.<sup>28</sup>

In his decision Justice Adams made a number of very critical comments about the conduct of certain ASIO officers. These comments were principally directed towards two ASIO officers who were assigned the designators B15 and B16 when giving evidence at Mr Ul-Haque's pre-trial hearings.

Having read the Judgment and reflected on the matter, I decided that it would be appropriate for me to commence an own motion inquiry into:

- actions taken by ASIO in respect of Mr Ul-Haque throughout 2003, and
- ASIO's policy, procedures and general practices on the interviewing of persons of security interest, as they stood in November 2003 and currently (if different).

My inquiry commenced on 14 November 2007 and was ongoing at the conclusion of the reporting period.

## **Administrative inquiry into the arrest of Dr Mohamed Haneef**

Dr Mohamed Haneef is medical doctor of Indian nationality who was arrested on 2 July 2007 at Brisbane Airport, on suspicion of various terrorism-related activities.

The circumstances of Dr Haneef's arrest, the laying and subsequent dropping of charges against him, and his ultimate voluntary departure from Australia have been a subject of considerable debate and not a little public controversy.

On 13 March 2008, the Attorney-General, the Hon Robert McClelland MP, announced the appointment of the Hon John Clarke QC, a retired judge of the New South Wales Court of Appeal, to conduct an inquiry into the above matter. Mr Clarke has been asked by the Government to report back by 30 September 2008.

Details of Mr Clarke's terms of reference and other important information relating to this inquiry are accessible via the inquiry's website.<sup>29</sup>

Although the following information was revealed outside of the 2007–08 reporting period, I should note that it is now a matter of public record that this office conducted an administrative review of some of the key ASIO records of its work in respect of Dr Haneef.<sup>30</sup> I had advised the outcome of this administrative review to the Attorney-General in December 2007.

<sup>27</sup> Mr Ul-Haque has subsequently completed his undergraduate medical studies and has recently been formally conferred the title of Doctor but as at the dates referred to in this section this was not the case. I have therefore referred to him by the title "Mr" for the purposes of this report.

<sup>28</sup> *R v Ul-Haque* [2007] NSWSC 1251, which is available at the following website: <[http://www.lawlink.nsw.gov.au/lawlink/caselaw/ll\\_caselaw.nsf/pages/cl\\_sc](http://www.lawlink.nsw.gov.au/lawlink/caselaw/ll_caselaw.nsf/pages/cl_sc)> and following the links (accessed 6 August 2008).

<sup>29</sup> The Clarke inquiry website is located at <<http://www.haneefcaseinquiry.gov.au/>> (accessed on 6 August 2008).

<sup>30</sup> *ibid*, unclassified ASIO submission dated 25 July 2008, p.3.

# parliament, legislation and liaison

## Overview

The 2007–08 period saw continuing high levels of public interest in, and debate about, the role, functions and activities of the AIC.

The interest of the public in such matters has been naturally fuelled by a succession of:

- high profile cases (e.g. Dr Mohamed Haneef, Mr David Hicks, Mr Mamdouh Habib)
- prosecutions (e.g. the conduct of pre-trial hearings and trials of 22 individuals in Melbourne and Sydney on terrorism related charges)
- legal judgements (e.g. Mr Izhar Ul-Haque, Mr Scott Parkin, Mr Jack Thomas)
- events (e.g. planning for, and the execution of, security arrangements for events such as the APEC leaders meeting in September 2007, the Olympic torch relay in April 2008, and the Papal visit in July 2008), and
- issues (e.g. the legal and other protections which should be afforded by the Australian government to Australian persons suspected of involvement in terrorist related activities, the exploitation of new technologies for surveillance purposes, the appropriateness of travel advisory notices, border control issues etc.).

At the core of many of these cases and issues is a debate about where the balance should lie between the security needs of the community and obligations of the state on the one hand, and the way of life most Australians enjoy and the civil liberties of individuals on the other.

Against this background it is not surprising that Parliament, which reflects and represents the sovereign will of the Australian people, should be a focal point for many of these arguments and debates.

Either side of the election of 24 November 2007, the Parliament was involved in the development, passage and implementation of various laws, some of which have or could have an impact upon the powers of the AIC agencies (and in consequence the monitoring and inspection function of this office).

As the business of government and public administration is enduring regardless of who is in power, a number of formal reviews were initiated, conducted and/or concluded during the reporting period which will also be influential in shaping the future legislative framework in which the AIC agencies and OIGIS operates.

The following chapter therefore briefly sets out some of the interactions of this office with parliamentary bodies during the reporting period, summarises legislative developments affecting the AIC in which OIGIS has an interest, and briefly details input I have made to some legislative reviews.

I have also included in this chapter, for the sake of completeness, some details of interactions with other government agencies and bodies, which might be characterised as attempts to aid the development and maintenance of public sector governance structures.

## Parliamentary oversight

### Parliamentary Joint Committee on Intelligence and Security

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) came into existence on 2 December 2005, as a successor to the Parliamentary Joint Committee on ASIO, ASIS and DSD.

The composition, role and functions of the PJCIS are prescribed under sections 28–29 of the *Intelligence Services Act 2001* (the ISA).

The PJCIS plays a significant role in overseeing the activities of the AIC agencies, particularly in respect of the administration and expenditure of the AIC agencies. This office has a complementary remit that is focused on the operational activities of the AIC agencies.

A new PJCIS was established when the 42nd Australian Parliament commenced business in February 2008 with a significant number of new members.

That there would be a significant change in the composition of the PJCIS could be reasonably anticipated as some former members of the PJCIS either chose to retire at the federal election, or did not win their seat in the election. The change of government also saw several former members of the committee promoted to Ministerial or Parliamentary Secretary positions meaning that they were no longer in a position to serve on the committee.<sup>31</sup>

The changed electoral landscape also saw two former Ministers in the Howard government become members of the PJCIS in the 42nd Parliament.<sup>32</sup>

The new Chair of the PJCIS is the Hon Arch Bevis MP, while the Hon Philip Ruddock MP serves as the Deputy Chair of this committee.

Although OIGIS is not one of the six AIC agencies and therefore not directly within the remit of the PJCIS, it has been my usual practice to meet with

the PJCIS two to three times a year to provide an overview of the work of my office and to discuss issues of mutual interest or concern.

During 2007–08 I did not meet formally with the PJCIS in either of its guises. I read nothing of consequence into this but believe that this is simply the by-product of a disrupted parliamentary schedule brought about as a consequence of the federal election, and the need for the new PJCIS to become fully conversant with the six AIC agencies.

Despite my lack of formal contact with the PJCIS, I monitored the work of the committee during the reporting period and the various reports it produced. My office and I also maintained a good and productive working relationship with the PJCIS Secretariat.

I expect to engage with the members of the PJCIS on a more direct and regular basis during the next reporting period, and would expect to liaise with it in planning for the International Intelligence Review Agencies conference which we will jointly host in Australia, in 2010.

### Senate Finance and Public Administration Committee

I prepared during 2007–08 to appear before the Senate Finance and Public Administration committee during its consideration of Supplementary Budget Estimates, Additional Estimates, and Budget Estimates, but was not called upon to do so.

### Parliamentary accountability – general

Despite not being required to attend before the above committee during 2007–08, I was nonetheless accountable to the Parliament through my responses to a range of questions on notice, through the tabling of my previous annual report, and through the provision of input to several parliamentary inquiries and other forms of legislative review.

<sup>31</sup> Senator the Hon John Faulkner was made Cabinet Secretary / Special Minister of State, the Hon Mr Anthony Byrne MP was made a Parliamentary Secretary reporting to the Prime Minister, while the Hon Duncan Kerr SC MP was appointed the Parliamentary Secretary for Pacific Island Affairs.

<sup>32</sup> Namely the former Attorney-General, the Hon Philip Ruddock MP, and the former Minister for Foreign Affairs, the Hon Alexander Downer MP.

## Legislative proposals and developments

### *Telecommunications (Interception and Access) Amendment Act 2007*

The Telecommunications (Interception and Access) Amendment Bill 2007 (the Bill) was introduced into the House of Representatives on 14 June 2007.

The purpose of the above Bill was to give effect to several recommendations made by Mr A.S. Blunn AO, in the report of an inquiry he had conducted into the then *Telecommunications (Interception) Act 1979*<sup>33</sup>, which had not been dealt with in previous legislative amendments.

The Bill was referred to the Senate Standing Committee on Legal and Constitutional Affairs for review on 21 June 2007.

I provided a submission to the Committee on 11 July 2007.

One of the provisions of the Bill of particular interest to me and upon which I offered comment was a proposal that very senior officers of ASIO would be able to issue authorisations requiring telecommunications carriers or carriage service providers to provide prospective telecommunications data for the duration of the authorisation (i.e. up to 90 days).

In my submission I supported this proposal but suggested that there would perhaps be merit in my office establishing a formal inspection process to periodically review any authorisations of this kind which may be issued.

I suggested that this inspection activity would be akin to my office's existing inspection activities in relation to special powers warrants issued to ASIO.

The Committee provided a report of its review of the Bill to the Senate on 1 August 2007.

In its report the Committee considered the proposal that senior ASIO officers be able to

issue authorisations in respect of prospective telecommunications data in prescribed circumstances, and adopted my suggestion as one of its recommendations, as follows:

*"The committee recommends that the Inspector-General of Intelligence and Security incorporate into his regular inspection program oversight of the use of powers to obtain prospective telecommunications data by the Australian Security Intelligence Organisation."*<sup>34</sup>

The Bill was passed by both houses of Parliament and received Royal Assent on 28 September 2007.

### *Telecommunications (Interception and Access) Amendment Act 2008*

The *Telecommunications (Interception and Access) Amendment Bill 2008* was introduced into the House of Representatives on 20 February 2008.

The purpose of this Bill was to amend the *Telecommunications (Interception and Access) Act 1979* to extend sunset provisions relating to network protection activities undertaken by network administrators in law enforcement and security agencies, to clarify reporting requirements for warrants, and to clarify that multiple telecommunications devices can be intercepted on a named persons warrant.

The Bill was also referred to the Senate Standing Committee on Legal and Constitutional Affairs for review.

I did not make a formal submission to the Committee in respect of this Bill but closely read its report when it was tabled on 13 May 2008<sup>35</sup>.

I also discussed the implications of the Bill with various agencies within my remit both prior to and subsequent to its passage into law.

The *Telecommunications (Interception and Access) Amendment Act 2008* passed through both Houses

<sup>33</sup> Review of the Regulation of Access to Communications, Canberra, August 2005 (aka The Blunn Review)

<sup>34</sup> Report of the Senate Legal and Constitutional Affairs Committee into the *Telecommunications (Interception and Access) Amendment Bill 2007*, dated 1 August 2007, paragraph 3.79. This report is accessible at the following location: <[http://www.aph.gov.au/Senate/committee/legcon\\_ctte/completed\\_inquiries/2004-07/telecommunications\\_interception/report/index.htm](http://www.aph.gov.au/Senate/committee/legcon_ctte/completed_inquiries/2004-07/telecommunications_interception/report/index.htm)> (accessed on 7 August 2008).

<sup>35</sup> Report of the Senate Legal and Constitutional Affairs Committee into the *Telecommunications (Interception and Access) Amendment Bill 2008*, dated 6 May 2007. This report is accessible at the following location: <[http://www.aph.gov.au/Senate/committee/legcon\\_ctte/ti\\_2008/index.htm](http://www.aph.gov.au/Senate/committee/legcon_ctte/ti_2008/index.htm)> (accessed on 7 August 2008).

of Parliament in May 2008, and received Royal Assent on 26 May 2008.

### **Independent Reviewer of Terrorism Laws Bill 2008**

On 17 March 2008, the federal member for Kooyong, Mr Petro Georgiou MP, introduced a private members bill in the House of Representatives for the purpose of establishing an independent reviewer of terrorism laws, and for related purposes.

The notion of creating an independent reviewer for terrorism laws is of interest to me because it aligns with the thinking of the Security Legislation Review Committee (SLRC), of which I was a member.

The SLRC was established in October 2005 to conduct a public and independent review of the operation, effectiveness and implications of amendments in six Acts relating to terrorism which were passed by the Commonwealth Parliament in 2002 and 2003.

The SLRC (more commonly referred to as the Sheller Committee after its chair, the Hon Simon Sheller AO QC), delivered a report of its findings to the then Attorney-General and to the PJCIS on 21 April 2006.<sup>36</sup> This report was in turn tabled in Parliament on 15 June 2006.

In that report the SLRC suggested that there would be utility in keeping Australia's security and terrorism related legislation under on-going rather than occasional review and contemplated various mechanisms for doing so.

*"From information available to the SLRC, there are several existing models set up to undertake ongoing reviews of security legislation, such as a public advocate, a public interest monitor (PIM) and an independent reviewer, which governments could consider."*<sup>37</sup>

Elsewhere in the SLRC's report, the Committee considered the workings of the United Kingdom's 'Independent Reviewer', and offered the following view:

*"If the Government is minded to establish a similar body in Australia, the SLRC favours it being attached to the office of the IGIS or the office of the Commonwealth*

*Ombudsman. The Independent Reviewer would be required to provide a report to the Attorney-General every twelve months, which the Attorney-General should be obliged to table in Parliament."*<sup>38</sup>

The *Independent Reviewer of Terrorism Laws Bill 2008* has not progressed, at this stage, beyond its introductory reading.

### **Independent Reviewer of Terrorism Laws Bill 2008 (No.2)**

On 23 June 2008, Senator the Hon Judith Troeth and Senator Gary Humphries, introduced the *Independent Reviewer of Terrorism Laws Bill 2008 (No.2)* into the Senate.

This Bill is expressed in virtually identical terms and has the same purpose as the private members bill introduced by Mr Georgiou (referred to above).

Further debate on this Bill had been adjourned at the conclusion of 2007–08.

### **Inspector-General of Intelligence and Security Act 1986**

As indicated in my previous annual report, I have been considering a range of possible minor and technical amendments to the IGIS Act.<sup>39</sup>

These possible amendments, which have been informed by my experiences as Inspector-General over the past four years, have been the subject of initial discussions with the new Government.

### **ALRC review of the Privacy Act 1988**

On 31 January 2006 the then Attorney-General, the Hon Mr Philip Ruddock MP, provided a reference to the Australian Law Reform Commission (ALRC) for an inquiry into the extent to which the *Privacy Act 1988* and related laws continue to provide an effective framework for the protection of privacy in Australia.

I met with the Commissioner in charge of this review, Professor Les McCrimmon on 15 March 2007, to discuss a range of privacy related issues pertaining to the AIC, with a focus on how the

<sup>36</sup> Report of the Security Legislation Review Committee, April 2006.

<sup>37</sup> *ibid*, paragraph 18.4.

<sup>38</sup> *ibid*, paragraph 18.8.

<sup>39</sup> IGIS Annual Report 2006–07, pp. 28–29.

privacy rules and guidelines which exist in the AIC are interpreted and applied.

The ALRC released a discussion paper on 12 September 2007, based on their research to that point and invited comment on it.<sup>40</sup>

I wrote to Professor McCrimmon in December 2007, responding to several of the proposals contained in the discussion paper which pertain directly to this office.

The final report of this review was delivered to the current Attorney-General, the Hon Robert McClelland MP, on 30 May 2008. The report had not been tabled in Parliament at the conclusion of 2007–08.

### ALRC review of client legal privilege

I included in my previous annual report a submission I had made on 1 June 2007 to the ALRC review of client legal privilege and federal investigations. The final report of this review was tabled in Parliament in February 2008.<sup>41</sup>

In that report the ALRC recommended, among other things, that the IGIS Act, the *Ombudsman Act 1976* and the *Human Rights and Equal Opportunity Commission Act 1986* be amended to state that where client legal privilege cannot be claimed over legal advice given to a Minister, an agency or an authority of the Commonwealth, this abrogation applies to litigation privilege as well as advice.

I welcome this recommendation and hope that it will be accepted and acted upon.

## Contributions to public sector governance

### Membership of the Administrative Review Council

The then Attorney-General, the Hon Mr Philip Ruddock MP, announced in a media release dated 26 April 2007, that I had been reappointed as a part-time member of the Administrative Review Council (ARC) for a further three years.

During 2007–08 I attended four ARC meetings, and participated in two ARC related teleconferences.

One of the major ARC related activities in which I was involved was the preparation of a report on *The Coercive Information-gathering Powers of Government Agencies*.<sup>42</sup>

The above report developed a list of 20 best practice principles as a guide to legislators and government agencies, to ensure fair, efficient and effective use of coercive information-gathering powers which hopefully strike a balance between an agency's objectives in using coercive information-gathering powers and the rights of those in relation to whom the powers are being exercised.

### Homeland and Border Security Review

On 22 February 2008, Prime Minister Rudd announced that he had asked the recently retired former Secretary of the Department of Defence, Mr Ric Smith AO PSM, to conduct a comprehensive review of homeland and border security arrangements in Australia, and to report back to him by 30 June 2008.<sup>43</sup>

The purpose of the Smith Review is to consider the roles, responsibilities and functions of departments and agencies involved in homeland and border security, and to also consider possible changes to optimise the coordination and effectiveness of Australia's homeland and border security efforts.

I met with Mr Smith and members of his review team during the period of his review, offering my perspectives on a range of issues relating to the AIC.

I understand that Mr Smith reported by the due date. There has not yet been any announcement of a response by the government.

### Providing advice on the outcome of complaints investigations

The Commonwealth Ombudsman, the Australian Public Service Commissioner and I had some discussions in 2006 about concerns that an overly strict interpretation of the *Privacy Act 1988* may have been inhibiting some public sector agencies from

<sup>40</sup> ALRC Discussion Paper 72, Review of Australian Privacy Law. A copy of this paper can be found at <<http://www.austlii.edu.au/au/other/alrc/publications/dp/72/>> (accessed 7 August 2008).

<sup>41</sup> ALRC Report No. 107, February 2008, Privilege in Perspective: Client Legal Privilege in Federal Investigations.

<sup>42</sup> ARC Report No. 48, May 2008, *The Coercive Information-gathering Powers of Government Agencies*.

<sup>43</sup> Prime Minister's press release dated 22 February 2008, entitled 'Homeland and Border Security Review' which can be found at: <[http://www.pm.gov.au/media/release/2008/media\\_release\\_0084/cfm](http://www.pm.gov.au/media/release/2008/media_release_0084/cfm)> (accessed 9 August 2008).

providing sufficient advice to complainants about the outcome of investigations into their complaints, especially where the outcome involved disciplinary action being taken against one of the parties.

The raising of this subject led to the creation of a small working group, which included a representative from my office, to examine this issue.

The end result of the above was the publication of a policy circular by the Australian Public Service Commission on 23 April 2008, about what information Australian Public Sector agencies can or should give complainants about the outcome of their complaints.<sup>44</sup>

### **Review of Part D of Protective Security Manual**

The Australian government Protective Security Manual (PSM) is issued by the Attorney-General's Department and endorsed by government.

The PSM is the principal means for disseminating Australian government protective security policies, principles, standards and procedures to be followed by all Australian government agencies for the protection of official information and resources.

The PSM is a living document and is subject to periodic review to take account of changing security policies, practices and circumstances.

The body which is responsible for ensuring that the PSM is accurate and up to date is the Protective Security Policy Committee (PSPC).

The PSPC has a program in place to progressively review every part of the PSM. This review is currently examining Part D of the PSM, which provides standards, procedures and guidance in relation to personnel security practices.

During 2007–08 my office was asked to participate in a working group which is examining certain aspects of Part D of the PSM. I was happy to accept this invitation and to contribute to this important work.

### **Liaison with other Commonwealth integrity agencies**

During 2007–08 I attended several meetings of heads of Commonwealth agencies which have a functional interest in promoting integrity and accountability in public administration.

I found these periodic meetings to be a useful forum for the exchange of ideas and of assistance in developing common approaches to issues of mutual interest or concern.

These meetings are likely to continue on a regular basis.

### **Renewed involvement with CrimTrac**

Immediately prior to commencing as Inspector-General, I served for a number of years as a Deputy Secretary in the Attorney-General's Department (AGD). During that time I was involved in the establishment of a new specialist agency, CrimTrac and was the first Chair of its Board of Management (2000–2004).

CrimTrac exists to provide specialist support to Australian police services through the provision of information and specialist investigative tools, and national criminal history record checks for accredited agencies.

Given my earlier involvement, I was happy to be invited in September 2007 to sit on CrimTrac's Audit Committee. I attended three meetings of the CrimTrac Audit Committee during 2007–08.

---

<sup>44</sup> APSC Policy Circular 2008/3, dated 23 April 2008, entitled Providing Information on Code of Conduct Investigation Outcomes to Complainants.

# performance

## Outcomes and outputs

In program budgeting terms, OIGIS has one specified outcome. The fact that the office has only one outcome reflects our relatively small size and the comparatively narrow focus of our activities (i.e. OIGIS is a small specialist review agency operating within a well defined niche).

The planned outcome for OIGIS is to offer (where possible and appropriate):

“Assurance that Australia’s intelligence agencies act legally, ethically and with propriety.”<sup>45</sup>

The approach to achieve this outcome is set out under item 2.1.1 of the OIGIS Budget Statements and commits OIGIS to:

- continue and expand the Agency’s inspection activities, which involve proactively monitoring and/or reviewing the activities of the AIC agencies, and
- where appropriate, investigate complaints about the activities of the AIC agencies, and when appropriate initiate ‘own motion’ inquiries (as provided for under the IGIS Act).<sup>46</sup>

## Performance indicators

The effectiveness of the office in achieving its objectives can be assessed against several key

performance indicators. The following measures take into account the office’s unique role and functions:

- the time taken to deal with complaints and conclude inquiries
- acceptance by ministers and agency heads of recommendations arising from inquiries
- the responses of agencies to issues raised arising from inspection activities, and
- the level of assurance the Inspector-General can provide that the agencies are conducting their activities legally, with propriety, and regard to human rights.

## Levels of complaint and inquiry

At the conclusion of 2006–07 two full inquiries and one preliminary inquiry remained open and were thus carried over into 2007–08.

The first of the on-going full inquiries referred to above was an own motion inquiry I had initiated on 14 February 2007 into the statutory independence of ONA’s assessments<sup>47</sup>, which was concluded on 5 December 2007.

The second of the on-going full inquiries was an own motion inquiry which I had initiated on 5 June 2007 into Organisational Suitability Assessment processes in DIGO, DIO and DSD. This was concluded on 15 February 2008.

<sup>45</sup> PM&C Portfolio Budget Statement 2008–09 – Office of the Inspector-General of Intelligence and Security, p. 177, (available at <<http://www.pmc.gov.au/accountability/budget/2008-09/pbs/oigis.pdf>> accessed on 29 July 2008).

<sup>46</sup> *ibid*, p. 177.

<sup>47</sup> The conduct of periodic inquiries into ONA’s statutory independence had been recommended Mr Philip Flood in the report of his review into Australian Intelligence Agencies published in July 2004, and is also specifically provided for under section 8(3)(c) of the IGIS Act.

The one outstanding preliminary inquiry carried over into 2007–08 related to a complaint about ASIO which had been made by a member of the public, which I was able to conclude on 27 July 2007.

I commenced three new own motion inquiries in 2007–08.

More broadly, OIGIS received 298 approaches from individuals with new or continuing complaints against a nominated AIC agency.

This global figure of 304 compares with 152 complaints/inquiries which were actioned in the previous reporting period. The 304 approaches described above can be broken down as follows:

- three inquiries carried over from 2006–07. (All of which were completed)
- three new own motion inquiries, compared to three in the previous reporting period. (Two of these inquiries remained open as at 30 June 2008)
- 15 new complaints leading to preliminary or full inquiries, compared to 10 such complaints in the previous reporting period. Two of these complaints concerned the timeliness of ASIO's immigration related security assessment processes which I had initially dealt with administratively (in 2006–07) but which I decided to pursue as preliminary inquiries in July 2007. Of the 15 new complaints leading to inquiries during the reporting period only one of these remained open as at 30 June 2008. In the previous reporting period 10 complaints led to preliminary or full inquiries<sup>48</sup>
- 15 complaints about alleged delays by ASIO in conducting immigration related security assessments which were either carried over from 2006-07 or where a former complainant contacted the office again seeking further assistance
- 193 new complaints about alleged delays by ASIO in conducting immigration related security assessments that were handled administratively rather than as preliminary or full inquiries. (This figure compares to only 17 such complaints in 2004–05, 26 such complaints in 2005–06, and 71 complaints of this kind in 2006–07<sup>49</sup>)

- 25 approaches from persons who have previously been in contact with OIGIS who were either seeking a re-examination of their original complaint or who wished for an inquiry to be conducted into a new matter of complaint. This figure is compared to 28 in the previous reporting period, and
- 50 approaches from individuals who have not previously been in contact with OIGIS who wished to lodge a complaint against a specifically identified an AIC agency. There were 37 such complaints in the previous reporting period.<sup>50</sup>

Some of the above figures require clarifying comment to place them in a proper context.

Since the creation of the office in the 1986–87, the average number of new matters or complaints which were formally pursued as preliminary or full inquiries averages out at 20.63 per annum. In the five year period between 2002–03 and 2006–07, the average was 23.6 per annum.

In 2007–08 I commenced 18 preliminary or full inquiries (i.e. 3 own motion inquiries and 15 complaints).

As can be seen from the above figures, the number of preliminary and full inquiries which were commenced in 2007–08, is just below the long term average (18 compared to 20.6), but there is a bigger differential when compared with the current five-year average (18 inquiries compared to 23.6).

As was indicated in my previous annual report, this gap is linked to how I have chosen to handle some of the more straightforward matters, particularly the upsurge in complaints I have received about the timeliness with which ASIO is conducting security assessments on applicants for various forms of visas.

In 2004–05, I received a total of 31 complaints on immigration related matters and pursued 14 of these as preliminary inquiries.

In 2005–06, I received a total of 34 complaints on immigration related matters, pursuing six of these as preliminary inquiries and two as full inquiries.

My decision to process 22 immigration related complaints in the period between 2004 and

<sup>48</sup> Tabular information relevant to these two dot points is provided at Annex 1, Table 1.

<sup>49</sup> Summary information relevant to these two dot points is provided at Annex 1, Table 3.

<sup>50</sup> Summary information relevant to these two dot points is provided at Annex 1, Table 2.

2006 as either full or preliminary inquiries rather than administratively, has served to increase the five-yearly average number of preliminary and full inquiries.

By way of contrast in 2006–07, I received a total of 71 complaints on immigration related matters. I pursued all of these complaints administratively, while in 2007–08 the office received 193 separate complaints of this kind.

A more detailed explanation of the spike in the number of immigration related security assessment complaints we have received is provided elsewhere in this report, in the chapter devoted to ASIO.

Suffice to say that I will continue to monitor ASIO's performance in this area and adjust my approach as necessary.

While immigration related complaints increased markedly in the reporting period, OIGIS also received 75 non-immigration related complaints where an AIC agency was named, or where reference was made to the AIC as a whole, which I chose to handle administratively.

Wherever possible my office processes complaints about AIC agencies which do not proceed to preliminary or full inquiry within a few days.

In addition to the 304 cases identified above, 34 other individuals contacted the office with concerns which did not directly refer to or involve an AIC agency (this is compared to a total of 30 in 2006–07). Each of these contacts was handled administratively.

As I have reported in previous annual reports, a significant proportion of the complaints or contacts received from members of the public come from individuals who are clearly suffering from genuinely held but nonetheless imaginary concerns.

These delusions have many forms but frequently involve the complainant expressing an unshakeable belief that one or other of the AIC agencies, or some other agency of the state, is using mind control or other advanced technologies (including surgical implants) to adversely affect their behaviour and quality of life.

Other typical beliefs include conspiracy theories linking various government and non-government bodies together to subjugate the rights of individuals, and more commonly, the purported use of bugging and other forms of surveillance to silence persons with unusual or unorthodox views.

While my office considers each case on its merits and attempts to deal with all complainants in an honest and respectful manner, the fantastical nature of some of the claims which are presented to this office are such that there is little to be gained by engaging in a full scale investigation, and indeed it would only serve to fuel delusions of this kind if we were to do so.

In addition to persons with manifestly delusional concerns the office is also contacted from time to time by persons who wish to raise matters which clearly fall outside of our jurisdiction, or who wish to provide "tip-off" information and are unsure where else to turn.

In the case of matters falling outside of my remit, it is our practice to refer complainants to an appropriate review body which does have the power to investigate their complaints (this is frequently the Commonwealth Ombudsman or a State-based Ombudsman).

Any tip-off information received which appears credible will ordinarily be passed to the National Security Hotline (NSH), or other agencies, as appropriate.

As the NSH has the capacity to disseminate security related tip-offs to appropriate government agencies in a more timely manner than OIGIS, we encourage persons with information of this kind to contact the NSH directly on 1800 123 400 (this is a free call from anywhere within Australia).

Of course, if the information to be imparted concerns allegations of illegality or impropriety on the part of any member of the AIC, it is still appropriate for these matters to be brought to the attention of my office.

## Timeliness

In the five years between 1 July 2003 and 30 June 2008, the average time taken for inquiries to be completed was 104.31 days. The average time taken to finalise preliminary and full inquiries in 2007–08 was 100 days, compared to 95 days for the previous year.

The five day increase reflected above is largely explained by the intensive and in-depth nature of the ONA statutory independence inquiry, and the Organisational Suitability Assessment

inquiry completed by this office during the reporting period.

More generally, I do not believe that it is possible or desirable to apply rigid target times for completing preliminary or full inquiries, and to use performance against such deadlines as a gauge of effectiveness. This is because a variety of factors, many of which are beyond the powers of this office to control or influence, have an impact upon the timeliness with which an inquiry can be handled.

Such factors include but are not limited to, the complexity and range of issues raised by the complainant or to be considered in the course of an own motion inquiry, the accessibility of relevant files and documents to be reviewed, the availability of agency staff, and fulfilling other procedural requirements.

Notwithstanding the above, it must always be my objective to be as timely as possible in completing inquiries and I will endeavour, if feasible, to reduce the average time taken in 2008–09.

## Acceptance of recommendations

It is not usual for an agency to reject recommendations which are made by an Inspector-General following the conclusion of an inquiry.

There are many reasons why this is the case but this situation usually pertains because recommendations for change are not made lightly, generally involve prior consultation with the agency which is directly concerned and hopefully reflect a practical response to a particular issue or concern.

In all instances where I made formal recommendations in reports of inquiries which were concluded during 2007–08, these were accepted by the relevant agency.

## Responsiveness to issues raised

Following inspection visits to each of the AIC agencies, it is the agreed practice that I write to the relevant agency head on the outcome of the visit, and where appropriate, offer suggestions on how procedures could be improved.

I also meet on a regular basis with senior members of the collection agencies and use these meetings to

discuss topical issues, or to follow up on issues raised in correspondence.

During 2007–08, I made a number of suggestions for procedural changes and reforms. These suggestions were generally accepted and acted upon.

I should also note that the intelligence and security agencies continue to seek the views of my office on draft policies and procedures. Where I have an interest or a concern about a particular activity, which cannot be adequately canvassed in our periodic meetings, I do not hesitate to seek a specific briefing.

In the vast majority of cases where I have sought such briefings, or additional information, my requests have been agreed to without question or qualification.

I am generally encouraged by the willingness of the agencies to seek and accept input from this office and believe that it demonstrates a genuine and continuing commitment on their part to conduct their activities legally and with propriety.

## Level of assurance

I can state unequivocally that the number of persons contacting my office is greater now than at any time during which OIGIS has existed.

While this might be regarded by some as an outward sign that the AIC is under stress or is problematic, having analysed these various contacts I am reassured that this upward trend does not indicate that the AIC agencies are running out of control, or that their activities are causing more offence. Rather, to date it is a by-product of the AIC's increasing size and public profile, its greater engagement with the community, and its increasing operational tempo as it seeks to respond to new challenges.

I also believe that the increasing number of contacts made to this office reflects a greater knowledge of the existence of my office and a greater preparedness by some elements in the community to invest their trust in it. (This is especially true in regard to complaints about the timeliness with which security checks are undertaken for immigration related purposes).

My staff and I make a significant number of presentations on the role and functions of this office, within the AIC, and also to community groups who sit outside the AIC and I believe that this also encourages more people to make contact when they have a concern about an AIC agency.

As reflected in the above figures individuals with a complaint about the AIC seem to have no trouble in identifying that an office of this kind exists and then making appropriate representations.

This process is aided considerably by our Internet website which makes information about the role and functions of the IGIS readily accessible to a larger number of people than has ever previously been the case.

I have been planning a redesign of the office website to make it even more accessible and user-friendly. This project did not advance as quickly as I would have liked during 2007–08 because of the demands of other work, but I am committed to seeing it concluded in 2008–09.

### Summary

As indicated in “The Year in Review” chapter of this report, I noticed an increase in the number of contacts and complaints received from current or former members of the AIC, or applicants for positions with AIC agencies, raising personnel management related grievances or concerns about recruitment practices. When viewed in isolation these complaints could easily be written off as being of limited significance but when taken together may provide some evidence that the AIC agencies are experiencing varying degrees of organisational stress as a consequence of their growth. At the same time it must be acknowledged that the number is not large in a relative sense. This is naturally something which I will continue to monitor.

There was a marked increase in the number of complaints to my office about alleged delays by ASIO in making immigration related security assessments. ASIO was not at fault in a significant number of these matters, but it is one area of significant ongoing challenge for ASIO.

I can report that during the course of my office’s inspection activities, and as a consequence of my inquiry related work, relatively few substantive concerns were identified and each of these was corrected or addressed by the relevant agency. A somewhat greater number of procedural issues were raised, particularly through the office’s inspection activities, and these were also corrected or addressed satisfactorily.

I am very appreciative of the efforts of my staff in responding to the increasing demands placed on OIGIS and in fulfilling the planned program.

# Australian Security Intelligence Organisation

## What ASIO does

ASIO is Australia's national security service. Its 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.

ASIO's role is to identify and investigate 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 ASIO Act.

Security is defined in the ASIO Act as:

- espionage
- sabotage
- politically motivated violence
- the promotion of communal violence
- attacks on Australia's defence system, or
- acts of foreign interference.

It also includes the carrying out of Australia's responsibilities to any foreign country in relation to threats to security.

ASIO collects information using intelligence methods (such as human sources, special powers authorised by warrant, and through its liaison relationships) as well as from published sources.

The ASIO Act does not limit the rights of persons to engage in lawful advocacy, protest or dissent. ASIO does not carry out criminal investigations nor have powers of arrest, but does conduct activities

in parallel to Australian law enforcement agencies in matters where there is a security dimension as well as possible criminality.

ASIO does not have the statutory authority to engage in surveillance of ordinary members of the community going about their lawful business.

ASIO has to obtain external approval for use of its most intrusive powers.

Further information about ASIO, the Attorney-General's guidelines and the ASIO Act, can be found on ASIO's Internet homepage located at <<http://www.asio.gov.au>>.

ASIO also produces an unclassified annual report to Parliament.

## Significant issues

### New Attorney-General's Guidelines

Section 8A of the ASIO Act provides that the Attorney-General may issue guidelines to the Director-General of Security in respect of the performance by ASIO of its functions or the exercise of its powers, and must issue guidelines in relation to the performance by ASIO of that part of its functions which relate to politically motivated violence.

On 12 October 2007 the then Attorney-General, the Hon Philip Ruddock MP, announced that he had issued a new set of guidelines to the Director-General of Security<sup>51</sup>. A copy of the new guidelines is provided at Annex 7.

<sup>51</sup> Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its functions of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence). Available at <<http://www.asio.gov.au/About/Content/AttorneyAccountability.aspx>> (accessed 7 August 2008). The Guidelines are also at Annex 7 of this report.

The new guidelines are based on two similarly themed directives issued by the then Attorney-General in 1992, but with updates to reflect technological developments and contemporary practices, remove repetitious and confusing language, and consolidate the guidelines into a single document.

I was consulted during the development of the guidelines and am supportive of a number of the changes which have been made. I am especially supportive of the emphasis which is placed on ensuring proportionality in investigations.<sup>52</sup>

There are some aspects of the new guidelines which require ASIO to confirm its existing policies or develop new internal procedures. Two examples of this are:

- the former guidelines required ASIO determine in advance whether an investigation should be undertaken at a preliminary or general level. The new guidelines remove this distinction, and
- the new guidelines specifically provide for ASIO to collect and maintain a comprehensive body of reference material to contextualise intelligence and to maintain a broad database (based on that reference material) against which information can be checked and assessed<sup>53</sup>. A previous prohibition against speculative data-matching has also been removed.

I have been or am being consulted on the development of ASIO's new internal policies and procedures, and am naturally keen to ensure that ASIO maintains stringent business rules and security standards in respect of these important issues.

It is also likely that my office's inspection program will be revised once the new internal processes referred to above have been settled.

## Ul-Haque Inquiry

In "The Year in Review" chapter of this report, I referred to a major inquiry which I initiated on 14 November 2007, into certain aspects of an investigation by ASIO into Mr Izhar Ul-Haque.

Mr Ul-Haque is an Australian citizen of Pakistani heritage who, following an investigation undertaken by ASIO and the Australian Federal Police (AFP), was arrested in April 2004 and charged with the offence of training with a proscribed terrorist organisation.<sup>54</sup>

My decision to initiate this inquiry was prompted by the comments of Justice Michael Adams of the NSW Supreme Court in a decision dated 5 November 2007.<sup>55</sup>

In his decision, Justice Adams found that certain records of interview between the accused (i.e. Mr Ul-Haque), and the AFP which had been tendered as evidence were inadmissible because:

- they were influenced by oppressive conduct toward Mr Ul-Haque by ASIO and AFP officers (with reference to s.84 of the *Evidence Act 1995*)<sup>56</sup>
- the truth of certain admissions made by Mr Ul-Haque was likely to have been adversely affected by the methods of questioning employed by two ASIO officers, known to the court as B15 and B16 (with reference to s.85 of the *Evidence Act*)<sup>57</sup>, and
- admissions had been obtained through improper conduct by the ASIO officers, B15 and B16 (with reference to s.138 of the *Evidence Act*).<sup>58</sup>

The Judgement in this matter also stated that one or both of B15 and B16 had committed the offences of false imprisonment and kidnapping at common law and under s.86 of the *Crimes Act 1900* (NSW); the tort of false imprisonment; and unlawful trespass at the residence of Mr Ul-Haque. However, neither B15 or B16 had been charged with any such offences.

<sup>52</sup> Clause 10.4 of the new guidelines.

<sup>53</sup> Clause 6.2 of the guidelines.

<sup>54</sup> Mr Ul-Haque was charged with offences under s102.5(1) of the *Criminal Code*. That is, "between 12 January 2003 and 2 February 2003, in Pakistan, he did receive training with respect to combat and the use of arms from a terrorist organisation, namely Leshkar-e-Taiba, ... knowing that the said organisation was a terrorist organisation."

<sup>55</sup> *R v Ul-Haque* [2007] NSWSC 1251.

<sup>56</sup> *ibid.*, paragraphs 94–99.

<sup>57</sup> *ibid.*, paragraphs 100–103.

<sup>58</sup> *ibid.*, paragraphs 104–106.

While it is not my role to reach any conclusions about whether criminal offences have been committed, my functions under the IGIS Act do include inquiring into the legality and propriety of the activities of ASIO, and providing a report and making recommendations in that regard. Having read the Judgment and reflected on the matter, I decided that it would be appropriate for me to commence an own motion inquiry into:

- actions taken by ASIO in respect of Mr Ul-Haque throughout 2003, and
- ASIO's policy, procedures and general practices on the interviewing of persons of security interest, as they stood in November 2003 and currently (if different). This included interviews conducted during the execution of entry and search warrants as well as those in other circumstances, and the interaction of these activities with activities of the AFP.

My inquiry was ongoing at the conclusion of the reporting period.

### **Increase in the number of immigration-related complaints**

The Department of Immigration and Citizenship (DIAC) has overall responsibility for the administration of visas being granted to specified categories of people wishing to enter Australia.

In some instances DIAC will require persons wishing to enter Australia to complete DIAC Form 80 - *Personal particulars for character assessment*.

DIAC reviews each completed Form 80 it receives and refers some of these to ASIO (in accordance with its statutory obligations and its own internal requirements and procedures), so that ASIO can conduct security checks on these applicants, as part of the visa application process.

Over the past two reporting periods there has been a noticeable increase in the number of complaints I have received about the timeliness with which ASIO processes security assessments for immigration applications.

As detailed in the "Performance" chapter of this annual report, this office received a total of 193 new complaints in 2007–08, compared to 71 such complaints received in 2006–07<sup>59</sup> and 26 complaints of this kind in 2005–06.

I sought special briefings on a number of occasions during the year from ASIO senior managers about the changes ASIO was introducing to improve its procedures for the processing of security assessments. The purpose of these briefings and meetings was to:

- ascertain if there were any apparent reasons for the recent rise in complaints to my office (as mentioned above), and
- maintain visibility of the implementation of an ASIO-DIAC project to increase the accuracy and speed of information passing between the two agencies.

It is my belief that one significant contributing factor in the substantial rise in immigration related complaints to my office is a growing awareness within immigrant communities in Australia and among migration agents of the existence and remit of my office. I would also note advice to me that ASIO increased by 36% the number of visa security assessments it processed in 2007–08.

Further detail on the general conduct of my inquiries in response to these complaints is contained elsewhere in this chapter.

### **ASIO's continued growth, litigation and review workload**

As mentioned in my previous annual reports, ASIO has received increased funding from the government over recent years to allow it to respond promptly and effectively to the challenging security environment in which it operates.

During the reporting period ASIO made a major contribution to the security arrangements for a number of high-profile events (e.g. various APEC meetings, the Olympic torch relay, and the initial planning of World Youth Day).

ASIO's continued growth has necessarily led it to reconsider and adjust its internal structures to better meet the needs of the Organisation. I have been briefed about these matters.

While I cannot reveal too much about these changes for obvious security reasons, any reader of the nation's classified advertisements will be aware that ASIO has been attempting to upgrade the number of legally qualified individuals it has at its disposal.

<sup>59</sup> Annex 1 Table 3 of the IGIS Annual Report 2006–07 noted that 74 immigration related complaints had been handled administratively that year. This included three matters carried over from the previous reporting period.

This need is a necessary and appropriate response to ASIO's growing counter-terrorism litigation caseload.

It is a matter of public record that during 2007–08 trials or pre-trial hearings commenced relating to the prosecution of 22 individuals on terrorism related charges in both Melbourne and Sydney.

In addition to these prosecutions, ASIO also had a direct interest in a range of other high profile legal actions.

ASIO has also committed significant resources to providing information to a number of external security reviews such as the Clarke Inquiry into the case of Dr Mohamed Haneef.

### **Monthly meetings and special briefings**

Immediately prior to the commencement of 2007–08, I began moves to set up regular monthly meetings with senior ASIO personnel. The first of these meetings was held in August 2007.

I believe that these meetings have proven to be a useful vehicle for improving communication between my office and ASIO senior managers.

Our monthly meetings provide a forum for candid discussions about issues arising out of the inquiry and inspection activities of my office, and to exchange views on other issues in which we have a common interest.

These meetings have also provided a mechanism for me to receive regular updates on outstanding correspondence, when necessary, and for me to respond to any requests for feedback, clarification or comment levied on my office.

The meetings are also an opportunity for ASIO to provide me with special briefings when the need arises. The inquiry, inspection, monitoring and review activities of the office frequently turn up subjects or issues on which I require or would like additional information.

On those occasions when I require special or additional briefing on a particular subject I will either raise it for consideration at the monthly meeting or write to the Director-General of Security seeking his assistance. If the issue is more pressing, I may also directly contact the relevant senior manager.

The Director-General of Security, Mr Paul O'Sullivan, has not placed any restrictions on who I might seek briefings from, or to whom I might speak within ASIO.

I met with senior ASIO officers on at least 22 separate occasions, in addition to our monthly meetings, to discuss issues such as the Attorney-General's Guidelines, the retention of data and destruction of records by ASIO, the progress of various legal actions, immigration related security checking, the internal structure of ASIO, various inspection and inquiry tasks, and in regard to specific operational matters.

I would like to thank those ASIO officers who have contributed to the free flow of information and views between our respective agencies.

### **Training**

The workload of the office has increased substantially in the period since my initial appointment. Despite this I place very significant store on personally delivering as many presentations and training sessions as I can to each of the AIC agencies, including to ASIO staff.

During this reporting period, my staff and I delivered a total of 11 presentations which were tailored for ASIO specific audiences.

My staff and I also spoke to other ASIO staff when making presentations to various courses where participants were drawn from across all AIC agencies.

A number of opportunities were also identified for my staff and me to observe or participate in ASIO training. I was particularly grateful for the training provided to a number of OIGIS staff on the use of a particular information system, which has enhanced the office's capacity to undertake independent checks of various electronic records.

## Inspection activities

### General scope

ASIO has a strong domestic focus and is the AIC agency most likely to directly interact with members of the Australian public. Hence it is logical and appropriate that its intelligence collection activities should be subjected to more intensive and more frequent review by my office than the other agencies of the AIC.

During this reporting period my office conducted 55 inspection visits to ASIO's various offices compared to 56 separate inspections in the previous reporting period. While the number of visits is consistent between the reporting periods, there was a significant increase in the number of OIGIS staff allocated to these activities and the duration of some of these inspections.

### Range of current and new inspection activities

As with previous years, my office inspected records associated with a wide range of ASIO activities including warrant operations, approvals to commence an investigation, reviews of investigations, access to sensitive financial records, liaison with law enforcement agencies, use of assumed identities and exchange of information about Australian persons with foreign liaisons.

My office also conducted a new inspection project, relating to intelligence information on currently serving politicians.

Details of the outcome of these inspection activities, to the extent that security considerations permit, are summarised below.

### Project to review the retention of intelligence information on currently serving politicians

Since becoming Inspector-General, the activities of OIGIS have largely been focussed on areas such as ASIO's new powers and capabilities. However, I have also reflected that it is important not to lose sight of more "traditional" concerns about intelligence and security agencies, for example that they do not act in a politically partisan manner.

With this in mind, I decided that reviewing the manner in which ASIO handles any intelligence information regarding currently serving parliamentarians would be a worthwhile activity for my office.

In March 2008 I wrote to the Director-General of Security proposing a new inspection project covering these matters. In broad terms the project involved a review of relevant ASIO policies and procedures and then identifying and reviewing a sample of records which might include reference to currently serving parliamentarians.

My decision to commence this inspection activity was not precipitated by any particular event, nor did it reflect a view that ASIO had acted in ways that could be said to be politically partisan. Rather, it simply reflects my view that this is an important inspection activity that my office should undertake from time to time and an increase in the resources available to me.

At the end of the reporting period the project was largely completed. The preliminary outcome of this activity was that there was very little of concern identified. I was minded at the conclusion of the reporting period to make a number of minor suggestions to the Director-General of Security to tighten procedures (and indeed have since done so). It is my intention to follow this up in the forthcoming reporting period.

### Warrant operations

ASIO has access to a range of special powers to assist it to perform the functions set down for it by Parliament. These special powers can only be used in limited circumstances following the issue of a properly authorised warrant. The range of special powers warrants available to ASIO includes:

- telecommunications interception
- entry and search
- computer access
- listening device
- tracking device (on persons or objects), and
- postal and delivery service articles.

As the exercise of these special powers will often not be apparent to the subject of the warrant and are by their nature highly intrusive, special powers warrants should only be considered for use when other, less intrusive, means of obtaining information are likely to be ineffective or are not reasonably available.

The Attorney General is the issuing authority for all special powers warrants, with the exception of questioning and questioning and detention warrants, which can only be obtained from a properly qualified issuing authority (i.e. a Federal magistrate, or a judge).

In those cases where it is decided that the best way ahead is to obtain a special powers warrant, ASIO must:

- coordinate the preparation of the submission which is ultimately to be put to the Attorney-General
- ensure that all of the information which is put forward is double-checked and as accurate as possible
- advise relevant functional areas when a warrant has been endorsed, so that they might initiate collection activities
- monitor and respond to any issues which arise while the warrant is active
- coordinate and develop reports to the Attorney-General on the utility of each warrant to ASIO, and
- commence the process again, should it be decided to renew a warrant.

### Outcome of warrant inspections

ASIO's warrant operations constitute some of its most sensitive and highly classified activities. While I can speak in general terms about our inspection findings, there are naturally some issues which, for reasons of security, cannot be included in this report.

Each year my staff and I aim to inspect every warrant request by ASIO. This objective was achieved in 2007–08, with the exception of documentation associated with one warrant. The one outstanding warrant request will be reviewed at the first available opportunity in 2008–09.

The inspections go beyond simply seeing and 'ticking off' each warrant. My staff examine each set of warrant related papers to be satisfied that:

- the intelligence or security case that ASIO has made in support of the application is soundly based and all the legislative requirements are met

- the individuals named in these warrants are actually identical with, or closely linked to, persons of serious security interest (this is particularly relevant where a 'B-Party' telecommunications interception warrant is being sought)
- appropriate internal approvals for the request have been obtained
- the Director General of Security has identified in writing those individuals who may execute the warrant, or communicate information obtained from the warrant
- reports to the Attorney General on the outcome of executed warrants are factual and provided in a timely manner, and
- the activity concerned did not begin before, or continue after, the period authorised by the warrant.

Based on my own observations and information which is fed back to me by my staff, I can report that the quality of the warrant requests and other warrant related documentation which goes to the Attorney-General have been of a consistently high standard.

The records reviewed indicated that in each case where a special powers warrant was issued in 2007–08 that ASIO had:

- reasonable and sufficient grounds for seeking the warrant
- provided sufficient information for the Attorney-General to make an informed decision
- appropriate procedures in place to check that the conditions of the warrant were being fulfilled
- reported the results of warrant operations to the Attorney-General in a timely manner, and
- maintained the key accountability documents on the relevant files for examination by me and my staff.

In past annual reports I have made particular reference to my interest in ASIO's use of B-Party warrants.<sup>60</sup>

B-Party warrants are targeted at telecommunications services which a person of security interest is likely to be in contact with, rather than actually being owned by that person.

<sup>60</sup> IGIS Annual Report 2006–07, p.43.

On the basis of the office's inspection activities and various briefings which I have received, I continue to be reassured that this type of warrant is used sparingly.

On those occasions when such warrants were sought, I was satisfied that all other practical methods of identifying the telecommunications services of the person of interest had been exhausted, or that it was not otherwise possible to intercept the services of the persons of interest.

Notwithstanding this generally very favourable assessment of the overall manner in which warrants are processed in ASIO, my staff and I did identify several issues which merit comment.

### Unauthorised telecommunications interception

During 2007–08 my office identified two instances where an error or fault which was within ASIO's control led to unauthorised telecommunications interception. This compares with one such instance during the previous reporting period. In both cases the intercepted data was destroyed and all related records were purged from ASIO's electronic databases.

In addition, my staff identified or had brought to their attention, four other instances where technical or human error within ASIO's control had the potential to cause unauthorised collection to occur, but such collection did not eventuate. This compares with three such instances during the previous reporting period.

While any instance where unauthorised interception occurs, or has the potential to occur, is serious, I am pleased with the low number of instances during the reporting period. As I noted in my previous annual report<sup>61</sup>, this achievement is even more commendable when one considers that the overall number of services intercepted under telecommunications interception warrants was greater than the previous reporting period and the legal framework under which warrants are issued is quite complex.

In addition to the above cases, I can also report that no instances where the actions of bodies external to ASIO resulted in, or could potentially have resulted in, unauthorised collection occurring were identified. This compares to five such instances in the previous reporting period.

### Interception management systems

In addition to my office's frequent and regular review of ASIO's warrant documentation files, my staff also periodically interrogate ASIO's interception management systems.

The purpose of undertaking these checks is to gain independent assurance that collection is only occurring against telecommunications services which are listed on properly authorised warrants, and within the specified collection period.

I can advise that none of the checks my staff conducted during 2007–08 revealed any instances of inappropriate or otherwise unauthorised collection.

### Reports of warrant activity

In addition to ensuring that all warrant documentation is as complete and accurate as possible when submitted to the Attorney-General or an Issuing Authority (in the case of questioning and questioning and detention warrants), ASIO is also required to provide a written report to the Attorney-General on the outcome of every warrant which is issued to it.

Reports on telecommunications interception warrants issued to ASIO under the *Telecommunications (Interception and Access) Act 1979* must be furnished within three months of their expiry or revocation, whereas there is no mandatory deadline for reports on the outcome of the other forms of warrants available to ASIO.

ASIO brought to my attention one instance where the outcome of a telecommunications interception warrant was not provided to the Attorney-General within the requisite timeframe. This was due to an administrative oversight. However, I am confident that ASIO continues to make its best endeavours to guard against errors of this kind.

I consider it noteworthy that ASIO brought this error to my attention rather than leaving my staff to detect it. I believe this speaks well of ASIO's commitment to meeting its obligations and also sends a strong message to its staff that while mistakes will naturally happen they should be acknowledged and corrected expeditiously.

<sup>61</sup> IGIS Annual Report 2006–07, p.44.

## Questioning warrants/questioning and detention warrants

The capacity for ASIO to access questioning warrants and/or questioning and detention warrants derives from Division 3 of Part III of the ASIO Act. Division 3 was inserted into the Act by the *ASIO Legislation Amendment (Terrorism) Act 2003*.

A summary of the main features of Division 3 of Part III is provided in the IGIS Annual Reports for 2003–04 and 2005–06<sup>62</sup>.

My position remains that either I or a senior member of my staff will attend for at least the first day where an individual is questioned under such a warrant and that further attendance will be determined on a discretionary basis.

No warrants were issued under either section 34E (questioning) or section 34G (questioning and detention) of the ASIO Act during 2007–08.

### Approval to investigate – procedures

Staff employed within ASIO cannot commence an investigation into a person or organisation unless a formal and auditable process is followed.

The Attorney-General's Guidelines (referred to earlier in this chapter) set out in general terms the circumstances in which ASIO may obtain intelligence relevant to security. These guidelines are supplemented by detailed internal policies and procedures, the application of which is monitored by this office.

Taken together, the Attorney-General's Guidelines and ASIO's internal policies and procedures require that before an investigation can be commenced a specific approval must first be obtained.

The initial steps involved in this process require the requesting officer to take steps to properly identify the person or organisation to be investigated, to detail how that person or organisation is linked or potentially linked to a matter of security interest, and to also detail the objectives, nature and proposed duration of the investigation.

The work classification level within ASIO at which an approval can be given is dictated by the nature and sensitivity of the investigation being proposed. The more sensitive or intrusive the proposed investigation, the more senior the approving officer in ASIO has to be.

During this reporting period my staff conducted 26 separate file reviews of investigation approvals, spread over 34 days. These inspections were conducted in Canberra and at ASIO's various interstate offices. During these inspections, the following checks were made:

- whether there were reasonable grounds for the request to conduct an investigation
- whether the level of the authority was appropriate for the proposed investigative activities
- if the proposed duration of the approval was appropriate
- what limits, if any, had been placed on the investigative activity, and whether these were appropriate and reasonable
- if those checks undertaken were conducted within the authorised period
- whether a formal review of an investigation has taken place at the completion of the investigation or where a renewal has been sought, and
- whether supporting paperwork had been placed on file.

### Approval to investigate – inspection results

As with most of the office's inspection activities, detailed discussion of specific cases is not possible but some general comments can be made on the issues noted in the course of the inspection activities.

Overall I was satisfied with the manner in which the approval process worked during the reporting period. Many, if not most, of the approvals reviewed were of a high standard.

Nonetheless I continued to provide feedback to encourage improvement in standards and consistency in approach across ASIO.

The inspections revealed that a few senior officers were regularly using the same form of words when putting limits on particular investigative activities. My feedback was consequently largely focused on the comments and guidance provided by senior ASIO officers when approving investigations.

<sup>62</sup> IGIS Annual Report 2003–04, Canberra, October 2004 pp. 15–18; 2005–06, Canberra, October 2006 pp. 11–12.

I actively seek to discourage the use of formulae, as it does not show evidence that the approving officer has considered the case on its individual merits, nor does it provide meaningful guidance to case officers who have to act in accordance with this advice.

Instances of minor procedural defects (e.g. where expiry dates have not been properly inserted, the creation of duplicate authorities, and instances where some relevant supporting documentation was not on file) were also noted but these were very much the exception and did not point to any systemic concerns.

The Attorney-General's Guidelines require that each approval which is issued should be reviewed, at least annually. In practice this means that a formal review is conducted within a reasonable period following the expiry of an approval, or prior to a new approval on the same subject being sought.

In almost all cases reviews were completed prior to an approval being renewed or within a reasonable period following their expiry.

I was particularly supportive of some policy changes that ASIO instituted over the reporting period, in respect of investigations of persons who have proven to be of long-standing relevance to security. These policy changes will lead to increased transparency in respect of the regular review and continuation or cancellation of such investigations.

### **ASIO and law enforcement agencies**

ASIO naturally has quite close links to law enforcement agencies in all Australian jurisdictions. These links are necessary because there is often a nexus between persons who are planning for or engaged in criminal activities, and persons of security interest.

Cooperation is also necessary in order to plan effectively for major events (such as APEC and World Youth Day) where Australia has obligations with respect to the protection of visiting foreign dignitaries.

As has been the case for many years, whenever OIGIS staff visit ASIO's state offices they review those files which detail ASIO's interactions with locally based law enforcement agencies. No substantive concerns arose from review of these records.

### **Interoperability issues**

During 2007–08 the Commissioner of the Australian Federal Police (AFP), Mr Mick Keelty APM, established a committee to examine, inter alia, the effect of interactions between ASIO and the AFP on its national security operations.

The committee comprised the Hon Sir Laurence Street AC KCMG QC, Mr Ken Moroney AO APM and Mr Martin Brady AO. The committee has come to be known by the shorthand title of 'The Street Review'.

I met with the committee during the course of its inquiries and offered my perspectives on a range of issues of interest to the Committee.

*The Street Review: a review of interoperability between the AFP and its national security partners*<sup>63</sup> was released to the public on 12 March 2008.

The report of the Street Review contains a number of recommendations which I believe will help to ensure that ASIO's activities complement those of the AFP.

The Street Review recommendations covering a joint decision making framework, a joint operations protocol, counter-terrorism prosecution guidelines, and training enhancement should all assist in this regard.

I had particular regard to the recommendations of the Street Review in the context of my inquiry into the UI-Haque matter.

### **Information obtained from AUSTRAC**

Since 2000 ASIO and I have each been party to separate Memorandums of Understanding (MOUs) with the Australian Transaction Reports and Analysis Centre (AUSTRAC). These MOUs set out the circumstances under which:

- ASIO might access and use information which is collected and kept by AUSTRAC, and
- OIGIS would monitor ASIO's access to, and use of, this information.

A new IGIS – AUSTRAC MOU was signed on 29 August 2007. A copy is at Annex 6 to this report.

The purpose of this was to reflect the legislative changes that had been introduced under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) and the *AML/CTF Amendment Act 2007*.

<sup>63</sup> <[www.afp.gov.au/\\_data/assets/pdf\\_file/71833/The\\_Street\\_Review.pdf](http://www.afp.gov.au/_data/assets/pdf_file/71833/The_Street_Review.pdf)> (accessed 29 August 2008).

As mentioned in some detail in my previous annual report, the AML/CTF Act provides a legal framework in which “designated agencies” are able to access, in strictly controlled circumstances, information which is held by AUSTRAC, with ASIO and OIGIS being “designated agencies” for the purposes of the Act.<sup>64</sup>

The ASIO-AUSTRAC MOU was also reviewed during the reporting period, with the intention of the parties making a new agreement sometime in 2008–09.

The OIGIS – AUSTRAC MOU requires that I provide a certificate to the Attorney-General on the annual basis, specifying whether or not ASIO has complied with the requirements under the ASIO – AUSTRAC MOU.

A compliance certificate of this kind was provided to the Attorney-General in respect of 2006–07 on 9 January 2008. I am happy to advise that my office identified no issues of concern.

During 2007–08 my staff conducted eight Canberra-based AUSTRAC related inspections compared to nine inspections in the previous year. My staff also review relevant records in ASIO state offices whenever the need or opportunity presents itself.

In the course of these inspections a small number of procedural issues were identified, none of which were of material effect.

In the future I expect to be in a position to send the annual compliance certificate to the Attorney-General in a timelier manner than occurred in this reporting period.

### Access to taxation information

Section 3EA of the *Taxation Administration Act 1953* provides that the Commissioner of Taxation may disclose tax information to an authorised ASIO officer if the Commissioner is satisfied that the information is relevant to the performance of ASIO’s functions under subsection 17(1) of the ASIO Act.

ASIO’s access to taxation information is the subject of an MOU between the Director-General of Security and the Commissioner of Taxation, and also ASIO’s internal guidelines and procedures.

ASIO accesses tax information infrequently due to the particular sensitivities associated with information of this kind. I consider this to be a sensible and prudent approach.

### Use of assumed identities

It has been the practice of my office for many years to periodically review ASIO’s assumed identity registers. During this reporting period, one such inspection was conducted (compared to two inspections in 2006–07).

The registers reviewed record all instances where an assumed identity has been officially allocated to an ASIO officer for operational purposes, details what documentation has been obtained to support that identity, sets out what limitations have been imposed on the use of the identity, identifies who has authorised the use of the identity, and also details any variations which have been authorised following the original issuing of an assumed identity.

On the basis of the last inspection and an additional briefing, I concluded that the authorisation, allocation and use of assumed identities by ASIO staff continues to be tightly controlled, and that adequate internal checking and review mechanisms exist to ensure that allocated assumed identities are not being misused or abused.

Due to the high standards that ASIO has displayed in this area over a long period of time, and the competing priorities of my office’s inspection program, I have decided not to inspect ASIO’s assumed identities register during 2008–09. Instead, I will simply require that ASIO provide me with:

- copies of the ASIO internal audit reports on compliance with the assumed identities provisions of the *Crimes Act 1914* and the *NSW Law Enforcement and National Security (Assumed Identities) Act 1998*, and
- a certificate at the end of the financial year which satisfies the requirements of section 15XUA of the *Crimes Act 1914*.

### Exchange of information with foreign liaisons

During the last reporting period I commenced a new inspection project on the manner in which ASIO shares information about Australian persons with foreign intelligence services and overseas law enforcement agencies.

In preparation for that review ASIO developed a new electronic template to ensure it applied a consistent approach to the release of such information to its foreign liaisons.

<sup>64</sup> IGIS Annual Report 2006–07, p.28.

My office continued this inspection activity during 2007–08, by examining the relevant records from a particular ASIO liaison office, over a three month period.

We will continue to monitor, on an occasional basis, that ASIO continues to tailor its approach in each instance, having due regard to the overseas agency with which it is dealing, the type of information being requested or provided, and the potential use to which that information might be put.

## Complaints and inquiries

As at 30 June 2007 I had the following inquiries in train into complaints about ASIO, which were carried over into this reporting period:

- one preliminary inquiry, and
- 17 administrative inquiries concerning the timeliness with which ASIO processed immigration related security checks.

All of these inquiries were concluded early in the reporting period, with the exception of two immigration-related matters which were later progressed as preliminary inquiries (see below).

In the period following the commencement of the new reporting period on 1 July 2007 until 30 June 2008, I initiated three full inquiries into new complaints about ASIO (which is the same number as in the previous reporting period) and 11 preliminary inquiries (compared to five in the previous period).

In addition to the preliminary and full inquiries, the office received 251 other complaints specifically about ASIO, from individuals seeking to reopen former complaints, or making new complaints raising specific concerns. This compares to 199 such complaints in 2006–07.

Of these 251 new complaints which were handled administratively, 193 were concerned with the timeliness with which ASIO processed immigration related security checks. My handling of these complaints is discussed below.

## Operational interactions between ASIO and members of the community

As noted above, I initiated full inquiries into three new matters during 2007–08. All of these matters dealt with operational interactions between ASIO and members of the public.

The most complex of these investigations is an inquiry I initiated on 14 November 2007 into the actions taken by ASIO throughout 2003 in respect of a Mr Izhar Ul-Haque. This inquiry necessarily required me to examine ASIO's policy, procedures and general practices on the interviewing of persons of security interest.

The other two full inquiries were conducted in response to complaints received about the actions of ASIO officers at their respective family homes.

- In the first instance the complainant felt intimidated by the presence of ASIO officers at the family home during the execution of an entry and search warrant, and subsequently during visits by ASIO officers to return seized items and in the conduct of interviews.
- In the second instance the complainant felt intimidated by an ASIO officer coming to the family home to seek an interview.

In both cases I found that the evidence did not support a finding that ASIO officers had acted improperly, or that any ASIO officer had intended to act in a threatening, harassing or intimidating manner. To the contrary, the evidence pointed to an active intention by the ASIO officers concerned to avoid offence, rather than to cause it.

Nonetheless, these cases highlight the potential for members of the public to feel anxiety as a result of contact with ASIO and the need for ASIO to remain sensitive to this.

I also conducted one preliminary inquiry, at the request of two community organisations, into whether a member of the public was under surveillance and being harassed by ASIO. The community organisations made this request out of concern for the well-being of that person.

In cases such as this, it is not possible for me to confirm whether or not a specific individual is a person of interest to ASIO or to any of the other AIC agencies. The reason for this is that to do so could provide a 'back door' means by which any person who is of genuine or legitimate security interest could determine whether or not they have come to the attention of the AIC. This would obviously be self-defeating for the intelligence community, and would also serve to undermine the capacity of this office to fulfil the objectives for which it was established.

In this case, I was able to advise that my inquiries revealed no evidence of any illegal or improper conduct by ASIO.

### Archives related complaints

ASIO routinely receives a large number of requests, via the National Archives of Australia (NAA), for access to its records which are more than 30 years old. These records are in the so-called 'open period'.

Such applications range from straightforward requests from people seeking the records of a family member, through to professional researchers who submit multiple applications for considerable volumes of records.

Upon receipt of an application for access to open period records, the *Archives Act 1983* provides that there can be up to 90 days to:

- examine records to which access is sought
- determine if those records, or parts of those records, are exempt records, and
- release any record, or part of a record, that is not exempt.

I conducted one preliminary inquiry into the timeliness with which ASIO processes applications for access to open period records.

This inquiry was concerned with whether ASIO had processed a number of high volume applications as expeditiously as possible, having proper regard to the 90 day period described above and also to the proper examination of those records.

I found that ASIO had acted with propriety both in respect of its prioritisation of applications and in respect of its treatment of certain cases, where the volume of material that had been requested is so large as to make it impossible to complete for the required examination within 90 days.

I was also satisfied that ASIO is taking reasonable steps to improve the timeliness of its processing of archival material, to the extent it can.

In 2007–08 I also received two queries from members of the public seeking to clarify why ASIO had not given them prior notice that records cleared for release included personal information about themselves. I dealt with these queries administratively.

The Director-General of Security continues to provide my office with quarterly progress reports on ASIO's overall performance in relation to archives requests. I have also been advised that on 21 May 2008, ASIO and the NAA signed a section 35 agreement under the *Archives Act 1983* to establish more formal arrangements for the examination and handling of ASIO's exempt records.

### Release of RCIS papers

During 2007–08 ASIO was also actively engaged in a major activity, preparing for the public release of records associated with the Royal Commission on Intelligence and Security (RCIS).

The RCIS was conducted by the late Justice Robert Hope between 1974 and 1977 and involved a root and branch review of the operation of the agencies which then comprised the AIC. The NAA released many of the records associated with the RCIS on 27 May 2008.

### Concerns about recruitment experiences

As touched upon elsewhere in this report, I noted an increase in the number of complaints made to my office about recruitment and selection matters.

During 2007–08 I conducted two preliminary inquiries into complaints about recruitment activity undertaken by ASIO. In both cases, I found ASIO's administrative arrangements to be generally satisfactory.

### Concerns held by former employees

Sections 8(5) and 8(7) of the IGIS Act limit my capacity 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, or friction between two individuals).

When a complaint to my office relates to this type of grievance, my 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 *Intelligence Services Act 2001* for employees of ASIO and ASIS respectively.

Having said that, I do have some flexibility in regard to situations where:

- the complainant has exhausted his or her avenues for internal redress and there are related policy or procedural matters that I can usefully pursue, and/or
- a complainant is a former, 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.

I conducted three preliminary inquiries and one administrative inquiry during the reporting period into employment-related grievances from ex-employees of ASIO, as follows:

- two matters dealt substantially with the complainant's difficulties in pursuing compensation claims, and
- two matters related to the complainants suffering illnesses which they attributed, at least in part, to issues of alleged workplace bullying. One of these inquiries was still ongoing at the conclusion of the reporting period.

I have reviewed ASIO's policy regarding workplace bullying and the avenues for employees to raise concerns of this nature. I believe that the policy is sound and provides all employees with clear guidance on acceptable behaviour and the range of options available to staff to address areas of concern.

Both the ASIO Staff Association and senior management have assured me that agency staff are made aware of their responsibilities in this regard, and that there is not an agency-wide culture of accepting workplace bullying.

### Assessment of security equipment

I received one complaint about the procedures that ASIO applies to the listing of equipment in the Australian Government Security Equipment Catalogue (SEC).

At the conclusion of my preliminary inquiry, I was satisfied that the relevant procedures (which require equipment owners to apply for SEC listing and to provide samples of their equipment for evaluation and possible testing) are appropriate. The procedures ensure that:

- each equipment owner/supplier who applies for listing is treated fairly, and
- Commonwealth entities who purchase the products listed in the SEC can be certain that the products are fundamentally sound, suited to their purpose, and can be readily supported.

### Immigration related complaints

As mentioned in the "Significant Issues" section at the beginning of this chapter, there has been a noticeable increase over the past two reporting periods in the number of complaints received about the timeliness with which ASIO processes security assessments for immigration applications.

A total of 193 new complaints were received in this reporting period. This compares with 71 complaints received in 2006–07 and 26 such complaints in 2005–06.<sup>65</sup>

The complainants varied from permanent protection visa applicants to skilled migrant and spouse visa applicants. (See Table 3 of Annex 1 for a detailed breakdown).

These complaints were variously lodged by the complainants themselves, migration agents, family members or Members of Parliament acting on their behalf, or following a referral by another government agency such as the Commonwealth Ombudsman.

<sup>65</sup> Annex 1 Table 3 of the 2006–07 IGIS Annual Report noted that 74 immigration related complaints had been handled administratively that year. This included three matters carried over from the previous reporting period.

All of the 193 new complaints received during 2007–08 were handled administratively.

The administrative processing of these complaints means that my office makes an informal inquiry of ASIO to verify that the case has actually been referred to ASIO by DIAC, to determine the length of time a request for a security assessment has been with ASIO, and to receive a brief outline of the nature of the case. Based on this I can, in many cases, make a judgement on the legality or propriety of ASIO's handling of the case.

During this reporting period my administrative inquiries revealed a small but significant number of cases where administrative errors within ASIO had caused considerable delays in the completion of security assessments.

While this was regrettable, I was able to engage the relevant functional area of ASIO about the causes of these errors. In response ASIO has improved its management systems to ensure the better tracking of immigration related cases, so as to reduce the risk of similar errors occurring in future.

ASIO also initiated an increase in staff resources allocated to liaise with my office on these matters. This has resulted in improved responsiveness to my queries over the year, and also provided a greater level of detail to me on the circumstances of each case.

I am appreciative of the efforts of the ASIO officers who assisted my office during 2007–08, as it has allowed me to respond to complainants more quickly and fully than might otherwise have been the case.

In those cases where a judgement cannot be made based on ASIO's response to an administrative inquiry, preliminary or full inquiries can be commenced to investigate the matter further.

In the reporting period I commenced two preliminary inquiries into immigration related cases (relating to complaints which had originally been received in 2006–07).

The first case highlighted some deficiencies in communication between DIAC and ASIO that have since been addressed under a project to enhance the IT connectivity between these agencies.

In the second case the applicant's security assessment was not straightforward and had therefore taken longer to progress than would otherwise be the case. Having said that, the case had been additionally delayed by an avoidable administrative error that led to processing delays.

# Australian Secret Intelligence Service

## What ASIS does

ASIS was established in May 1952 and operated under a series of government directives until it was put onto a statutory footing in October 2001, with the coming into effect of the *Intelligence Services Act 2001 (ISA)*.

ASIS's various functions are set out at section 6 of the ISA, and its activities are regulated by a series of ministerial directions, ministerial authorisations (MAs) and privacy rules, made pursuant to the ISA.

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.

ASIS's other functions include communicating such intelligence in accordance with government requirements, conducting counter-intelligence activities and liaising with intelligence or security services, or other authorities, of other countries.

So as to discharge its functions 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.

The foreign intelligence collection priorities for ASIS and other members of the AIC are established

in a planning document that is endorsed and regularly reviewed by the National Security Committee of Cabinet.

Further information about ASIS is available at <<http://www.asis.gov.au>>.

## Significant issues

### New Minister

When the Rudd Government was sworn in on 3 December 2007, the Hon Stephen Smith MP replaced the Hon Alexander Downer MP as the Minister for Foreign Affairs

As the Minister for Foreign Affairs Mr Smith also automatically assumed executive responsibility for ASIS.

I am aware through our inspection and review activities, and other senior level briefings, that ASIS has devoted considerable effort to providing detailed briefings to the new Minister, and to put in place secure systems so that they might communicate with him as necessary when he is not located in Canberra.

### Growth and expansion

ASIS, like the other AIC agencies, continues to remain in a period of expansion and growth.

The total appropriation granted to ASIS in the 2008–09 Commonwealth Budget was \$199.2 million,<sup>66</sup> compared to \$162.5 million<sup>67</sup> in the 2007–08 Budget.

<sup>66</sup> DFAT Portfolio Budget Statement 2008–2009, ASIS statement available at: <[http://www.dfat.gov.au/dept/budget/2008\\_2009\\_pbs/2008-2009\\_FA+T\\_PBS\\_06\\_ASIS.pdf](http://www.dfat.gov.au/dept/budget/2008_2009_pbs/2008-2009_FA+T_PBS_06_ASIS.pdf)> (accessed 9 August 2008).

<sup>67</sup> DFAT Portfolio Budget Statement 2007–2008, ASIS statement available at <[http://www.dfat.gov.au/dept/budget/2007\\_2008\\_pbs/2007-2008\\_FA+T\\_PBS\\_06\\_ASIS.pdf](http://www.dfat.gov.au/dept/budget/2007_2008_pbs/2007-2008_FA+T_PBS_06_ASIS.pdf)> (accessed 9 August 2008).

In the case of ASIS I have sought and received updates on the rebalancing of organisational structures and priorities within ASIS flowing from this, and on recruitment, training, and accommodation issues.

I like to maintain a watchful eye on the organisational health of each AIC agency and do this by periodically seeking access to, or being briefed about, staff survey findings and results. I did so with respect to ASIS during the 2007–08.

### Special briefings

In seeking to fulfil my various duties as Inspector-General I have regular dealings with the Director-General of ASIS, his senior managers, and a range of less senior officers who hold key positions.

I have now worked with Mr Irvine for an extended period and found him to be candid and forthright in our various dealings, but also a strong supporter of the role and functions of this office.

In addition to our regularly scheduled inspection visits (some of which are described elsewhere in this chapter), I met with senior ASIS officers on at least 18 separate occasions during 2007–08.

These briefings covered a wide variety of issues ranging from personnel management issues to particularly sensitive operational activities.

Due to the inherent sensitivity of these subject matters, I am not able to make further comment in this report.

I continue to appreciate the responsiveness of ASIS to my various requests for briefings.

### Visits and contact with staff

In the four years since my initial appointment as Inspector-General, I have tried to meet with senior ASIS officers prior to the commencement of their overseas postings.

The purpose of these meetings is to remind each ASIS officer of the role and functions of this office, and to stress the expectations being placed upon them.

I believe that these meetings serve an important purpose by reinforcing with ASIS officers that their actions are subject to on-going external scrutiny no matter where they are posted, and that they are obliged to conduct themselves in an appropriate manner at all times.

I also meet occasionally with heads of mission who are being sent to posts where ASIS officers are present, to discuss any issues they might have prior to their departure. This is a useful means of sharing information relevant to our respective functions.

### Training

During 2007–08 I delivered several presentations to ASIS's new intelligence officer trainees, to explain the role and functions of my office and to talk generally about governance and accountability structures.

Members of my staff and I also regularly make presentations to ASIS officers when we speak at AIC training courses at which they are participants.

The frequency with which we make these presentations is less than for ASIO and DSD, but is nonetheless at an appropriate level given the respective sizes of these agencies and the interests of this office.

I am hopeful that in the coming reporting period members of my staff and I might either directly observe or be involved in several training activities involving ASIS personnel so that we might obtain a greater depth of understanding of the work of the Service.

### Access to AUSTRAC data

ASIS has entered into an MOU with AUSTRAC which sets out the terms and conditions under which it may in the future obtain direct access to financial transaction reporting information via various AUSTRAC databases.

I had several meetings with representatives from AUSTRAC and ASIS during 2007–08 with a view to mapping out appropriate future inspection activities for this office.

It is my intention to institute regular inspections of ASIS's records during 2008–09 to ensure that ASIS complies with the conditions under which its access to AUSTRAC derived financial transaction reporting information has been provided to it.

## Inspection activities

### Range and scope

During the reporting period I maintained many of the features of the usual inspection program. Inspection activities undertaken during the reporting period included:

- reviewing all MAs issued to ASIS
- reviewing all submissions made to the Minister for Foreign Affairs
- reviewing and reconciling weapons related authorisations
- regularly inspecting current operational files
- on-going monitoring of compliance with the ASIS privacy rules, and
- conducting regular roundtable meetings to discuss issues of common interest.

### Review of Ministerial Authorisations

Section 8(1) of the ISA requires the Minister for Foreign Affairs to issue a written direction to the Director-General of ASIS setting out the circumstances when ASIS must obtain the Minister's authorisation to undertake certain activities.

Ministerial Directions are reviewed periodically to ensure their currency, when external circumstances change or new priorities emerge, or when there is a change of Minister or both.

In those instances where there is a change of Minister, pre-existing Ministerial Directions have continuing legal effect until such time as they are formally revoked, or overridden, by the issue of a new, properly authorised, direction.

Mr Smith issued several new Ministerial Directions to ASIS, in accordance with section 8(1) of the ISA, in January 2008.

The directions are similar in nature to those which were in place prior to him becoming the Minister for Foreign Affairs.

Section 32B of the IGIS Act requires that when directions of this kind are issued a copy must be provided to the Inspector-General as soon as practicable after the direction is given. This occurred.

These directions are classified and therefore cannot be released publicly.

My office reviews all MAs to ensure that they conform to the requirements of the ISA and the terms of the Ministerial Directions to which ASIS is subject.

During 2007–08 six inspections were conducted during which several issues were identified about which clarification or comment was sought from the Director-General of ASIS. Most of these issues were of an essentially technical and administrative nature and of minor concern.

I was satisfied that the MAs examined by this office were appropriate and in conformity with the requirements of the ISA.

### Ministerial submissions

Whenever my staff and I conduct a review of MAs, we also review all of the other submissions which the Director-General puts to the Minister.

The content of these submissions is necessarily sensitive, dealing as they do with a wide range of topical subjects affecting ASIS upon which the Director-General believes the Minister should be kept informed.

As a consequence of reviewing ASIS's ministerial submissions I sometimes seek briefings from the Director-General.

I am grateful to the Director-General for providing me with continuing access to these documents.

### Authorisations related to training in/or use of weapons for self-defence purposes/self-defence techniques

Subclause 1(5) of Schedule 2 of the ISA requires the Director-General to provide me with copies of all approvals issued by the Minister of Foreign Affairs in respect of training in the use of a weapon for self-defence purposes, the provision of a weapon for self-defence purposes, or the delivery of training in other self-defence techniques.

I am confident that I had visibility of every authorisation which was issued during this reporting period.

While I cannot report the precise number of authorisations which were issued I can advise that it was not an excessive number, and in my view each request for an authorisation was soundly based and proportionate to the requirements of ASIS.

I am satisfied that the powers afforded to ASIS under Schedule 2 of the ISA are being used professionally and as intended.

Clause 3 of Schedule 2 of the ISA also requires the Director-General to provide me with a written report should a weapon allocated to an authorised person for self-defence purposes be discharged in specified circumstances (other than during training). This requirement was fully satisfied during 2007–08.

### **Operational file review activities/use of former IGIS as a consultant**

During 2007–08 I continued the practice of many years of devoting significant resources to regularly reviewing ASIS's operational case files.

I believe this is a very important inspection activity as the information contained in these files provides insight into the operational environment in which ASIS's field officers operate, some appreciation of the special pressures they are placed under, and the extent to which their activities are being directed and controlled by headquarters staff.

I continued the consultancy arrangement I have with my immediate predecessor, Mr Bill Blick AM PSM, to assist me in the on-going review of ASIS's operational activities.<sup>68</sup>

Mr Blick typically spends two days per month intensively reviewing ASIS's operational case files in the company of one of my senior staff, and then reports back to me at the completion of each inspection with a list of issues and findings.

Mr Blick brings a critical rigour to this task which derives, in part, from his extensive experience as a former Inspector-General.

The task of reviewing ASIS's operational files is never complete, but I am keen to cycle through as many files as possible each year in a targeted way.

While I cannot report the nature and range of issues which have come to light as a result of this particular inspection activity I can assure readers of this annual report that our examination of this material is rigorous and thorough.

Following each inspection I provide the Director-General with a detailed letter setting out our findings. These letters frequently pose questions relevant to the conduct of the operations under review.

Towards the end of 2007–08 I initiated a project whereby Mr Blick was to review this office's operationally related correspondence with ASIS over a four year period, to discern any pattern or trends, and to ensure that each issue raised had been dealt with satisfactorily and to finality.

I am appreciative of the efforts of those ASIS officers who have provided assistance during these inspections, have provided briefings, or have been involved in the preparation of responses to my questions.

### **Privacy rules**

Section 15(1) of the ISA requires that written rules exist to regulate the communication and retention by ASIS of intelligence information concerning Australian persons.

The then Minister for Foreign Affairs, the Hon Mr Alexander Downer, issued a set of privacy rules to ASIS in October 2001 to coincide with the coming into effect of the ISA.

A copy of the ASIS privacy rules was published in the IGIS Annual Report 2001–02<sup>69</sup> and can also be accessed via the ASIS website<sup>70</sup>.

The extant ASIS privacy rules have continuing legal effect until such time as they are formally revoked, or overridden, by the issue of new privacy rules.

The ASIS privacy rules are important because ASIS generates and receives a significant amount of secret intelligence information some of which refers to Australian persons.

<sup>68</sup> Information on this arrangement is set out at Annex 2 of this report.

<sup>69</sup> IGIS Annual Report 2001–02, Canberra, October 2002, Annex 4, pp. 91–92.

<sup>70</sup> See <<http://www.asis.gov.au/privacygov.html>> (accessed on 9 August 2008).

Intelligence information of this kind can only be included in ASIS reporting if the information serves a clear purpose linked to Australia's overarching national interests.

If it is determined that intelligence information about an Australian person should be included in a report, it can then only be circulated to appropriately cleared addressees with a demonstrated need to know this information.

My office devoted significant resources in the first half of 2007–08 to regularly reviewing every report which either directly or indirectly referred to an Australian person, to ensure that such reporting was properly justified in accordance with the requirements of the ASIS privacy rules.

I temporarily suspended this review activity in April 2008 because I have confidence in ASIS's internal compliance mechanisms and continuing the activity, at least for a period, did not represent best use of OIGIS resources.

It is my intention to review this situation in the forthcoming reporting period. In such a review I will weigh the merits of conducting sampling and spot audits, rather than the 100% compliance checking in which the office was previously engaged.

### Periodic roundtable meetings

As mentioned at various places throughout this annual report, I place significant importance on meeting with key staff in each of the intelligence collection agencies on a regular basis, so that we might discuss issues of common interest or concern openly and candidly.

I meet with ASIS in a roundtable meetings of this kind approximately every six weeks.

My ordinary practice is to circulate an agenda approximately one week before each meeting and invite officers who are involved in policy development, legal affairs and intelligence production to attend.

I find these meetings to be of great utility as they frequently involve discussion of practical issues and concerns at the desk officer level.

### Use of assumed identities

Section 15XUA of the *Crimes Act 1914* requires ASIS to, as soon as practicable after 30 June each year, provide me with a report for the preceding 12 months on:

- the number of instances in which formal alternative identity documentation has been obtained
- a general description of the activities undertaken by approved officers and approved persons when using their assumed identities, and
- whether or not any fraud or other unlawful activity was identified by the agency when auditing use of the assumed identity documentation.

ASIS continues to satisfy this requirement by providing me with six-monthly reports on the above matters.

### Complaints and inquiries

I received three new complaints about ASIS during the reporting period which led me to initiate preliminary inquiries. These complaints related to allegedly deficient selection and recruitment practices. Each of these preliminary inquiries was concluded before 30 June 2008.

In addition to these matters five other people contacted this office with queries or concerns about ASIS which were handled administratively.

Four of these complaints were from current or former employees of ASIS and raised a variety of issues or concerns.

I took each of these five complaints seriously and engaged ASIS senior management a number of times in respect of the issues which had been raised.

I had chosen not to initiate preliminary or full inquiries into any of these five complaints as at 30 June 2008, either because the complainants' personal circumstances had changed, they were pursuing remedies within ASIS, or they were contemplating other options.

I will maintain a watching brief on these complaints in case it becomes necessary to take any of these matters forward in a more formal manner.

# Defence Signals Directorate

## What DSD does

DSD is Australia's national authority for signals intelligence (sigint), and for information security (infosec).

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

In performing this function DSD must not intercept communications within the domestic Australian telecommunications network. If the collection of foreign intelligence requires such interception, this can only be conducted by ASIO under warrant authority.

DSD's various intelligence collection and reporting activities are regulated by ministerial directions, ministerial authorisations (MA) and privacy rules which are made pursuant to the *Intelligence Services Act 2001* (ISA).

The foreign intelligence collection priorities for DSD and other members of the AIC are established in a planning document that is endorsed and regularly reviewed by the National Security Committee of Cabinet.

DSD's intelligence-related activities are highly sensitive and are therefore classified in the interests of national security.

The other significant function DSD performs is to provide infosec products and services to the Australian Government and to the ADF. The underlying purpose of this function is to protect Australian official communications and information systems from unauthorised access and other potential threats.

As Australia's infosec authority DSD also plays an important role working with industry towards the development of new cryptographic products and the evaluation of other information security products.

General information about the various infosec products and services DSD provides can be accessed via the DSD website.

Further information about DSD can be found at <<http://www.dsd.gov.au>>.

## Significant issues

### New Minister

The change of government which occurred following the Federal election of

24 November 2007 saw a suite of new Ministers sworn into office on 3 December 2007. One of the new ministers sworn in on that day was the new Minister for Defence, the Hon Joel Fitzgibbon MP.

In assuming his appointment as the Minister for Defence Mr Fitzgibbon took on executive responsibility for the three Defence intelligence agencies, which includes DSD.

### Ministerial Directions

Section 8 of the ISA provides that the responsible Minister in relation to DSD must issue a written direction to the Director DSD, which among other things, sets out the circumstances in which the Director must obtain a ministerial authorisation (MA) before engaging in particular activities.

This requirement was satisfied with the issue of a Ministerial Direction by the then Minister for Defence, immediately before the ISA took effect on 28 October 2001.

Ministerial Directions are reviewed periodically for their currency, and also when there is a change of Minister.

In those instances where there is a change of Minister, pre-existing Ministerial Directions have continuing legal effect until such time as they are formally revoked, or overridden, by the issue of a new, properly authorised, direction.

Mr Fitzgibbon issued several new Ministerial Directions to DSD, in accordance with section 8(1) of the ISA, on 25 June 2008. The directions are similar in nature to those which were in place prior to him becoming the Minister for Defence.

I was consulted about the changes which were proposed to be made with the Ministerial Directions DSD operates under and had no concerns with them.

These new Ministerial Directions, like their predecessors, are classified documents and therefore cannot be made available to the public.

### **DSD privacy rules**

Section 15(1) of the ISA requires that the responsible Minister in relation to DSD must make written rules regulating the communications and retention by DSD of intelligence information concerning Australian persons.

As was the case with the Ministerial Directions (referred to above), Minister Fitzgibbon also inherited the existing DSD privacy rules when he assumed office. Mr Fitzgibbon re-endorsed the DSD privacy rules, without change, on 25 June 2008.

Further commentary on the application of the privacy rules by DSD and the role of this office in monitoring them is provided elsewhere in this chapter.

### **Compliance oversight of ADF signals intelligence activities**

In 2007–08 there was a change in the oversight arrangements in relation to the specialist units of the ADF which are involved in the collection and dissemination of foreign sigint.

DSD now has formal compliance oversight responsibilities for these units through authority afforded to it by a directive issued by the Chief of the Defence Force on 4 September 2007. The contents of this directive are classified.

While I cannot reveal the contents of this directive, I was consulted in the course of its development and am satisfied that the directive establishes the same policy framework for the ADF as is applicable to DSD under the ISA and the DSD privacy rules.

It should be noted that this office does not have direct oversight responsibilities for these specialist ADF units, but does have authority to oversight DSD's monitoring role with respect to these bodies.

During the reporting period I visited some of these specialist units, with a senior member of DSD, and was satisfied with the compliance regimes and reporting processes put in place by DSD.

### **Support to military operations**

DSD devotes significant resources to meeting the needs of the ADF and the wider Defence Organisation.

In the last 10 years the number and variety of ADF deployments has increased significantly. As at 30 June 2008 up to 3 500 ADF personnel were deployed to a variety of locations including but not limited to Iraq, Afghanistan, Timor Leste, the Solomon Islands, Sinai and Sudan.

As this list reflects, the operational environments into which service personnel are deployed can range from the relatively benign to the extremely hostile.

So as to minimise the risks that the ADF deployments face and to facilitate their operational effectiveness, as well as to ensure the operations of these deployments are not compromised, DSD is being increasingly called upon to provide high-quality and timely sigint and infosec products and services to the ADF.

I received several briefings throughout 2007–08 on the support provided to the ADF by DSD, and on a range of cognate issues.

These briefings and discussions have indicated that DSD is properly focussed on delivering to the ADF the best possible service it is able to provide.

## Support for counter-terrorism activities

While providing support to military operations is a critical part of DSD's mission, it is not the only function DSD performs.

A very important focus for DSD in the current global security environment is to identify, collect and share foreign intelligence information connected with terrorism-related targets.

Obtaining and sharing information of this kind directly assists the government to develop policies and plans to reduce the risks posed by these targets to Australian persons and Australian interests, both within Australia and abroad.

### NSW coronial inquiry into the late Mr Brian Peters

DSD devoted significant resources during 2007–08 to meeting the requirements of the NSW Coroner in the course of a coronial inquiry into the late Mr Brian Peters.

As has been very widely reported, Mr Peters and four colleagues who have come to be known as the 'Balibo Five', all died in the small village of Balibo, East Timor, in October 1975.

A fuller summary of the findings of this coronial inquiry, and DSD's role in assisting the Coroner, is provided in the 'Significant Issues' section of "The Year in Review" chapter of this report.

## Inspection activities

During 2007–08 my office undertook the following inspection activities:

- reviewing all MA submissions made by DSD to the Minister for Defence
- monitoring DSD reporting for compliance with the ISA and the DSD privacy rules
- conducting spot checks of a number of DSD databases
- holding monthly meetings with relevant DSD officers to discuss compliance, intelligence policy, and legal issues, and
- visiting various DSD collection sites outside of Canberra.

## Ministerial authorisations

The ISA provides a framework within which DSD can deliberately collect the foreign communications of Australians, in limited circumstances.

If DSD wishes to obtain an MA to intercept the foreign communications of an Australian person, the Minister for Defence must be satisfied that the person of interest is, or is likely to be, involved in one or more of a range of activities including:

- activities that present a significant risk to a person's safety
- acting for, or behalf of a foreign power
- activities that are, or are likely to be a threat to security, or
- committing a serious crime.<sup>71</sup>

In order to obtain an MA, the Director DSD provides a comprehensive written submission to the Minister for Defence in respect of each individual about whom DSD wishes to produce intelligence.

My office has access to the details of every authorisation which is approved, and I and my staff review documentation for each new or renewed authorisation, usually within four weeks of the authorisation being granted.

The Director DSD brought to my attention one instance where an administrative error had occurred in the production of an MA which was not identified prior to it being submitted to the Minister. The Director took immediate and appropriate corrective action to remedy this oversight and to brief me on what had occurred.

While no error of this kind is desirable, I commend the Director on his responsible approach to this matter.

### Spot checking of databases

As proposed in my previous annual report<sup>72</sup>, a member of my staff conducted a spot check audit of various DSD databases to ensure that collection activities which were enabled by the granting of each MA did not exceed any limits imposed in that approval, and to ensure that such collection only occurred during the period specified in the authorisation.

<sup>71</sup> Section 9(1A) of the *Intelligence Services Act 2001*.

<sup>72</sup> IGIS Annual Report 2006–07, p. 61.

The spot check took place towards the end of the reporting period. I am pleased to advise that this audit revealed that the requirements of each MA were being strictly complied with.

### Monthly meetings

I place great store on meeting regularly with senior level managers and desk officers, in each of the collection agencies so that we can candidly discuss issues of common interest or concern.

The meetings I hold with DSD usually involve a senior DSD manager, as well as drawing staff from the compliance and oversight area of the Directorate, staff involved in intelligence policy issues, and DSD's legal adviser.

These meetings typically involve broad-ranging discussion on privacy rules casework, collection priorities, MAs, legislative and parliamentary reviews, and current legal and operational issues, as well as any topical issues.

Any briefings I might seek on specific aspects of DSD's work are also usually scheduled to coincide with these meetings.

I also meet with the Director DSD, either prior to, or following each monthly meeting, or in his absence, with one of the Deputy Directors.

I have been pleased with the candour and quality of discussion in these meetings, and find them very helpful in maintaining a sound understanding of the important work which DSD undertakes.

### Privacy rules – monitoring and compliance

Earlier in this chapter I indicated that the Minister for Defence had re-endorsed the DSD privacy rules on 25 June 2008.

Simply put, the DSD privacy rules enable DSD to include references to Australian persons in its reporting, in limited circumstances, and so long as these references are properly justified in accordance with the privacy rules.

A fully staffed section within DSD monitors that the requirements of the privacy rules are being met. My office fulfils a similar function independently of DSD.

My staff and I engage in regular dialogue with DSD's compliance staff on a range of issues. It is not possible to provide details of these issues in a public report, but I can say that the incidence of Australian persons being identified in DSD reporting is extremely low relative to the number of reports DSD disseminates.

It has been my experience as the Inspector-General that DSD has a strong compliance culture, and that staff across the spectrum of its activities are usually very well schooled in their legal obligations.

The leadership shown by various Directors and senior managers combined with the efforts of DSD's compliance staff, policy advisers, legal counsel and trainers satisfy me that notwithstanding that DSD's work is necessarily intrusive, privacy issues are taken very seriously.

### New collection activities

In order to remain effective DSD must continually enhance its collection activities and counter threats to its capabilities.

DSD regularly informs this office of its capability development projects and we discuss any aspects of these projects that could give rise to concerns about legality and propriety.

I was pleased that DSD briefed me on several such projects during the reporting period and seriously addressed the various questions which I asked.

### Site visits

DSD maintains a number of facilities around Australia which are integral to its collection activities.

During the reporting period I visited one such facility, as well as two ADF units whose work is very closely aligned with DSD's mission.

### Training

DSD continues to devote significant resources to delivering technical and professional training opportunities to its staff on a wide range of subject matters, including compliance with the ISA.

In this reporting period I, or a senior member of my staff delivered 11 presentations to DSD staff on the role of my office and the principles underpinning the ISA.

## Complaints and inquiries

The level of complaint about DSD is generally low because its intelligence function is to collect foreign sigint by technical means. Given this focus DSD's activities are unlikely to come to the notice of or impact directly on members of the Australian public.

### Wider review of OSA policy and procedures

I decided towards the end of the last reporting period to initiate an own motion inquiry into OSA policy, procedures and practices across the three Defence intelligence agencies of which DSD is one.

This inquiry was finalised during the reporting period and my findings are summarised in "The Year in Review" chapter and Annex 5 of this report.

### Matters handled administratively

In addition to this formal inquiry, I dealt with three complaints about DSD relating to recruitment and other personnel matters.

One of these complaints concerned claims that an applicant for a particular position had been disadvantaged by the length of time involved in the security assessment process which was a necessary precondition for employment. In this case DSD assisted the complainant by locating an appropriate and acceptable position with another agency.

Another complainant raised concerns about the appropriateness or otherwise of some internal personnel management procedures. My office assisted the complainant by referring them to a relevant senior level manager.

The other complaint received by my office related to OSA processes. The complainant's views were considered as part of the wider review of OSA policy and procedures which was in train at the time of the complaint.

# Defence Imagery and Geospatial Organisation

## What DIGO does

DIGO was established under a Cabinet Directive on 8 November 2000, by amalgamating the Australian Imagery Organisation, the Directorate of Strategic Military Geographic Information, and the Defence Topographic Agency.

DIGO operated under the authority of this directive until it was inserted into the legal framework of the ISA, with effect from 2 December 2005.

DIGO's functions are detailed in section 6B of the ISA, and like ASIS and DSD, it is subject to a regime of ministerial directions, ministerial authorisations (MAs) and privacy rules, which are provided for under the ISA.

DIGO is responsible for the acquisition and analysis of satellite and other imagery and for the development, acquisition and exploitation of geospatial data, in support of Australia's defence and other national interests.

This means that DIGO collects and analyses images of foreign and domestic subjects (eg. landforms, waterways, disputed territories etc.), and develops mapping and imagery intelligence products for the ADF and a range of other Commonwealth clients.

DIGO also has the capacity to combine imagery with other available sources of data to prepare highly accurate topographical maps and other aids that are of value in the preparation of plans relevant to national defence and security.

DIGO operates out of two sites, with its headquarters located in the Russell Defence complex in Canberra, and its other facility located in Bendigo, Victoria.

Further information about DIGO can be found on its website which is located at <<http://www.defence.gov.au>>.

## Significant issues

### New Minister

When the Rudd Government was sworn in on 3 December 2007, the Hon Joel Fitzgibbon MP replaced the Hon Dr Brendan Nelson MP as the Minister for Defence.

As the Minister for Defence Mr Fitzgibbon took on executive responsibility for the three Defence intelligence agencies, of which DIGO is one.

### Ministerial Directions and DIGO privacy rules

Section 8(1) of the ISA provides that the responsible Minister in relation to DIGO must issue a written direction to the Director DIGO, which among other things, sets out the circumstances in which the Director must obtain an MA, before engaging in particular activities.

Section 15(1) of the ISA requires that the responsible Minister in relation to DIGO must make written rules regulating the communications and retention by DIGO of intelligence information concerning Australian persons.

Upon becoming the Minister for Defence and assuming executive responsibility for DIGO, Mr Fitzgibbon inherited the section 8(1) Ministerial Directions and section 15(1) DIGO privacy rules which had been established by his predecessors in that role.

These pre-existing directions and rules have continuing legal effect until such time as they are formally revoked, or over-riden, by the issue of new directions or rules.

## Inspection activities

### Ministerial and Director DIGO authorisations

Members of my staff and I visit DIGO headquarters approximately every two months to review materials relating to DIGO's collection activities.

In the course of these visits we review every MA which has been issued by the Minister for Defence in the period since our previous visit, and we also examine any approvals given by the Director DIGO in the same period.

As indicated above, those collection activities which can only be approved by the Minister for Defence are specified in the Ministerial Direction under which DIGO operates. This is a classified document and therefore cannot be released to the public.

The Minister is only required to personally consider/approve a relatively small number of sensitive collection activities undertaken by DIGO. This is entirely reasonable as the Minister would otherwise be overwhelmed by the administrative burden of considering a significant number of non-sensitive requests for items such as maps and other imagery products which are in some cases already commercially available.

As it is not reasonable to expect the Minister to consider every tasking request levied on DIGO, the Director DIGO is empowered to consider requests for imagery products which do not need to be put to the Minister for approval.

In my previous annual report I indicated that during 2006–07 I had sought clarification from DIGO in relation to the interpretation of section 9(1A) of the ISA.<sup>73</sup>

Without going into the detail of the case which prompted my interest, the central issue revolved around the circumstances where the approval of the Attorney-General must be first obtained, before an MA can be sought from the Minister for Defence in relation to particular tasking requests.

Legal advice was obtained during that reporting period which greatly clarified the matters which I had queried.

In the course of the inspections conducted during 2007–08 my office closely monitored whether any tasking requests levied on DIGO raised similar issues or concerns. I am happy to report that none did.

During the 2007–08 inspections my staff and I either noted, or had brought to our attention, a small number of instances where tasking requests which ordinarily require authorisation by the Director DIGO, were undertaken prior to that approval having been obtained.

In the cases in question I was satisfied that this occurred because the individuals involved did not fully appreciate that the activities they were involved in required authorisation rather than anything of a more sinister character, and that if such an authorisation had been sought beforehand it would undoubtedly have been granted.

The Director DIGO took immediate corrective action including requiring relevant officers undergo appropriate privacy rules refresher training, and also issuing an appropriate level authorisation for the activities in question.

While no error is desirable I was satisfied that this was no more than an administrative breach of internal policy. Indeed, the above instance has served as a useful training tool.

In the course of the inspection visits, my staff and I queried the specific grounds upon which the Director DIGO had justified several collection activities.

By way of background, each Director DIGO authorisation must be justified by reference to one of DIGO's functions.<sup>74</sup> There is a degree of overlap between DIGO's five functions so it is not surprising that there will occasionally be debate as to which is the most appropriate reference.

In each of the instances identified the Director was able to fully and properly justify his selections.

On the basis of our discussions about such matters, I am satisfied that the Director DIGO is fully committed to ensuring that DIGO staff are properly conversant with their obligations.

<sup>73</sup> IGIS Annual Report 2006–07, p. 65–66.

<sup>74</sup> Section 6B of the ISA.

## DIGO privacy rules

During our bi-monthly visits to DIGO headquarters my staff and I also closely examine all tasking requests that DIGO actions, for compliance with the DIGO privacy rules.

DIGO faces some unique challenges in applying its privacy rules in that those rules are predicated on the assumption that the privacy of “Australian persons” will be protected, unless appropriate justification is put forward to enable the reporting of intelligence information to recipients with an established need to know.

The term “Australian persons” has a broader meaning than living human beings, and is also applicable to bodies corporate which are registered in Australia and controlled by Australians. By extension this can be applied to premises or property controlled by Australian companies.

Although the application of the privacy rules has its complexities for every agency, it can be more difficult for DIGO than the other AIC agencies which are bound by similar rules because its reporting is primarily image-based and focussed on property or premises, which may or may not be an “Australian person” for the purposes of the privacy rules.

While this does create some interpretative issues from time to time, for the most part it has a limited impact upon DIGO’s business operations because the vast majority of DIGO’s reporting has an off-shore focus, in which case the privacy rules have a much more limited application.

On the basis of our periodic inspections I am satisfied that DIGO is genuinely committed to strictly applying the privacy rules.

## Meetings with senior DIGO staff

As with each of the other collection agencies, I think there is distinct benefit in meeting regularly with senior agency staff to candidly discuss matters of mutual interest or concern.

During the reporting period we conducted six such meetings, each of which coincided with our inspection / visits.

On each occasion I met with the Director DIGO or the Acting Director and a representative from DIGO’s policy and compliance area.

I am grateful to all DIGO staff who have been involved in these exchanges for giving freely of their time to participate in these meetings.

## Training

My office did not make any specific presentations to DIGO staff during the reporting period but we did make a number of presentations to AIC-wide induction and senior officer courses which included a number of DIGO personnel.

## Visits

During 2007–08 a member of my staff visited DIGO’s Geospatial Analysis Centre, which is located in Bendigo, Victoria.

## Complaints and inquiries

### Wider review of OSA policy and procedures

I decided towards the end of the last reporting period to initiate an own motion inquiry into OSA policy, procedures and practices across the three Defence intelligence agencies of which DIGO is one.

This inquiry was finalised during the reporting period and my findings are briefly summarised in “The Year in Review” chapter of this report.

The visit which was undertaken by one of my staff to DIGO’s Bendigo facility was associated with this inquiry.

### Matters handled administratively

In addition to the OSA inquiry referred to above, I also received two complaints about DIGO relating to concerns about OSA processes and practices from persons applying for positions with DIGO.

The issues raised by these complainants were handled administratively, and helped to inform the direction taken by our OSA inquiry.

# Defence Intelligence Organisation

## What DIO does

DIO is Australia's strategic level, all-source Defence intelligence assessment agency. It provides intelligence assessments to inform the decision-making of the Department of Defence including the ADF, and the broader Australian government.

DIO is an assessment agency rather than an intelligence collection agency.

DIO's assessments cover strategic, political, defence, military, economic, scientific and technical issues which have the potential to impact on Australia's security interests. DIO also plays an important role in assisting with the planning, command and conduct of current and potential operations by the ADF. It assesses the strategic posture, policy and intent and the military capabilities of countries relevant to Australia's security.

DIO focuses on overseas developments and does not concern itself with domestic concerns or situations within Australia.

DIO also has the responsibility of developing and maintaining a defence intelligence capability for use in time of crisis and conflict.

Further information about the role and functions of DIO can be found at <http://www.defence.gov.au/dio/>.

## Analytic Integrity

As discussed in the "ONA" chapter, since the amendments made in late 2005 to the IGIS Act allow the IGIS to initiate inquiries into matters relating to ONA and DIO without ministerial referral, I have conducted both inspection and inquiry activities in relation to ONA's statutory independence.

As a logical next step, on 29 February 2008, I advised the Minister for Defence, the Deputy Secretary Intelligence, Security and International Policy and the Director DIO of my intention to conduct an own motion inquiry into the propriety of the assessment activities of DIO (as per section 8(3)(a)(iii) of the IGIS Act).

While DIO does not have a statutory basis, unlike ONA, I consider that the concept of propriety clearly covers the notion of "integrity" of the assessment process.

Integrity of the assessment process requires that assessments are made objectively, dispassionately and free from improper external pressure/direction, and on the basis of intelligence that is considered to be both reliable and valid.

The methodology used in conducting this inquiry has been informed in part by the approach taken to the inquiry into the statutory independence of ONA.

I commenced this particular inquiry by developing a set of principles that articulate what analytic integrity at DIO is and is not. I then held a series of focus groups with DIO analysts to refine these principles. In addition to providing a 'yardstick' for this inquiry, I anticipate that the principles will continue to be a useful reference for analysts. A copy of these principles is provided at Annex 4.

As with the ONA inquiry, I decided to canvass the views of DIO staff, through a survey, on matters relating to DIO's analytic integrity. I also held seven focus groups (consisting of small numbers of analysts and managers) with DIO staff to outline the review, to hear their thoughts and suggestions and gain an appreciation of the various experiences of individuals across the branches and at different classifications levels in DIO.

At the end of the reporting period this inquiry was close to being finalised. Further details of my findings will be reported in my next annual report.

## Privacy guidelines

The DIO privacy guidelines, implemented in December 2005, govern the use of references to personal information about Australians in external communications – including reports, briefings, emails and advice – emanating from DIO.

Since implementation my office has conducted 10 inspections (including four in this reporting period). I have observed improvements in the administrative practices that underpin the guidelines in that time.

Overall I was pleased with the quality and level of detail contained in the documentation. There is a continued gradual increase in the sophistication of analysts' appreciation of the privacy guidelines.

This is due in large part to DIO's ongoing organisation-wide programs and training to educate analysts on applying the guidelines and reporting on compliance with the guidelines. DIO's commitment during the reporting period to ensuring that privacy guidelines training is regularly undertaken by all analysts was evident. I will continue to monitor DIO's provision of privacy guidelines training over the coming year.

I was particularly pleased by the increasing sophistication of DIO's own audit procedures concerning conformance with the privacy guidelines. DIO conducts an annual audit. The audit uses a sampling methodology focussing on material produced by a randomly selected section of the organisation. I regard this initiative as a positive one as it provides for increased confidence in the overall accuracy of DIO's audit activities.

I intend to continue conducting regular inspections relating to DIO's use of the privacy guidelines at quarterly intervals.

## Training

I have continued to raise awareness about my office and also encourage greater interaction between my office and DIO. In addition to my presentations to the AIC common induction and senior officers courses, to which DIO staff are regularly allocated places, I made two presentations to staff at DIO during the reporting period.

Information about the role and functions of my office is also accessible on DIO's internal web pages.

## Complaints and inquiries

I received no complaints about DIO which required inquiry action during this reporting period. Four matters were handled administratively.

As mentioned in the "DSD" and "DIGO" chapters, I finalised an own motion inquiry into the OSA process in these three Defence agencies. A copy of the executive summary of the report is provided at Annex 5 of this annual report.

# Office of National Assessments

## What ONA does

ONA provides assessments on international matters of political, strategic and economic significance to the Prime Minister, members of the National Security Committee of Cabinet and key senior policy makers in the government. ONA bases its assessments on information from a range of sources, both inside and outside the government.

While ONA reports directly to the Prime Minister and sits within the Prime Minister's portfolio, responsibility for the preparation of assessments and day-to-day management issues falls to the Director-General of ONA. The Director-General of ONA is an independent statutory officer who is not subject to external direction on the contents of ONA assessments.

In addition to setting out ONA's assessment function, the *Office of National Assessments Act 1977* (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.

Further information about ONA can be found at <<http://www.ona.gov.au>>.

## Statutory Independence – Inquiry 2007

On 14 February 2007 I advised the then Prime Minister and the Director-General of ONA of my intention to conduct an own motion inquiry into the statutory independence of ONA (as provided for under section 8(3)(c) of the IGIS Act).

While the inspection activity conducted in the previous reporting period was generally positive, I decided that as a matter of proper process I should conduct a full inquiry using all the powers available to me on matters relating to the statutory independence of ONA.

The inspection activity in 2006 was useful in establishing an outline of what independence means for ONA, in scoping how to best examine it and providing a preliminary perspective. The methodology used in conducting this inquiry, while largely consistent with the methodology used in undertaking the 2006 inspection activity, was more wide-reaching.

As well as undertaking the same review activities as in 2006, I decided to look in greater detail at a range of activities including source documentation procedures, practices regarding review of previous judgements in intelligence assessments, and consideration and evaluation of divergent viewpoints within and outside ONA. To that end I sought access to documentation on end-noting, internal ONA reviews of key judgements, documentation on dissent, and drafts of ONA product and documentation indicating changes made to drafts.

I also undertook a series of confidential, individual discussions with selected staff, both current and former, with a view to gaining an appreciation of thoughts and experiences across the branches and at different APS classification levels in ONA.

ONA's internal culture is one of constructive debate and contestability, and analysts are well imbued with the concept of ONA judgments needing to be independent. There are various internal processes which support independence and integrity in the preparation of assessments and analysts were very positive about these. I made some minor suggestions for strengthening of these processes.

In the course of this inquiry, I found no evidence or indication of improper pressure or attempted direction from ministers or their offices.

While policy departments very occasionally could press their arguments in a way which bordered on undue pressure, ONA's final judgements did not appear to have been affected in any improper way.

A copy of the key judgements of the report is at Annex 3.

## **Privacy guidelines**

In December 2005 ONA adopted a set of privacy guidelines that outline standards for the handling, use, and further dissemination of information about Australian persons. The guidelines apply to references to personal information about Australian persons in any external communications — including reports, briefings, emails and advice — emanating from ONA.

The ONA privacy guidelines are essentially identical to the privacy rules which are applicable to ASIS, DSD and DIGO. (A copy of the ONA privacy guidelines can be found at Annex 7 of the IGIS Annual Report 2005–06).

In the two and a half years since implementing the privacy guidelines, ONA's processes for managing appropriately information about Australian persons have become increasingly sophisticated. These improvements are underpinned by continued training for analysts on applying the guidelines and reporting on compliance with the guidelines.

During this reporting period I conducted four inspections of ONA's use of the privacy guidelines. I was satisfied with ONA's application of, and compliance with, the privacy guidelines and the efforts undertaken to improve the quality and care taken in the documentation.

I will continue to conduct inspections relating to ONA's use of the privacy guidelines at quarterly intervals.

## **Training**

I have continued to raise awareness about my office and also encourage greater interaction between my office and ONA. Throughout the year I presented to the AIC common induction and senior officers courses, to which ONA staff are regularly allocated places.

Information about the role and functions of my office is also accessible on ONA's internal web pages.

## **Complaints and inquiries**

There were no complaints made to my office about ONA in the reporting period.

# the year 2008-09 in prospect

The following is a summary of the main activities which I propose be undertaken by either myself or my staff during 2008–09.

## **Inspection and review activities involving AIC agencies**

### **ASIO**

OIGIS will continue to pay very close attention to the granting of special powers warrants to ASIO and the execution of these warrants.

Given that nearly all warrants are authorised by the Attorney-General, and the Attorney-General also has direct executive responsibility for ASIO, it is appropriate that there be some form of external oversight of the warrants process. In addition to this, as every category of special powers warrant which is available to ASIO relies on methods and capabilities which either are, or have the potential to be, coercive and/or intrusive, it is important that these powers be subject to external oversight.

It is therefore my intention that OIGIS will review every warrant which is issued to ASIO and all associated accountability documentation.

It is also my intention that, in a number of selected cases, the review will go beyond the basic warrant documentation and examine relevant operational case files to obtain a fuller understanding of the operation in question.

As indicated elsewhere in this annual report, ASIO has commenced utilising “B-party” telecommunications interception warrants, when other collection methods have proven to be ineffective, or are not available.

I will continue to be especially vigilant in monitoring all aspects of the use of “B-Party” warrants during the 2008–09 reporting period.

Whenever this office conducts a warrants inspection, I will ask ASIO to also provide for inspection any authorisations which have been issued in order to obtain prospective telecommunications data.

My staff will also continue to conduct independent checks on telecommunications services which are being intercepted to ensure that they comply with relevant warrant conditions.

As discussed in the “ASIO” chapter of this annual report, it has been the practice of the office to be present for at least the first day of questioning which is conducted pursuant to any questioning warrant which has been granted to ASIO. It is my intention to continue this practice during 2008–09, should any questioning, or questioning and detention warrants be granted to ASIO.

Several years ago section 23 of the ASIO Act was amended to provide ASIO with the power to compel airline and vessel operators to provide information.

I propose conducting inspection activities during the forthcoming reporting period to ensure that ASIO’s collection activities comply with their legal obligations and to ensure that any data which is collected is handled appropriately.

During 2007–08 members of my staff and I commenced meeting with senior ASIO personnel on a monthly basis. As I believe that these meetings have been successful in advancing the interests of this office, and have hopefully been of benefit to ASIO as well, I intend to continue these meetings for the foreseeable future.

My staff will examine investigative approvals generated in ASIO's central office and those generated by ASIO's State and Territory offices during our periodic visits. The files on which actions resulting from the approvals are recorded will also be examined.

I will continue monitoring ASIO's access to, and use of, AUSTRAC and taxation records, to ensure compliance with the legislation and the various MOUs under which this access is provided.

I will continue to monitor ASIO's procedures for controlling the use of alternative documentation associated with assumed identities, but will do this on the basis of internal audit and exception reporting rather than by previous methods.

I will also continue to monitor ASIO's performance with regard to its obligations under the *Archives Act 1983*.

My office will continue to make presentations to ASIO training courses on ethics and accountability, and intends to observe training activities associated with ASIO's intelligence officer training program.

ASIO's internal audit program will be monitored and I will obtain reports on reviews that are of interest to this office.

On occasion this office is consulted by ASIO in the development of internal guidelines and procedures. I intend for this office to provide constructive and timely input to all requests for comment of this kind.

Subject to the resources available to this office, it is my intention to conduct several pilot projects or reviews, as a means of scoping future inspection activities.

It is my intention to spend more time, if I am able, visiting functional areas of ASIO which are new or with which this office has not had frequent contact in the past, in order to deepen our knowledge of ASIO.

### **ASIS**

During 2008–09 this office will design and conduct inspection activities to ensure that ASIS complies with its MOU obligations, should it seek to access any financial transaction records held by AUSTRAC, or to communicate any information of this kind, to other parties.

In addition to this new inspection activity my office will continue our standing practice of reviewing all ministerial submissions which are lodged by ASIS with its Minister, and also closely review all MAs which are sought by ASIS under the terms of the ISA.

I will continue to closely monitor the application of the guidelines and protocols associated with the provision of, training in, and use of weapons and self-defence techniques by ASIS staff.

Despite my best intentions I was not able to observe a weapons training course during 2007–08. It is therefore my intention that either I or a senior member of my staff should do so during 2008–09, in order to gain a first hand appreciation of what is involved.

My staff will continue to closely inspect operational files having regard to the legality and propriety of the conduct of ASIS officers.

I intend to maintain our scrutiny of records relevant to ASIS's compliance with the privacy rules, although the methods we use will be subject to review.

It is my intention to meet with ASIS's intelligence coordinators, legal and policy staff approximately every six weeks, to be briefed on emerging issues and to discuss issues arising out of our inspection activities.

ASIS's procedures for controlling the use of alternative documentation associated with assumed identities will also be the subject of review.

I or senior members of my staff will continue to address ASIS training courses and other forums on accountability.

I will also continue to meet with more senior ASIS officers before they proceed on postings to reinforce that they are subject to internal and external scrutiny and are accountable for their conduct.

### **DSD**

My office will continue to access and review each DSD submission to the Minister for Defence seeking an MA under the ISA.

I will continue to monitor DSD's compliance with its obligations under the DSD privacy rules.

My staff and I will meet key DSD staff on a monthly basis to discuss issues arising out of our monitoring activities, the internal monitoring activities undertaken by the relevant section in DSD which deals with such matters, and policy issues affecting compliance.

I expect DSD to continue to consult me on a range of operational matters and my office will provide prompt advice on issues related to legality and propriety.

My office will continue to address DSD training courses and other forums on accountability.

We will initiate projects to review selected DSD activities and/or to gain a better appreciation of DSD's various capabilities.

### **DIGO**

My office will review all submissions made by DIGO to the Minister for Defence seeking an MA under the ISA.

I will review internal submissions made to Director DIGO specifically seeking authorisation in respect of Australian territory or Australian interests.

I will also closely monitor compliance with the DIGO privacy rules.

My office will meet with relevant DIGO senior managers approximately every two months at DIGO Headquarters to discuss issues arising out of the above inspection activities, and to discuss matters of common interest.

### **DIO**

I will complete the inquiry into analytic integrity of DIO assessments.

My office will regularly review DIO's compliance with the DIO privacy guidelines.

### **ONA**

I intend to plan and commence a further examination of the independence and integrity of ONA assessments.

I will meet with Director-General ONA on an occasional basis, to discuss matters affecting his agency, or the wider AIC, as circumstance dictates.

My office will also monitor the application of ONA's privacy guidelines.

## **Inquiries and complaints**

Three inquiries under the IGIS Act were in progress at the close of the reporting period. I expect to conclude investigations into each of these matters during the first half of the new reporting period.

## **OIGIS staffing and recruitment**

During the 2007–2008 reporting period I recruited two full time on-going officers and lost one full time on-going officer on transfer and one to retirement.

I initiated two major staff selection exercises during 2007–08 with a view to identifying appropriately qualified staff at the APS 6 and Executive Level 1 employment classifications.

The first exercise, which was conducted in the first half of 2007–08, proved fruitless when the two preferred candidates withdrew their applications during the security clearance process after having found alternate positions which were immediately available and which did not require the holding of a security clearance.

The office conducted another selection exercise in the second half of 2007–08 with a view to recruiting up to three staff. Preferred candidates were identified in June 2008 and have each commenced the security clearance process. I am hopeful that this will prove to be more fruitful.

As I have funding to further expand the size of OIGIS, one current staff member is approaching retirement, and it is possible that other staff might wish to pursue employment elsewhere, it is probable that the office will conduct further selection exercises in 2009–10.

I am hopeful that should additional staff be recruited that I will be able to enhance our existing visits and inspections program by devoting more time and more staff to specific inspection and review tasks, and to add new inspection tasks as appropriate.

## **Other OIGIS corporate activities**

In addition to acting upon the staffing needs of the office, I am keen to progress several other corporate activities.

As mentioned elsewhere in this annual report, I am keen to update and revamp the OIGIS website.

I intend to devote further resources to developing a tailored and comprehensive business continuity plan for OIGIS, to ensure that the work of the office could be continued in the event of a disaster or some other unanticipated event.

The machines and equipment upon which any modern office relies have a finite life and some of those which exist in OIGIS are reaching the end of their productive lives. I am therefore keen to explore options to upgrade and replace this equipment, if this is possible.

## **Other matters to be pursued**

The above items are indicative of my intentions but by no means comprise an exhaustive list. As the 2008–09 reporting period progresses no doubt new matters will arise of which I am currently unaware, which will require attention.

# corporate governance, human resources and financial management

## Corporate Governance

The corporate governance practices in place for the office reflect its size and function. In addition to planning processes in relation to resource and personnel management, senior members of staff meet each week to review operational priorities. The office has the advantage of being readily able to hold an 'all-staff' meeting each month. This meeting includes general information exchange, consideration of office performance against the range of activities in which it is involved and forward planning.

## Organisation structure

The small size of the office lends itself to a collegiate approach to dealing with the workload of the office and workplace issues more generally.

During the reporting period, positions were filled as follows:

- Inspector-General of Intelligence and Security  
Mr Ian Carnell
- Principal Investigation Officer  
Mr Neville Bryan, PSM
- Principal Review Officer  
Ms Rachael Spalding
- Senior Investigation Officers  
Mrs Jane Trevor  
Ms Samantha Clark  
Ms Sharon Dean (from 16 July 2007)  
Mr Stoney Burke (from 7 January 2008)
- Senior Review Officer  
Ms Lisa Buckingham (to 16 October 2007)

- Office Accountant  
Ms Jackie McRae
- Personal Assistant to the Inspector-General and Office Manager  
Ms Jodie Williams
- Office Manager and Monitoring Officer  
Ms Robyn Kelly (to 9 August 2007)
- Administration Officer  
Mrs Jocelyn Yosef

## Internal Audit

The office has an Audit Committee chaired by me and which also includes an external member from PMC. Staffing changes in PMC saw a new external member joining the committee during the reporting period. I anticipate that for the purposes of this committee, that transition will be seamless and would like to record my thanks to both members for their assistance during the period.

The 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.

## Risk Management

The office's Audit Committee has overall responsibility for the agency's risk management function. The Committee reviews the Risk Management Plan on an annual basis and makes amendments if required. It 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:

1. personnel related
  - departure or absence (eg through injury) of key staff with little notice
  - accidental or intentional loss of information
  - segregation of duties
2. failure or compromise of information technology systems
3. physical security of the office and facilities
4. corporate liability
5. fraud prevention, detection and management, and
6. 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.

### **Fraud control**

While the Risk Management Plan is comprehensive in that it covers fraud prevention, detection and management, the office also maintains a separate Fraud Control Plan which goes into greater detail on risks of that type and how they are dealt with.

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, and that the office has responded to the annual survey for fraud control data.

### **Disaster recovery plan/business continuity plan**

The office has its own Disaster Recovery/Business Continuity Plan to ensure its continued operation in the event of a disaster. This plan is closely integrated with the PMC plan and is reviewed periodically to ensure its currency.

### **Corporate and operational planning**

Increased office size during the reporting period also gave rise to the opportunity to bring a greater level of structure and formality to the office's corporate and operational planning activities. In particular, the office undertook planning activities which drew together the full range of activities undertaken by this office, and accorded each a relative priority. While not itself constituting a productivity gain, I anticipate that this planning will continue to provide a useful mechanism for optimising productivity across the many and varied activities of the office.

Further details of OIGIS forward plans are available in the "The year 2008–09 in Prospect".

### **External scrutiny**

The office has again received an unqualified audit report from the ANAO in relation to its financial statements.

Further details of OIGIS interaction with parliamentary committees are available in "The Year in Review" and the "Parliament, Legislation and Liaison" chapters of this report.

### **Support from PMC and DSD**

As a very small portfolio agency, co-located with PMC, my office relies on assistance from PMC in handling a range of administration issues and in providing general support.

While an office of this size with a modest appropriation cannot readily cover the full array of costs ordinarily incurred, the office made a \$46 000 (GST exclusive) payment to PMC in recognition of the increasing costs associated with the support provided to the office in 2007–08. This arrangement works well and I am very appreciative of PMC's continued support.

The other major provider of continued support to my office is DSD, which maintains the internal secure computer and communication network systems within the office. I would like to record my thanks for DSD's continued assistance.

## Human resources

### Background

At the end of 2000–01 (i.e. the last completed budgetary period before the 11 September 2001 terrorist attacks), OIGIS comprised the Inspector-General and four staff.

This figure was the same when I commenced as Inspector-General in March 2004, but not surprisingly there has been a need to expand the size of the office in a graduated manner. The AIC agencies have grown substantially in size and OIGIS was tasked with taking a specific interest in the assessment activities of ONA and DIO as a result of the Flood Inquiry.<sup>75</sup>

At the conclusion of 2007–08 OIGIS comprised myself and nine staff. My aim is to recruit two additional staff in 2008–09.

Additional resources allow OIGIS to keep pace with the increases in AIC activities, and also give me the opportunity to re-evaluate our range of inspection activities to ensure that they are still focussed and relevant, as well as providing flexibility to initiate new inspection activities and research projects, as appropriate.

It is also worth noting that I have recruited a dedicated, CPA accredited accountant, who works on a part time basis, as well as a full-time administration officer who does not have any inspection or review duties.

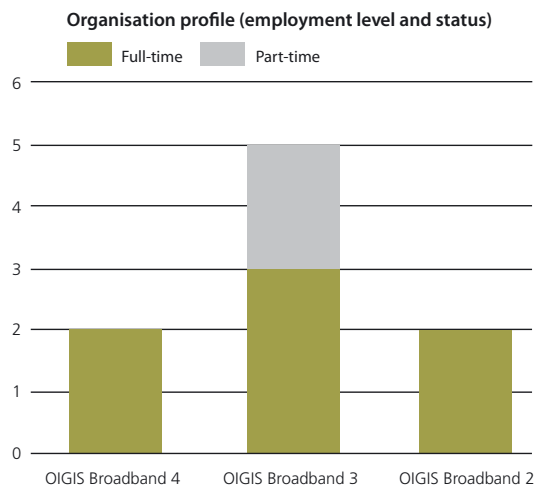
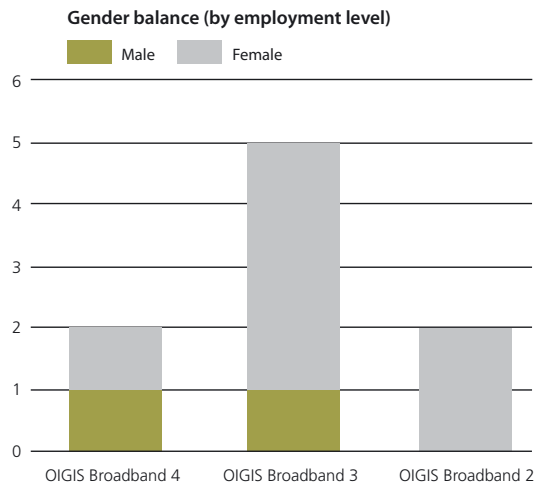
In addition to delivering a first rate service and providing me with significant reassurance that the OIGIS books are fully compliant with the reporting requirements of the Australian National Audit Office (ANAO) and the Department of Finance and Deregulation, the recruitment of a dedicated and fully qualified accountant has freed up one of the existing members of staff to engage wholly on inspection and review activities.

Similarly, the engagement of a dedicated administration officer allows other members of staff to focus on inspection, complaint and inquiry work.

### Organisation profile

As noted above, OIGIS is a very small agency comprising nine staff and the Inspector-General. Staff work in two teams, one responsible for assisting the Inspector-General with inspection, review and inquiry work in relation to ASIO, ASIS, DIGO and DSD, while the other is responsible for such activities in relation to ONA and DIO as well as the provision of corporate support to the office. In such a small workplace the background, skills, talents and viewpoints of each employee are recognised and highly valued.

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



<sup>75</sup> P. Flood, op. cit.

During the reporting period, OIGIS gained two staff. This gain was off-set by the loss of two officers, one who retired and another who transferred to a position located interstate. A recruitment activity was initiated late in the reporting period and I am hopeful of receiving three welcome additions to the office.

### **Training and development**

During the reporting period staff attended a range of training courses including in administrative law, leadership and management skills, first aid and a range of areas specific to the AIC.

In a small office it is especially important to ensure that staff have the requisite skills and training to undertake an unusually broad range of duties. The breadth of each officer's responsibilities is regarded as both an organisational strength and an opportunity to develop each officer's skill-set beyond that ordinarily possible in larger organisations with more strictly delineated functional roles.

### **Performance management and pay**

OIGIS has a formal performance management process which focuses specifically on expectations of staff, development opportunities and feedback on performance. This formal process is complemented by regular, though less formal, meetings to discuss team and individual priorities, work allocation and to monitor outcomes and outputs.

OIGIS does not have a performance based pay scheme.

### **Workplace agreements**

All staff continued to be employed under individual Australian Workplace Agreements. These agreements are subject to periodic review and will cease to have effect on 30 June 2009. In the coming reporting period OIGIS will consider moving to a collective agreement in place of the current individual agreements.

### **Personnel guidelines**

The increased size of the office provided the opportunity to review the existing human resource practices. A series of detailed guidelines relating to personnel management was produced. Further guidelines will be added to the series as and when the need arises.

## **Other information**

### **Occupational health and safety**

In accordance with the requirements of the *Occupational Health and Safety Act 1991* (OH&S Act), staff were consulted during the reporting period on the establishment of a Designated Work Group (DWG), the development of Health and Safety Management Arrangements (HSMA) and the selection of a Health and Safety Representative (HSR).

Due to the small size of the office, it was agreed not to establish a Health and Safety Committee at this point in time. Instead health and safety matters are regularly addressed within the office as standing items at our all-staff meetings and Audit Committee meetings and, as the need arises, directly with me through the team leaders and HSR.

During the year one health and safety hazard inspection and seven workstation assessments were conducted for the staff in the office. One First Aid Officer was appointed and received accredited training.

The office also gave particular consideration during the year to the potential health risks of staff interacting with difficult complainants. It is sometimes the case that a complainant can be dissatisfied with the level of assistance the office is able to provide them or the outcome of an inquiry. Although only a small proportion of these instances lead to persons exhibiting difficult behaviour, it is important to manage these situations well. I do not expect staff to tolerate significant abuse or aggression, or fear for their safety. New guidelines were issued to staff in respect of these issues.

No accidents or dangerous events occurred during the year that arose out of the conduct of undertakings by me that required the giving of notice under section 68 of the OH&S Act. No investigations were conducted relating to undertakings carried on by me and no notices were given to me under sections 29 or 47 (relating to provisional improvement notices and improvement notices respectively) of the OH&S Act.

## Disability Strategy

The office is committed to meeting its responsibilities under the *Disability Discrimination Act 1992* and the Commonwealth Disability Strategy. While the performance indicators and strategies in the Commonwealth Disability Strategy are not applicable or applicable in a limited sense only to the work of this office, it is fully accepted that OIGIS must satisfy the principles which underpin the strategy wherever relevant.

## Freedom of information

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

## Advertising and market research

OIGIS incurred no expenditure on general advertising or advertising campaigns during the reporting period.

## Ecologically sustainable development and environmental performance

The office through its co-location with PMC 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 (One National Circuit). These measures include, but are not limited to energy efficient lighting, heating and cooling.

Due to the small size of my office, PMC 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 PMC, 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 is used for 80 per cent of the office's photocopying, facsimile report and document printing (20 per cent new/virgin paper)

- printers are configured to default to double-sided (that is, using both sides of the paper) printing
- all office paper and cardboard waste is recycled
- empty toner cartridges are recycled, except where security considerations apply, and
- where there is no operational impact, office equipment is 'shut-down' over night, rather than being placed on 'stand-by'.

## Financial management

### Purchasing

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

### Consultancy services

The office has only a small need for consultancies each year. Information on expenditure on consultancies is available on the AusTender website <<http://www.tenders.gov.au>>.

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 PMC through an open tender or panel selection process.

During 2007–08 three new consultancy contracts were entered into involving total actual expenditure of \$51 020 (GST inclusive). This figure includes the mandatory superannuation payments. There were no ongoing consultancy contracts from 2006–07 active during 2007–08.

A consultancy services table is at Annex 2.

### Contract services

The office has only a small need for contracts each year. Information on expenditure on contracts is available on the AusTender website <<http://www.tenders.gov.au>>.

## Legal services

Legal services are obtained from the Australian Government Solicitor (AGS). In 2007-08 OIGIS paid for five separate AGS legal advices at a combined cost of \$114 056 GST inclusive (2005-06: \$3 339). Expenditure on legal expenses fluctuates from year to year and is largely dependent upon the nature of the inquiries undertaken.

My office did not engage any other solicitors or any counsel direct during the reporting period, and there are no internal legal services.

## Summary of the office's financial performance and resources for outcomes.

The office has one outcome and one output.

In 2007-08, the office received an operating appropriation of \$1.746 million as shown in the table below. The major components of 2007-08 expenditure were:

- 72% employee expenses
- 27% supplier expenses, and
- 1% depreciation expense.

The 27% supplier expenses outlined above consist of:

- 63% other goods and services
- 26% resources received free of charge
- 10% payment to PMC, and
- 1% Comcare premium.

The office realised an operating surplus of \$151 931 in 2007-08.

	2007-08 OUTCOME 1	2007-08 OUTPUT 1
<b>Revenue and Expenses</b>	<b>\$</b>	<b>\$</b>
Operating revenues		
Revenues from government (Budget and Additional Estimates Appropriations)	1 746 000	1 746 000
Other income (Resources received free of charge)	120 000	120 000
<b>Total operating revenues</b>	<b>1 866 000</b>	<b>1 866 000</b>
Operating expenses		
Employees	1 224 359	1 224 359
Suppliers	465 964	465 964
Assets written-off	7 196	7 196
Net losses from sale of assets		
Equipment depreciation	16 550	16 550
<b>Total operating expenses</b>	<b>1 714 069</b>	<b>1 714 069</b>
<b>OPERATING RESULT</b>	<b>151 931</b>	<b>151 931</b>

# financial statements

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

In my opinion, the attached financial statements for the year ended 30 June 2008 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*.



Ian Carnell  
Inspector-General  
of Intelligence and Security

3 September 2008



## INDEPENDENT AUDITOR'S REPORT

To the Special Minister of State

### Scope

I have audited the accompanying financial statements of the Office of the Inspector-General of Intelligence and Security for the year ended 30 June 2008, which comprise: a Statement by the Inspector-General of Intelligence and Security; Income Statement; Balance Sheet; Statement of Changes in Equity; Statement of Cash Flows; Statement of Commitments and Contingencies; and Notes to and forming part of the Financial Statements; including a Summary of Significant Accounting Policies.

### *The Responsibility of the Inspector-General of Intelligence and Security for the Financial Statements*

The Inspector-General of Intelligence and Security is responsible for the preparation and fair presentation of the financial statements in accordance with the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, including the Australian Accounting Standards (which include the Australian Accounting Interpretations). This responsibility includes establishing and maintaining internal controls relevant to the preparation and fair presentation of the financial statements that are free from material misstatement, whether due to fraud or error; selecting and applying appropriate accounting policies; and making accounting estimates that are reasonable in the circumstances.

### *Auditor's Responsibility*

My responsibility is to express an opinion on the financial statements based on my audit. My audit has been conducted 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 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 and fair presentation of the financial statements in order to design audit procedures that are appropriate in the

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

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 accounting policies used and the reasonableness of accounting estimates made by the Inspector-General of Intelligence and Security, as well as evaluating the overall presentation of the financial statements.

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

### ***Independence***

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

### **Auditor's 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 2008 and its financial performance and cash flows for the year then ended.

Australian National Audit Office



Simon Kidman

Executive Director

Delegate of the Auditor-General

Canberra

3 September 2007

**OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY**  
**INCOME STATEMENT**  
*for the year ended 30 June 2008*

<b>Income Statement</b>	<b>Notes</b>	<b>2007-08</b> \$	<b>2006-07</b> \$
<b>INCOME</b>			
Revenues from ordinary activities			
Revenues from Government	3A	1 746 000	1 485 000
<b>Total Revenues from ordinary activities</b>		<u>1 746 000</u>	<u>1 485 000</u>
Gains			
Resources received free of charge	3B	120 000	93 000
<b>Total Gains</b>		<u>120 000</u>	<u>93 000</u>
<b>TOTAL INCOME</b>		<u>1 866 000</u>	<u>1 578 000</u>
<b>EXPENSES</b>			
Employees			
Remuneration	4A	1 036 203	738 462
Superannuation		188 156	166 650
<b>Total employees</b>		<u>1 224 359</u>	<u>905 112</u>
Suppliers			
Resources received free of charge		120 000	93 000
Comcare premium	4B	2 917	2 750
Other goods and services	4B	343 047	337 123
<b>Total suppliers</b>		<u>465 964</u>	<u>432 873</u>
Net losses from sale of assets	4D	-	-
Assets written off	4E	7 196	9 676
Depreciation and Amortisation	4C	16 550	28 743
<b>TOTAL EXPENSES</b>		<u>1 714 069</u>	<u>1 376 404</u>
<b>OPERATING RESULT</b>		<u>151 931</u>	<u>201 596</u>

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

**BALANCE SHEET**  
as at 30 June 2008

Balance Sheet	Notes	2007-08 \$	2006-07 \$
<b>ASSETS</b>			
<b>Financial Assets</b>			
Cash and cash equivalents	5A	273 003	293 105
Receivables - current	5B		
Appropriations receivable		1 059 646	797 800
GST receivable		4 527	2 452
Other debtors		4 703	77 339
Total receivables		<u>1 068 876</u>	<u>877 591</u>
<b>Total financial assets</b>		<u>1 341 879</u>	<u>1 170 697</u>
<b>Non-financial assets</b>			
Infrastructure, plant and equipment	6A	67 687	31 200
Intangibles	6B	1 099	2 541
<b>Other non financial assets</b>			
Prepayments	6C	-	-
<b>Total non-financial assets</b>		<u>68 786</u>	<u>33 741</u>
<b>TOTAL ASSETS</b>		<u>1 410 665</u>	<u>1 204 438</u>
<b>LIABILITIES</b>			
<b>Provisions</b>			
Employee provisions	8A	673 924	596 148
<b>Total provisions</b>		<u>673 924</u>	<u>596 148</u>
<b>Payables</b>			
Suppliers	7A	22 921	46 036
<b>Total payables</b>		<u>22 921</u>	<u>46 036</u>
<b>TOTAL LIABILITIES</b>		<u>696 845</u>	<u>642 184</u>
<b>Net Assets</b>		<u>713 820</u>	<u>562 254</u>
<b>EQUITY</b>			
Asset revaluation reserve		2 146	2 511
Contributed equity		402 000	402 000
Retained Earnings		<u>309 674</u>	<u>157 743</u>
<b>TOTAL EQUITY</b>		<u>713 820</u>	<u>562 254</u>
<b>Current Assets</b>		1 341 879	1 170 697
<b>Non-Current Assets</b>		68 786	33 741
<b>Current Liabilities</b>		679 003	614 025
<b>Non-Current Liabilities</b>		17 842	28 159

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 2008*

Item	Retained Earnings		Asset Revaluation Reserve		Contributed Equity/Capital		Total Equity	
	2008	2007	2008	2007	2008	2007	2008	2007
	\$	\$	\$	\$	\$	\$	\$	\$
<b>Opening Balance</b>	<b>157 743</b>	<b>(43 853)</b>	<b>2 511</b>	<b>9 435</b>	<b>402 000</b>	<b>402 000</b>	<b>562 254</b>	<b>367 582</b>
Net Operating Result	151 931	201 596			-	-	151 931	201 596
<b>Total income and expenses</b>	<b>151 931</b>	<b>201 596</b>			<b>-</b>	<b>-</b>	<b>151 931</b>	<b>201 596</b>
<b>Asset Revaluation Movements</b>			<b>(365)</b>	<b>(6,924)</b>			<b>(365)</b>	<b>(6,924)</b>
Transactions with Owners	-	-	-	-	-	-	-	-
Distributions to owners	-	-	-	-	-	-	-	-
Returns of Capital	-	-	-	-	-	-	-	-
Contributions by Owners	-	-	-	-	-	-	-	-
Appropriation (equity injection)	-	-	-	-	-	-	-	-
Sub-total Transaction with Owners	-	-	-	-	-	-	-	-
Transfers between equity components	-	-	-	-	-	-	-	-
<b>Closing balance at 30 June</b>	<b>309 674</b>	<b>157 743</b>	<b>2 146</b>	<b>2 511</b>	<b>402 000</b>	<b>402 000</b>	<b>713 820</b>	<b>562 254</b>

**OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY**  
**STATEMENT OF CASH FLOWS**  
*for the year ended 30 June 2008*

Cash Flows	Notes	2007-08 \$	2006-07 \$
<b>OPERATING ACTIVITIES</b>			
<b>Cash received</b>			
Appropriations		1 484 154	1 104 200
Net GST refunds		28 558	15 742
Other cash received		152 927	34 120
<b>Total cash received</b>		<u>1 665 639</u>	<u>1 154 062</u>
<b>Cash used</b>			
Employees		(1 194 728)	(892 840)
Suppliers		(363 061)	(259 283)
Other Cash Used		(68 796)	(74 934)
<b>Total cash used</b>		<u>(1 626 585)</u>	<u>(1 227 057)</u>
<b>Net cash used from operating activities</b>	9	<u>39 054</u>	<u>(72 995)</u>
<b>INVESTING ACTIVITIES</b>			
<b>Cash received</b>			
Proceeds from sales of equipment		-	-
<b>Total cash received</b>		<u>-</u>	<u>-</u>
<b>Cash used</b>			
Purchase of equipment		(59 156)	(6 750)
<b>Total cash used</b>		<u>(59 156)</u>	<u>(6 750)</u>
<b>Net cash used from investing activities</b>		<u>( 59 156)</u>	<u>(6 750)</u>
<b>FINANCING ACTIVITIES</b>			
<b>Cash received</b>			
Equity injection		-	-
<b>Total cash received</b>		<u>-</u>	<u>-</u>
<b>Cash used</b>			
Return of equity		-	-
<b>Total cash used</b>		<u>-</u>	<u>-</u>
<b>Net cash used from financing activities</b>		<u>-</u>	<u>-</u>
<b>Net increase/(decrease) in cash held</b>		<u>(20 102)</u>	<u>(79 745)</u>
Cash at beginning of reporting period		<u>293 105</u>	<u>372 850</u>
<b>Cash at the end of the reporting period</b>	9	<u><u>273 003</u></u>	<u><u>293 105</u></u>

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

## STATEMENT OF COMMITMENTS AND CONTINGENCIES

as at 30 June 2008

The Agency had no contingencies to report in either 2006-07 or in 2007-08.

	2008 \$	2007 \$
<b>BY TYPE</b>		
<b>Commitments Receivable</b>		
GST recoverable on commitments	5 308	7 682
<b>Total Commitments Receivable</b>	<u>5 308</u>	<u>7 682</u>
<b>Capital Commitments</b>		
Infrastructure, plant and equipment	-	58 295
<b>Total Capital Commitments</b>	<u>-</u>	<u>58 295</u>
<b>Other Commitments</b>		
Operating Leases	58 395	118 814
<b>Total Other Commitments</b>	<u>58 395</u>	<u>118 814</u>
<b>Net Commitments by Type</b>	<u>53 087</u>	<u>169 427</u>
<b>BY MATURITY</b>		
<b>Commitments Receivable</b>		
<b>Operating Lease income</b>		
One year or less	5 148	1 587
From one to five years	160	850
Over five years	-	-
<b>Total operating lease income</b>	<u>5 308</u>	<u>2 437</u>
<b>Other Commitments Receivable</b>		
One year or less	-	5 244
From one to five years	-	-
Over five years	-	-
<b>Total other commitments receivable income</b>	<u>-</u>	<u>5 244</u>
<b>Commitments Payable</b>		
<b>Capital Commitments</b>		
One year or less	-	58 295
From one to five years	-	-
Over five years	-	-
<b>Total Capital Commitments</b>	<u>-</u>	<u>58 295</u>
<b>Operating Lease Commitments</b>		
One year or less	56 635	63 460
From one to five years	1 760	55 353
Over five years	-	-
<b>Total Operating Lease Commitments</b>	<u>58 395</u>	<u>118 813</u>
<b>Net Commitments by Maturity</b>	<u>53 087</u>	<u>169 427</u>

No contingent rentals exist.

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

## **Note 1 - Summary of Significant Accounting Policies**

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

The objective of the Agency is to meet the following outcome:

Assurance that Australia's intelligence agencies act legally, ethically and with propriety.

The Agency has one output:

Inspect, inquire into, and report on, the activities of the intelligence and security agencies.

The Agency's activities contributing towards this output are classified as departmental. Departmental activities involve the use of assets, liabilities, revenues and expenses controlled or incurred by the agency in its own right.

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

### **1.2 Basis of Accounting**

The financial statements are required by section 49 of the *Financial Management and Accountability Act 1997* and are a General Purpose Financial Report.

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

- Finance Minister's Orders (or FMOs) for reporting periods ending on or after 1 July 2007; and
- Australian Accounting Standards and Interpretations issued by the Australian Accounting Standards Board (AASB) that apply for the reporting period.

The financial report has been prepared on an accrual basis and is in accordance with the historical cost convention, except for certain assets 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 report is presented in Australian dollars and values are rounded to the nearest dollar.

Assets and liabilities are recognised in the Balance Sheet when and only when it is probable that future economic benefits will flow and the amounts of the assets or liabilities can be reliably measured.

However, assets and liabilities arising under agreements equally proportionately unperformed are not recognised unless required by an Accounting Standard. Liabilities and assets that are unrecognised are reported in the Schedule of Commitments and the Schedule of Contingencies.

Revenues and expenses are recognised in the Income Statement when and only when the flow or 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, the Agency 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.

## Note 1 - Summary of Significant Accounting Policies (continued)

### 1.4 Statement of Compliance

#### Adoption of new Australian Accounting Standard Requirements

No accounting standard has been adopted earlier than the effective date in the current period.

#### Financial Statement Disclosure

AASB 7 *Financial Instruments: Disclosures* is effective for reporting periods beginning on or after 1 January 2007 and amends the disclosure requirements for financial instruments. In general, AASB 7 requires greater disclosure than that previously required. Associated with the introduction of AASB 7 a number of accounting standards were amended to reference the new standard or remove the present disclosure requirements through 2005-10 Amendments to Australian Accounting Standards (AASB 132, AASB 101, AASB 114, AASB 117, AASB 133, AASB 139, AASB 1, AASB 4, AASB 1023 & AASB 1038). These changes have no financial impact but will affect the disclosure presented in future financial reports.

#### Other Effective Requirement Changes

The following new standards, amendments to standards or interpretations for the current financial years have no material financial impact or do not apply to the operations of the Agency:

- AASB 101 *Presentation of Financial Statements*
- AASB 1048 *Interpretation and Application of Standards*
- AASB 2007-5 *Amendments to Australian Accounting Standard – Inventories Held for Distribution by Not-for-Profit Entities* (AASB 102)
- 2007-4 *Amendments to Australian Accounting Standards arising from ED 151 and Other Amendments and Erratum: Proportionate Consolidation*
- 2007-7 *Amendments to Australian Accounting Standards*
- UIG Interpretation 11 AASB 2 – *Group and Treasury Share Transactions* and 2007-1 *Amendments to Australian Accounting Standards arising from AASB Interpretation 11*
- UIG Interpretation 10 *Interim Financial Reporting and Impairment*
- UIG Interpretation 1003 *Australian Petroleum Resource Rent Tax*
- ERR Erratum *Proportionate Consolidation* (AASB 101, AASB 107, AASB 121, AASB 127, Interpretation 113)

#### Future Australian Accounting Standard Requirements

The following new standards, amendments to standards or interpretations have been issued by the Australian Accounting Standards Board effective for future reporting periods, but either are not applicable to the operations of the Agency or will not have a material impact:

- AASB 3 *Business Combinations*
- AASB 101 *Presentation of Financial Statements*
- AASB 123 *Borrowing Costs*
- AASB 127 *Consolidation and Separate Financial Statements*
- AASB 1004 *Contributions*
- AASB 1050 *Administered Items*
- AASB 1051 *Land Under Roads*
- AASB 1052 *Disaggregated Disclosures*
- AASB Interpretation 12 *Service Concession Arrangements* and 2007-2 *Amendments to Australian Accounting Standards arising from AASB Interpretation 12*.
- AASB 8 *Operating Segments* and 2007-3 *Amendments to Australian Accounting Standards arising from AASB 8*.

**Note 1 - Summary of Significant Accounting Policies (continued)**

- 2007-6 Amendments to Australian Accounting Standards arising from AASB 123 Borrowing Costs.
- AASB 2007-2 Amendments to Australian Accounting Standards arising from AASB Interpretation 12 (AASB 1, AASB 117, AASB 118, AASB 120, AASB 121, AASB 127, AASB 131 & AASB 139)
- AASB 2007-8 Amendments to Australian Accounting Standards arising from AASB 101
- AASB 2007-9 Amendments to Australian Accounting Standards arising from the Review of AASs 27, 29 and 31 (AASB 3, AASB 5, AASB 8, AASB 101, AASB 114, AASB 116, AASB 127 & AASB 137)
- AASB 2008-1 Amendments to Australian Accounting Standard – Share-based Payments: Vesting Conditions and Cancellations (AASB 2)
- AASB 2008-2 Amendments to Australian Accounting Standards – Puttable Financial Instruments and Obligations arising on Liquidation (AASB 7, AASB 101, AASB 132, AASB 139 & Interpretation 2).
- AASB 2008-3 Amendments to Australian Accounting Standards arising from AASB 3 and AASB 127 (AASBs 1, 2, 4, 5, 7, 101, 107, 112, 114, 116, 121, 128, 131, 132, 133, 134, 136, 137, 138 & 139 and Interpretations 9 & 107)
- AASB 2008-4 Amendments to Australian Accounting Standard – Key Management Personnel Disclosures by Disclosing Entities (AASB 124)
- AASB Interpretation 1 Changes in Existing Decommissioning, Restoration and Similar Liabilities
- AASB Interpretation 4 Determining Whether an Arrangement Contains a Lease
- AASB Interpretation 13 Customer Loyalty Programmes.
- AASB Interpretation 14 AASB 119 – The Limit on a Defined Benefit Asset, Minimum Funding Requirements and their Interaction.
- AASB Interpretation 1038 Contributions by Owners Made To Wholly-Owned Public Sector Entities
- AASB 1049 Whole of Government and General Government Sector Financial Reporting

**1.5 Revenue**

Revenues from Government

The full amount of the departmental appropriation for Agency outputs for the year is recognised as revenue. Appropriations receivable are recognised at their nominal amounts.

Other Revenue

Receivables for goods and services, which have 30 day terms, are recognised at the nominal amounts due less any provisions for bad and doubtful debts. Collectability of debts is reviewed at balance date. Provisions are made when collectability of the debt is no longer probable.

**1.6 Gains**

Resources Received Free of Charge

Services received free of charge are recognised as revenue when and only when a fair value can be reliably determined and the services would have been purchased if they had not been donated. Use of those resources is recognised as an expense.

The main resources received free of charge in 2007-08 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 12.

## **Note 1 - Summary of Significant Accounting Policies (continued)**

### **1.7 Transactions with the Government as Owner**

#### Equity Injection

Amounts appropriated which are designated as 'equity injections' for a year (less any formal reductions) are recognised directly to Contributed Equity in that year.

### **1.8 Employee Benefits**

Liabilities for services rendered by employees are recognised at the reporting date to the extent that they have not been settled.

Liabilities for 'short-term employee benefits' (as defined in AASB 119) and termination benefits due within twelve months 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.

All other employee benefit liabilities are measured as the present value of the estimated future cash outflows to be made in respect of services provided by employees up to the reporting date.

#### 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 the Agency is estimated to be less than the annual entitlement for sick leave.

The leave liabilities are calculated on the basis of employees' remuneration, including the Agency'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 AASB 119 as at 30 June 2008. The estimate of the present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

#### Superannuation

Staff of the Agency are members of the Commonwealth Superannuation Scheme (CSS), the Public Sector Superannuation Scheme (PSS) or the PSS accumulation plan (PSSap).

The CSS and PSS are defined benefit schemes for the Australian Government. The PSSap is a defined contribution scheme.

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 by the Department of Finance and Deregulation as an administered item.

The Agency makes employer contributions to the employee superannuation scheme at rates determined by an actuary to be sufficient to meet the current cost of the Government of the superannuation entitlements of the Agency's employees. The Agency 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.

### **Note 1 - Summary of Significant Accounting Policies (continued)**

All other employee benefit liabilities are measured as the present value of the estimated future cash outflows to be made in respect of services provided by employees up to the reporting date.

#### **1.9 Financial Assets**

The Agency classifies its financial assets in the following categories:

- 'loans and receivables'.

The classification depends on the nature and purpose of the financial assets and is determined at the time of initial recognition.

##### Loans and receivables

Receivables are recognised at their nominal amounts due less any provisions for bad and doubtful debts. Collectability of debts is reviewed at balance date. Provisions are made when collection of the debt is judged to be less rather than more likely.

Credit terms are net 30 days (2006–07: 30 days).

##### Impairment of financial assets

Financial assets are assessed for impairment at each balance date.

#### **1.10 Financial Liabilities**

Financial liabilities are classified as either financial liabilities 'at fair value through profit or loss' or other financial liabilities.

##### Supplier and other payables

Supplier and other payables are recognised at their amortised cost, being the amounts at which the liabilities will be settled. 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.

#### **1.11 Cash**

Cash means notes and coins held and any deposits held at call with a bank or financial institution. Cash is recognised at its nominal amount.

#### **1.12 Acquisition of Assets**

Assets are recorded at cost on acquisition.

#### **1.13 Infrastructure, Plant and Equipment**

##### Asset Recognition Threshold

Purchases of 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).

**Note 1 - Summary of Significant Accounting Policies (continued)**

Revaluations

Plant and equipment are carried at valuation. Fair values have been determined by market selling price.

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. A full revaluation was conducted at 30 June 2008 by an independent valuer.

Revaluation adjustments are made on a class basis. Any revaluation increment is credited to equity under the heading of asset revaluation reserve except to the extent that it reverses a previous revaluation decrement of the same asset class that was previously recognised through operating result. Revaluation decrements for a class of assets are recognised directly through operating result 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 and Amortisation

Depreciable property plant and equipment assets are written-off to their estimated residual values over their estimated useful lives to the Agency using in all cases, the straight-line method of depreciation.

Depreciation rates (useful lives) and methods are reviewed at each reporting date and necessary adjustments are recognised in the current, or current and future reporting periods, as appropriate. Residual values are re-estimated when assets are revalued.

Depreciation and amortisation rates are for 1 to 5 years.

Impairment

All assets were assessed for impairment at 30 June 2008 and remaining useful lives were reassessed as part of the revaluation exercise. There were no indications of impairment and the assets are valued at their fair value.

**1.14 Intangibles**

The Agency's intangibles consists of purchased software only. These assets are carried at cost less accumulated amortisation and accumulated impairment losses. Software is amortised on a straight-line basis over its anticipated useful life.

All software assets are assessed for indications of impairment as at 30 June 2008.

**1.15 Taxation**

The Agency 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 for:

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

**1.16 Insurance**

The Office of the Inspector-General of Intelligence and Security has insured for risks through the Government's insurable risk managed fund, called 'Comcover'. Workers compensation is insured through the Government's Comcare.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for the year ended 30 June 2008

**Note 1 - Summary of Significant Accounting Policies (continued)**

**1.17 Comparative Figures**

Comparative figures have been adjusted to conform to changes in presentation in these financial statements where required.

**Note 2 – Events after the Balance Sheet Date**

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

**Note 3 – Income**

**Revenue**

Note 3A – Revenues from Government

	2008	2007
	\$	\$
<u>Revenue from Government</u>		
Appropriations for outputs	1 746 000	1 485 000
<b>Total revenue from government</b>	<u>1 746 000</u>	<u>1 485 000</u>

**Gains**

Note 3B – Other Gains

	2008	2007
	\$	\$
<b>Other Gains</b>		
Resources Received free of charge	120 000	93 000
<b>Total Other Gains</b>	<u>120 000</u>	<u>93 000</u>

**Note 4 – Expenses**

	2008	2007
	\$	\$
<b>Note 4A – Employee Benefits</b>		
Wages and salaries	946 552	726 444
Superannuation	188 156	166 650
Leave and other entitlements	89 651	12 018
Separation and redundancies	-	-
<b>Total employee benefits</b>	<u>1 224 359</u>	<u>905 112</u>

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for the year ended 30 June 2008

	2008	2007
	\$	\$
<u>Note 4B - Suppliers</u>		
Provision of goods – related entities	-	-
Provision of goods – external entities	15 614	236 845
Rendering of services – related entities	288 884	138 000
Rendering of services – external entities	158 549	55 278
Workers compensation premiums	2 917	2 750
<b>Total supplier expenses</b>	<b>465 964</b>	<b>432 873</b>

	2008	2007
	\$	\$
<u>Note 4C – Depreciation and Amortisation</u>		
Depreciation – Infrastructure, plant and equipment	15 108	27 301
Amortisation – Intangibles	1 442	1 442
<b>Total Depreciation and Amortisation</b>	<b>16 550</b>	<b>28 743</b>

	2008	2007
	\$	\$
<u>Note 4D – Net Losses from Sale of Assets</u>		
Infrastructure, plant and equipment:		
Proceeds from sale	-	-
Carrying value of assets sold	-	-
Selling expense	-	-
<b>Total losses from asset sales</b>	<b>-</b>	<b>-</b>

	2008	2007
<u>Note 4E – Assets Written Off</u>		
Infrastructure, plant and equipment	7 196	9 676
<b>Total Assets Written Off</b>	<b>7 196</b>	<b>9 676</b>

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for the year ended 30 June 2008

**Note 5 – Financial Assets**

	2008	2007
	\$	\$
<u>Note 5A – Cash and cash equivalents</u>		
Cash on hand or on deposit	273 003	293 105
<b>Total cash and cash equivalents</b>	<b>273 003</b>	<b>293 105</b>
	2008	2007
	\$	\$
<u>Note 5B – Trade and other receivables</u>		
Appropriations Receivable:		
For existing outputs	1 059 646	797 800
<b>Total appropriations receivable</b>	<b>1 059 646</b>	<b>797 800</b>
GST receivable from the Australian Taxation Office	4 527	2 452
Other receivables	4 703	77 339
<b>Total other receivables</b>	<b>9 230</b>	<b>79 791</b>
<b>Total trade and other receivables (gross)</b>	<b>1 068 876</b>	<b>877 591</b>
Less Allowance for Doubtful Debts	-	-
<b>Total trade and other receivables (net)</b>	<b>1 068 876</b>	<b>877 591</b>
Receivables are aged as follows:		
Not overdue	1 068 876	877 591

All Receivables are current.

**Note 6 – Non-Financial Assets**

Note 6A – Infrastructure, plant and equipment

	2008	2007
	\$	\$
<b>Infrastructure, plant and equipment</b>		
Infrastructure, plant and equipment:		
- gross carrying value (at fair value)	67 687	31 200
- accumulated depreciation	-	-
Infrastructure, plant and equipment		
- gross carrying value (at cost)		
- accumulated depreciation		
<b>Total Infrastructure, Plant and Equipment (non-current)</b>	<b>67 687</b>	<b>31 200</b>

Note 6B – Intangibles

Previously intangibles have been reported as Infrastructure, plant and equipment. Comparatives have been adjusted.

	2008	2007
	\$	\$
<b>Intangibles</b>		
Computer software at cost:		
Purchased	5 769	5 769
<b>Total computer software</b>	<u>5 769</u>	<u>5 769</u>
Accumulated amortisation	(4 670)	(3 228)
<b>Total intangibles (non-current)</b>	<u>1 099</u>	<u>2 541</u>

Note 6C – Other Non-Financial Assets

	2008	2007
	\$	\$
<b>Other Non-Financial Assets</b>		
Prepayments	-	-
<b>Total Other Non-Financial Assets</b>	<u>-</u>	<u>-</u>

Note 6D – Analysis of Infrastructure, plant and equipment

Table A – Reconciliation of the Opening and Closing Balances of Infrastructure, Plant and Equipment (2007-08)

Item	Infrastructure, Plant and Equipment
As at 1 July 2007	
Gross book value	31 200
Accumulated depreciation	-
Opening Net book value as at 1 July 2007	31 200
Additions	
by purchase	59 156
Depreciation expense	(15 108)
Disposals	
Net cost of disposals	(7 196)
Revaluations and impairments through equity	(365)
<b>Net Book Value 30 June 2008</b>	<b>67 687</b>
<b>Net Book Value as at 30 June 2008 represented by:</b>	
Gross book value	67 687
Accumulated depreciation	-

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for the year ended 30 June 2008

Table A – Reconciliation of the Opening and Closing Balances of Infrastructure, Plant and Equipment (2006-07)

Item	Infrastructure Plant and Equipment
As at 1 July 2006	
Gross book value	139 322
Accumulated depreciation	(70 970)
Opening Net book value as at 1 July 2006	68 352
Additions	
by purchase	6 750
Depreciation expense	(27 301)
Disposals	
Net cost of disposals	(9 677)
Revaluations and impairments through equity	(6,924)
<b>Net Book Value 30 June 2007</b>	<b>31 200</b>
<b>Net Book Value as at 30 June 2007 represented by:</b>	
Gross book value	31 200
Accumulated depreciation	-

Note 6E – Analysis of Intangibles

Table A – Reconciliation of the Opening and Closing Balances of Intangibles (2007-08)

Item	Computer Software Purchased
As at 1 July 2007	
Gross book value	5 769
Accumulated depreciation	(3 228)
Opening Net book value as at 1 July 2007	2 541
Additions	
by purchase or internally developed	-
Amortisation expense	(1 442)
Disposals	
Net cost of disposals	-
Revaluations and impairments through equity	-
<b>Net Book Value 30 June 2008</b>	<b>1 099</b>
<b>Net Book Value as at 30 June 2008 represented by:</b>	
Gross book value	5 769
Accumulated amortisation & impairment	(4 670)

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for the year ended 30 June 2008

Table A – Reconciliation of the Opening and Closing Balances of Intangibles (2006-07)

Item	Computer Software Purchased
As at 1 July 2006	
Gross book value	5 769
Accumulated depreciation	(1 785)
Opening Net book value as at 1 July 2006	3 984
Additions by purchase or internally developed	
Amortisation expense	(1 442)
Disposals	
Net cost of disposals	
Revaluations and impairments through equity	
<b>Net Book Value 30 June 2007</b>	<b>2 542</b>
<b>Net Book Value as at 30 June 2007 represented by:</b>	
Gross book value	5 769
Accumulated depreciation	(3 228)

All revaluations are independent and are conducted in accordance with the revaluation policy stated at Note 1. In 2007-08, the revaluations were conducted by an independent valuer Peter Dorrough FAPI (Certified Practising Valuer).

**Note 7 – Payables**

	2008	2007
	\$	\$
<u>Note 7A – Suppliers</u>		
Trade creditors	22 921	46 036
<b>Total Suppliers</b>	<b>22 921</b>	<b>46 036</b>

Supplier payables are represented by:

Current	22 921	46 036
Non-current	-	-
<b>Total supplier payables</b>	<b>22 921</b>	<b>46 036</b>

**Note 8 – Provisions**

	2008	2007
	\$	\$
<u>Note 8A – Employee provisions</u>		
Salaries and wages	11 131	7 016
Leave	616 436	545 353
Superannuation	46 357	41 795
Other – Fringe Benefits Tax	-	1 984
<b>Total Employee Provisions</b>	<b>673 924</b>	<b>596 148</b>

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for the year ended 30 June 2008

Employee provisions are represented by:

Current	656 082	567 989
Non-current	17 842	28 159
Total employee provisions	673 924	596 148

The classification of current includes amounts for which there is not an unconditional right to defer settlement by one year, hence in the case of employee provisions the above classification does not represent the amount expected to be settled within one year of the reporting date. Employee provisions expected to be settled in twelve months from the reporting date are \$132,934 (2007: \$139,891), and in excess of one year \$523,148 (2007: \$428,098).

**Note 9 – Cash Flow Reconciliation**

	2007-08 \$	2006-07 \$
<b>Reconciliation of Cash and cash equivalents as per Balance Sheet to Cash flow statement</b>		
<b>Report cash and cash equivalents as per:</b>		
Cash Flow Statement	273 003	293 105
Balance Sheet	273 003	293 105
Difference	-	-
<b>Reconciliation of net surplus to net cash from operating activities:</b>		
Operating result	151 931	201 596
Depreciation	16 550	28 743
Gain/Loss on disposal of assets	7 196	9 676
Write-off of assets	-	-
Increase/(Decrease) in provision for employee liabilities	77 776	102 376
Increase/(Decrease) in supplier trade creditors	(23 114)	20 126
(Increase)/Decrease in appropriations receivables	(261 846)	(380 800)
(Increase)/Decrease in other assets	72 636	(55 198)
(Increase)/Decrease in other prepayments	-	494
(Increase)/Decrease in GST receivable	(2 075)	(8)
(Increase)/Decrease in transfers to the Official Public Account	-	-
<b>Net cash flow from operating activities</b>	<b>39 054</b>	<b>(72 995)</b>

**Note 10 – Contingent Liabilities and Assets**

The Agency had no contingent liabilities or contingent assets at the reporting date.

**Note 11 – Executive Remuneration**

Executive Remuneration	2007-08	2006-07
Number of executives in the range \$385 000 to \$399 999:	1	1
The aggregate amount of separation and redundancy/termination benefit payments during the year to executives shown above:	Nil	Nil

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for the year ended 30 June 2008

**Note 12 – Remuneration of Auditor**

Financial statement audit services are provided free of charge to the Agency. No other services were provided by the Auditor-General.

Remuneration of Auditor	2007-08	2006-07
The fair value of audit services provided was:	<b>\$16 000</b>	\$14 100

**Note 13 – Staffing Level**

The average staffing level for the Agency in 2007-08 was 9.37 (2006-07: 7).

**Note 14 – Financial Instruments**

Note 14A – Categories of Financial Instruments

Financial Instruments	2007-08	2006-07
<b>Loans and Receivables</b>		
Loans and Receivables		
Cash and cash equivalents	273 003	293 105
Trade receivables	4 703	77 339
<b>Carrying amounts of financial assets</b>	<u>277 706</u>	<u>370 444</u>
<b>Financial Liabilities</b>		
Other Liabilities measured at amortised cost		
Payables – Suppliers	22 921	46 036
<b>Carrying amounts of financial liabilities</b>	<u>22 921</u>	<u>46 036</u>

Note 14B – Net Income and Expense from Financial Assets

Loans and Receivables	2007-08	2006-07
Interest Revenue	-	-
<b>Net gain (loss) from financial assets</b>	<u>-</u>	<u>-</u>

Note 14C – Net Income and Expense from Financial Liabilities

Other Liabilities	2007-08	2006-07
Interest Expense	-	-
<b>Net gain (loss) from financial liabilities</b>	<u>-</u>	<u>-</u>

Note 14D – Fair Value of Financial Instruments

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

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for the year ended 30 June 2008

Note 14E – Credit Risk

The Agency 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 the Agency 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.

	<b>Not Past Due Nor Impaired 2008</b>	Not Past Due Nor Impaired 2007	<b>Past due or Impaired 2008</b>	Past due or Impaired 2007
<b>Loans &amp; Receivables</b>				
Cash and cash equivalents	<b>273 003</b>	293 105		
Trade receivables	<b>4 703</b>	77 339		
<b>Total</b>	<b>277 706</b>	370 444		

Note 14F – Liquidity Risk

The Agency's financial liabilities only include payables. Any exposure to liquidity risk is based on the notion that the Agency 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.

The following table illustrates the maturities for financial liabilities.

	On Demand 2008	Within 1 year 2008	1 to 5 years 2008	Greater than 5 years 2008	Total 2008
<b>Other Liabilities at amortised cost</b>					
Payables - Suppliers		22 921			22 921
<b>Total</b>		<b>22 921</b>			<b>22 921</b>
	On Demand 2007	Within 1 year 2007	1 to 5 years 2007	Greater than 5 years 2007	Total 2007
<b>Other Liabilities at amortised cost</b>					
Payables - Suppliers		46 036			46 036
<b>Total</b>		<b>46 036</b>			<b>46 036</b>

Note 14G - Market Risk

The Agency does not participate in any transactions in foreign currencies and as such is not exposed to market risk as a result of changes in exchange rates. The Agency also only has indirect exposure in interest rates and as such the impact on supplier costs is not significant.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS

for the year ended 30 June 2008

**Note 15 – Special Accounts**

The Agency has two special accounts established under section 20 of the FMA Act. The accounts established are:

- Other Trust Moneys Account (s20 FMA Act 1997). The purpose of this account is 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 is for expenditure in connection with services performed on behalf of other Governments and bodies that are not FMA agencies.

These accounts have zero balances and have never been active.

**Note 16 – Appropriations**

Note 16A – Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund for Ordinary Annual Services Appropriations (Acts 1 and 3)

Particulars	Total
<b>Year Ended 30 June 2008</b>	<b>\$</b>
Balance carried from previous year	766 318
Appropriation Act (No.1) 2007-2008	1 754 000
Appropriation Act (No.3) 2007-2008	-
Subsection 9(1) Appropriation Act (No.1) 2007-2008 determination to reduce appropriation	(8 000)
Section 31 receipts (FMA Act)	150 147
Section 30 receipts (FMA Act)	2 636
GST credits (FMA s30A)	28 558
Total Appropriations available for payments	2 693 659
Payments made (GST inclusive)	1 683 522
<b>Balance carried to next year</b>	<b>1 010 137</b>
Represented by:	
Cash	253 964
Add: Receivables – Net GST Receivable from the ATO	4 527
Receivables – departmental appropriations	751 646
<b>Total</b>	<b>1 010 137</b>
<b>Year Ended 30 June 2007</b>	
Balance carried from previous year	459 119
Appropriation Act (No.1) 2006-2007	1 485 000
Appropriation Act (No.3) 2006-2007	-
GST credits (FMA s30A)	15 128
Section 31 receipts (FMA Act)	
Total Appropriations available for payments	1 959 247
Payments made (GST inclusive)	1 192 929
<b>Balance carried to next year</b>	<b>766 318</b>
Represented by:	
Cash	274 066
Add: Receivables – Net GST Receivable from the ATO	2 452
Receivables – departmental appropriations	489 800
<b>Total</b>	<b>766 318</b>

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for the year ended 30 June 2008

**Note 16 – Appropriations (continued)**

Note 16B – Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund for Other than Ordinary Annual Services Appropriations (Acts 2 and 4)

Particulars	Total \$
<b>Year Ended 30 June 2008</b>	
Balance carried from previous year	327 039
Appropriation Act (No.2) 2007-2008	-
Appropriation Act (No.4) 2007-2008	-
GST credits (FMA Act s30A)	-
Total Appropriations available for payments	327 039
Payments made (GST inclusive)	-
<b>Balance carried to next year</b>	<b>327 039</b>
Represented by:	
Cash	19 039
Add: Receivables – Receivable from the Official Public Account	308 000
<b>Total</b>	<b>327 039</b>
<b>Year Ended 30 June 2007</b>	
Balance carried from previous year	333 175
Appropriation Act (No.2) 2006-2007	-
Appropriation Act (No.4) 2006-2007	-
GST credits (FMA Act s30A)	614
Total Appropriations available for payments	333 789
Payments made (GST inclusive)	6 750
<b>Balance carried to next year</b>	<b>327 039</b>
Represented by:	
Cash	19 039
Add: Receivables – Receivable from the Official Public Account	308 000
<b>Total</b>	<b>327 039</b>

The Agency received \$402 000 as an equity injection in the financial year ended 30 June 2005. The Agency holds \$308 000 of this amount in the Official Public Account to partially fund the non-current portion of accrued leave liabilities.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
for the year ended 30 June 2008

**Note 17 - Reporting of Outcomes**

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

Note 17A – Net Cost of Outcome Delivery

The net cost of this outcome in 2007-08 was \$1 594 069 (Appropriation: \$1 746 000).

Note 17B – Agency Revenue and Expenses by Output Group

Revenue and Expenses	Output Group 1		OUTCOME TOTAL	
	2007-08	2006-07	2007-08	2006-07
	\$	\$	\$	\$
Operating revenues				
Revenues from government	1 746 000	1 485 000	1 746 000	1 485 000
Other income	120 000	93 000	120 000	93 000
<b>Total operating revenues</b>	<b>1 866 000</b>	<b>1 578 000</b>	<b>1 866 000</b>	<b>1 578 000</b>
Operating expenses				
Employees	1 224 359	905 112	1 224 359	905 112
Suppliers	465 964	432 873	465 964	432 873
Net losses from sale of assets	-	-	-	-
Assets written off	7 196	9 676	7 196	9 676
Equipment depreciation	16 550	28 743	16 550	28 743
<b>Total operating expenses</b>	<b>1 714 069</b>	<b>1 376 404</b>	<b>1 714 069</b>	<b>1 376 404</b>

**Note 18 – Compensation and Debt Relief**

No 'Act of Grace' payments were made during the reporting period, (2006-07: nil).

No waivers of amounts owing to the Commonwealth were made during the reporting period, (2006-07: nil).

No payments were made under the 'Defective Administration Scheme' during the reporting period, (2006-07: nil).

No payments were made under section 73 of the *Public Service Act 1999*, (2006-07: nil).

# Annex 1

## complaint and inquiry statistics

**Table 1**

**IGIS Act inquiries actioned between 1 July 2007 – 30 June 2008**

Agency	Source	Date initiated	Type of Inquiry <sup>1</sup>	Conclusion Notified	Current Status
ONA	Own motion	14/02/07	Full	05/12/07	Closed
ASIO	Public	29/03/07	Preliminary	27/07/07	Closed
DIG <sup>2</sup>	Own motion	05/06/07	Full	15/02/08	Closed
ASIO	Own motion	10/07/07	Preliminary	24/10/07	Closed
ASIO	Public	27/07/07	Full	05/12/07	Closed
ASIO	Public	27/07/07	Preliminary	01/11/07	Closed
ASIO	Public	01/08/07	Preliminary	26/10/07	Closed
ASIO	Employee	11/10/07	Preliminary	16/11/07	Closed
ASIO	Public	17/10/07	Full	15/02/08	Closed
ASIO	Public	02/11/07	Preliminary	22/01/08	Closed
ASIO	Own motion	14/11/07	Full		Open
ASIO	Public	23/11/07	Preliminary	22/02/08	Closed
ASIO	Ex-employee	03/12/07	Preliminary	21/04/08	Closed
ASIO	Public	03/12/07	Preliminary	29/02/08	Closed
ASIS	Public	04/12/07	Preliminary	20/12/07	Closed
ASIO	Public	14/12/07	Preliminary	17/01/08	Closed
DIO	Own motion	29/02/08	Full		Open
ASIS	Public	19/03/08	Preliminary	23/04/08	Closed
ASIS	Public	21/04/08	Preliminary	10/06/08	Closed
ASIO	Public	30/05/08	Preliminary	26/06/08	Closed
ASIO	Ex-employee	01/06/08	Preliminary		Open

<sup>1</sup> A preliminary inquiry allows the Inspector-General to determine whether the issues raised fall within the jurisdiction of the Inspector General and whether a full inquiry should be conducted. A full inquiry allows the Inspector-General to use the complete range of statutory powers in the IGIS Act.

<sup>2</sup> Defence Intelligence Group (comprising DSD, DIGO and DIO)

**Table 2**

Summary of non-immigration related concerns about AIC agencies that were handled administratively 1 July 2007 – 30 June 2008

Agency	Number of Complaints	Public	Employee or Ex-employee	Former Complainant	New Complainant
ASIO	56	49	7	21	35
ASIS	6	2	4	0	6
DSD	3	2	1	1	2
DIGO	2	1	1	1	1
DIO	5	1	4	2	3
ONA	1	1	0	0	1
AIC	2	2	0	0	2
Total Complaints	75	58	17	25	50

**Table 3**

Immigration related concerns that were handled administratively 1 July 2007 – 30 June 2008

Visa Category	Carried over from 2006–07	Migration Agent	Complainant	Complaint's spouse	Commonwealth Ombudsman	Total Complaints Handled	Number closed as at 30/06/2008
Protection	2	11	1	0	0	14	12
Spouse	4	25	3	72	5	109	109
Skilled	3	9	20	0	0	32	32
Marriage	0	5	0	8	0	13	13
Family	1	8	0	2	0	11	11
Temporary	1	4	0	1	0	6	6
Other	4	5	4	10	0	23	23
Total Complaints	15	67	28	93	5	208	206

# Annex 2

## consultancy services let during FY 2007–08 of \$10 000 or more

Consultant's Name	Description	Contract Price (GST inclusive)	Selection Process (1)	Justification (2)
WJ Blick	Specialist operational audits	\$14 280	Direct sourcing	B
WJ Blick	Specialist operational audits	\$19 635	Direct sourcing	B
Workplace Research	Specialist advice and assistance in connection with an inquiry	\$17 105	Direct sourcing	B & C
<b>Total</b>		<b>\$51 020</b>		

(1) Explanation of selection process terms drawn from the *Commonwealth Procurement Guidelines* (January 2005):

Direct sourcing: A form of restricted tendering, available only under certain defined circumstances, with a single potential supplier or suppliers being invited to bid because of their unique expertise and /or their special ability to supply the goods and /or services sought.

(2) Justification for decision to use consultancy:

- A – skills currently unavailable within agency
- B – need for specialised or professional skills
- C – need for independent research or assessment

# Annex 3

## report on the independence and integrity of ONA assessments

### Key Judgements

1. This formal inquiry (conducted pursuant to section 8(3) of the *Inspector-General of Intelligence and Security Act 1986*), examined the independence and integrity of ONA's assessment work in the 12 months to September 2007. It included a survey and extensive discussions with staff, as well as scrutiny of selected records.
2. ONA's internal culture is one of constructive debate and contestability, and analysts are well imbued with the concept of ONA judgments needing to be independent. There are several internal processes which support independence and integrity in the preparation of assessments and analysts were very positive about these.
3. There was no evidence or indication of improper pressure or attempted direction from ministers or their offices.
4. The general view of analysts is that ONA's assessments are independent and this was also my impression from reading the body of work over the period. One particular assessment was questioned, and I subjected it to close scrutiny including by formal interviews of two senior staff. The sworn testimony to me, and viewing the assessment in the totality of ONA's work on the topic, satisfied me that the assessment had been prepared with integrity.
5. A small minority of ONA staff feel that the careful presentation of some judgements compromises the message intended, but the small number of instances given to me did not prove the point.
6. While confident that ONA had always held its ground, a minority of staff were concerned that on rare occasions policy departments went beyond legitimately robust debate into bullying. The frequency with which this was perceived as occurring is low but the Director-General will emphasise at induction and other suitable opportunities, that staff shouldn't hesitate to raise any concerns with ONA managers if they feel it is occurring.
7. The general practice is for draft assessments to be circulated to all analysts within ONA for comment, but in practice some exceptions are made. The policy should reflect this and be clear on who can authorise exceptions.
8. While the documenting of source information by some analysts is of a high standard, there is room for improvement by others. The Director-General has recently issued revised instructions to analysts on the requirements. Inconsistencies between branches were also apparent in the new practice of regular internal review of key judgements made in the previous six months, but with the second iteration showing distinct improvement.
9. The actual keeping of records on the development of each assessment was not consistent and I have made a recommendation as to the minimum set I would expect to be available for each assessment.

10. No analyst accessed the formal internal dissent mechanism (in practice available after an assessment is published) in the period covered by this inquiry. Arguably there is scope for some arrangement to ensure senior ONA management is always aware of significant internal differences of opinion prior to assessments being finalised. During the course of the inquiry the Director-General clarified procedures in relation to recording external dissent.
11. National Assessments are seen as independent by analysts, and I had no concerns about ONA's approach to them.
12. I was satisfied that ONA biographies are independent and objective.

# Annex 4

## principles of analytic integrity – DIO

### What analytic integrity at DIO is...

- Assessments are:
  - focused in accordance with DIO's mandate.
  - made objectively
  - reflect careful and thorough consideration of all sources of information
  - not influenced by improper external (outside DIO) pressure/direction, and
  - reviewed routinely in the light of new information and to learn lessons.
- Analysts exercise and develop high level skills:
  - in source analysis
  - in assessing what is or isn't supported by available information
  - constructively questioning other analysts' work, with debates ideas driven and not personality based, and
  - having intellectual courage.
- The culture promotes independent thinking
  - Managers promote openness and sharing, a sense of shared purpose and teamwork, consultation, professionalism and impartiality.
  - The organisation fosters and develops high quality intelligence analysis that adequately accounts for cognitive bias and complexity.
  - Analysts are able to express dissent, during the drafting process, from the prevailing view in the organisation without detriment to career aspirations.

### What analytic integrity at DIO is not...

- Assessments are not:
  - outside DIO's mandate
  - biased towards the organisation's or stakeholders desired judgments rather than being objective in their own right
  - based on only that information that supports a pre-determined or earlier argument/position, or
  - based on the passive acceptance of information.
- Analysts who:
  - rely on the status quo; not revisiting judgments when there is new information
  - stretch or 'cherry-pick' information to fit particular views
  - ignore gaps or limitations in available information, or
  - overly qualify judgments.
- The culture stifles debate and dissent.
  - Intolerance of different views; groupthink.
  - Analysts are punished directly or indirectly for expressing contra-views.

# Annex 5

## inquiry into Organisational Suitability Assessment processes in Defence

### Executive Summary

- This formal inquiry (conducted pursuant to section 8 of the *Inspector-General of Intelligence and Security Act 1986*) examined the existing Organisational Suitability Assessment (OSA) policies, procedures and practices in the three Defence intelligence agencies – DIGO, DIO and DSD.
- The inquiry included:
  - examination of relevant policy and procedures documentation
  - interviews with a cross-section of employees and key staff
  - consultation with Deputy Secretary of Intelligence, Security and International Policy and Defence intelligence agency heads, and
  - expert examination of the psychometric instruments used and clinical assessments made by Defence intelligence psychologists.
- The general picture of the management of OSA policies and procedures within the Defence intelligence agencies is a positive one, although there are a number of important changes required to enhance decision-making and the reliability and validity of assessments, and to ensure that some procedural aspects align fully with the legal and policy framework.
- The OSA was implemented as a tool for improving personnel security on the basis of a recommendation by Mr WJ Blick PSM AM in early 2000 following his investigation of the activities of a former DIO officer, Mr Jean-Philippe Wispelaere who was convicted in the United States on espionage-related offences.
- It has since evolved to serve two separate purposes – security suitability and organisational ‘fit’. The first of these purposes is seeking to ascertain if a prospective or existing employee poses a threat to security. The second purpose is to assess whether the person’s attributes or skills are such that they can be expected to perform in a particular role or part of the organisation.
- The blending of these purposes has the risk that neither purpose may be realised as fully as is possible, and certainly creates several procedural issues. A separation of, or at the least a clear delineation between, the security suitability and ‘fit’ aspects of the OSA is required.
- This will facilitate procedural improvements including in the areas of informed consent, provision of feedback, maintaining appropriate privacy and confidentiality, portability of assessments and information sharing more generally. Importantly, it will also facilitate decision-making, validation and research.
- There are three distinct elements of the OSA – a battery of psychometric tests, a follow-up interview with a clinical psychologist and an assessment report. In general, these elements provide for a valid and reliable assessment of the potential security threat posed by an individual. However, both reliability and validity will be improved through the development of more rigorous quality assurance measures identifying explicit linkages between the various psychometric tests used, the factors being assessed, and greater structuring of clinical interviews.

- Where members of the ADF are posted to the Defence intelligence agencies it is important to ensure that the requirements of the OSA are satisfied prior to the issuing of a posting order. In addition to being an important efficiency measure for the department as a whole it is also an important strategy for ensuring that the OSA does not negatively affect the personal circumstances of the military member.
- Emphasis should be given to portability – within the AIC – of security suitability assessments and exchange of information regarding serial applicants.
- Resources should also be directed to a structured research program and validation studies. Also important is the refinement of the benchmarking and measurement strategies, including the collection of statistical data.

# Annex 6

## memorandum of understanding



**Australian Government**  
**Australian Transaction Reports  
and Analysis Centre**

# Memorandum of Understanding

**between**

**the Chief Executive Officer of the Australian Transaction Reports  
and Analysis Centre**

**and**

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

**regarding access to and use of AUSTRAC information or documents  
containing AUSTRAC information**

**August 2007**

## Interpretation

1. For the purposes of this Memorandum of Understanding (MOU) unless the contrary appears

*AML/CTF Act* means the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

*ASIO* means the Australian Security Intelligence Organisation.

*ASIO Act* means the *Australian Security Intelligence Organisation Act 1979*.

*ASIS* means the Australian Secret Intelligence Service.

*AUSTRAC* means the Australian Transaction Reports and Analysis Centre.

*AUSTRAC CEO* means the Chief Executive Officer of AUSTRAC.

*Director-General of Security* means the Director-General of ASIO.

*FTR Act* means the *Financial Transaction Reports Act 1988*.

*IGIS* means the Inspector-General of Intelligence and Security.

*IGIS Official* means an authorised specified official as per section 126(1) of the AML/CTF Act.

*Inspector-General* means Inspector-General of Intelligence and Security.

*IGIS Act* means the *Inspector-General of Intelligence and Security Act 1986*.

*IS Act* means the *Intelligence Services Act 2001*.

## Objective

2. AUSTRAC and the Inspector-General have entered into this MOU to facilitate a cooperative framework by which both parties will work together to effectively perform their respective functions within the terms of the applicable law.
3. This MOU is entered into having regard to:
  - The AML/CTF Act.
  - The IGIS Act.
  - The ASIO Act.
  - The *Attorney-General's Guidelines* in relation to the performance by ASIO of its functions.
  - The IS Act.
  - The Privacy Rules issued under section 15 of the IS Act.

- The FTR Act.
  - The MOU between the AUSTRAC CEO and the Director-General of Security regarding access to and use of AUSTRAC information<sup>1</sup> or documents containing AUSTRAC information.
  - The MOU between the AUSTRAC CEO and the Director-General of the ASIS regarding access to and use of AUSTRAC information or documents containing AUSTRAC information.
4. The agencies do not intend this MOU to create legally binding obligations between them.

## Commencement

5. This MOU comes into effect on the day of signing by the AUSTRAC CEO and the Inspector-General.
6. Upon signing of this MOU, the former MOU titled “Memorandum of Understanding between the Director, Australian Transaction Reports and Analysis Centre and the Inspector-General of Intelligence and Security” which was signed on 7 September 2000 will be revoked.

## Role of the Inspector-General

7. The Inspector-General will monitor compliance by ASIO and ASIS with:
- The AML/CTF Act.
  - The *Attorney-General's Guidelines* in relation to the performance by ASIO of its functions.
  - The IS Act.

---

<sup>1</sup> AUSTRAC information, as defined in the AML/CTF Act means:

- a) eligible collected information; or  
 b) a compilation by the AUSTRAC CEO of eligible collected information; or  
 c) an analysis by the AUSTRAC CEO of eligible collected information.

Eligible collected information, as defined in the AML/CTF Act means:

- a) information obtained by the AUSTRAC CEO under:  
 (i) this Act; or  
 (ii) any other law of the Commonwealth; or  
 (iii) a law of a State or Territory; or  
 (b) information obtained by the AUSTRAC CEO from a government body; or  
 (c) information obtained by an authorised officer under Part 13, 14 or 15;  
 and includes FTR information (within the meaning of the FTR Act).

- The Privacy Rules issued under section 15 of the IS Act.
  - The FTR Act.
  - The MOU between the AUSTRAC CEO and the Director-General of Security regarding access to and use of AUSTRAC information or documents containing AUSTRAC information.
  - The MOU between the AUSTRAC CEO and the Director-General of the ASIS regarding access to and use of AUSTRAC information or documents containing AUSTRAC information.
8. The Inspector-General will review 'Online Usage Statistical Reports', in relation to authorised online access officers from ASIO and ASIS to monitor online access to AUSTRAC information by these agencies.
  9. Where the Director-General of Security or the Director-General of ASIS makes a request in writing to the AUSTRAC CEO for access to information on parameters wider than those available through online access, the AUSTRAC CEO may agree to such a request. The AUSTRAC CEO will notify the Inspector-General of any such wider search requests, for the purposes of carrying out the Inspector-General's duties.
  10. The Inspector-General agrees to provide to the Attorney-General and disseminate to the AUSTRAC CEO, an annual compliance statement in relation to ASIO's compliance with the Attorney-General's Guidelines, the AML/CTF Act, the FTR Act and the MOU between the AUSTRAC CEO and the Director-General of Security regarding access to and use of AUSTRAC information or documents containing AUSTRAC information.
  11. The Inspector-General agrees to provide to the Minister for Foreign Affairs and disseminate to the AUSTRAC CEO, an annual compliance statement in relation to ASIS's compliance with the AML/CTF Act, the FTR Act, the IS Act, ASIS's Privacy Rules and the MOU between the AUSTRAC CEO and the Director-General of ASIS regarding access to and use of AUSTRAC information or documents containing AUSTRAC information.

## Access to AUSTRAC information

12. Access to AUSTRAC information by the Inspector-General or an IGIS official is made in accordance with sub-section 126(1) of the AML/CTF Act whereby the AUSTRAC CEO or a delegate may, in writing, authorise specified officials or a specified class of officials of a specified designated agency to have access to AUSTRAC information for the purposes of performing the agency's functions and exercising the agency's powers.
13. The AUSTRAC CEO or a delegate has signed an "Instrument of Authorisation" detailing the specified officials assisting the Inspector-General (IGIS officials) that have access to AUSTRAC information for the purpose of performing the functions of the Inspector-General and exercising the powers of the Inspector-General.
14. The AUSTRAC CEO will provide the Inspector-General with separate 'Online Statistical Reports' in relation to ASIO authorised online access officers and ASIS authorised online access officers, on a quarterly basis or more often if requested by the Inspector-General. (These Reports give the date and time each search is conducted for each ASIO and ASIS online access officer, the supporting authorisation number entered by the ASIO or ASIS officer, the information entered for search purposes and the type of searches conducted by that officer).
15. The AUSTRAC CEO agrees to provide the Inspector-General with details of alerts placed on the AUSTRAC system by ASIO or ASIS on a quarterly basis or more often if requested by the Inspector-General. This list would include the details of the alert requested, the date this alert was activated and the date these alerts were removed from the AUSTRAC database.
16. The AUSTRAC CEO and the Inspector-General acknowledge that for the purposes of performing the functions of the Inspector-General and exercising the powers of the Inspector-General, IGIS officials will have access to further classes of AUSTRAC information other than the 'Online Statistical Reports' and alert details disseminated to ASIO and ASIS by AUSTRAC. Accordingly the "Instrument of Authorisation" sets out access to all classes of AUSTRAC information.

## **Administrative Arrangements for Receipt of AUSTRAC information**

17. In addition to IGIS officials, all other staff from the Inspector-General's office shall be able to accept delivery of AUSTRAC information delivered by safe-hand to the office, sign for this safe-hand material and log its receipt in the office register.
18. To ensure that all IGIS officials and staff are aware of their obligations, the Inspector-General will brief all IGIS officials and staff on the specific requirements of accepting delivery of AUSTRAC information.

## **Communication of AUSTRAC information**

19. The Inspector-General and IGIS officials may disclose AUSTRAC information for the purposes of, or in connection with, the performance of their duties.
20. The AUSTRAC CEO agrees to provide to the Inspector-General a current list of ASIO and ASIS officials authorised to access AUSTRAC information pursuant to sub-section 126(1) of the AML/CTF Act.

## **Privacy and Security**

21. An IGIS official is bound by the secrecy provisions contained in section 34 of the *IGIS Act*.
22. An IGIS official cannot disclose AUSTRAC information except where they are permitted to do so in accordance with sections of the AML/CTF Act.
23. An IGIS official accessing AUSTRAC information must ensure that the information is protected by such security safeguards as is reasonable in the circumstances, against:
  - a) loss, unauthorised access, unauthorised use or unauthorised disclosure; and
  - b) modification or other misuse.

## **Training and Support**

24. The AUSTRAC CEO and the Inspector-General will, to the extent that they can reasonably do so, assist each other in carrying out their respective tasks under this MOU.

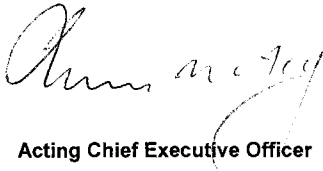
25. The AUSTRAC CEO agrees to provide training and support to the Inspector-General and IGIS officials to assist them to understand the AUSTRAC database and the ways in which they might monitor access by ASIO and ASIS and the use of AUSTRAC information as described in this MOU.

## Variation

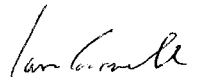
26. Any variation to this MOU will require the issue of a new MOU signed by the AUSTRAC CEO and the Inspector-General.

## Termination

27. This MOU will remain operative until replaced by a new MOU on the same subject matter or terminated. Either the AUSTRAC CEO or the Inspector-General may terminate the MOU at any time by written notice.



**Acting Chief Executive Officer**  
Australian Transaction Reports  
and Analysis Centre



**Inspector-General of  
Intelligence and Security**

Date *29 August, 2007*

Date *29 August 2007*

# Annex 7

## Attorney-General's guidelines to ASIO

### **Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)**

#### **1 Authority for Guidelines**

1.1 These guidelines are given by the Attorney-General to the Director-General of Security (the Director-General) under subsections 8A(1) and 8A(2) of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) and are to be observed by ASIO in the performance of its functions relating to:

- (a) the obtaining, correlating, evaluating and communicating of intelligence relevant to security; and
- (b) politically motivated violence.

#### **2 ASIO's functions**

2.1 ASIO's functions are specified in the ASIO Act (section 17). These are:

- (a) to obtain, correlate and evaluate intelligence relevant to security;
- (b) for purposes relevant to security and not otherwise, to communicate any such intelligence to such persons, and in such manner, as are appropriate to those purposes;
- (c) 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;
  - (ca) to furnish security assessments to a State or an authority of a State in accordance with paragraph 40(1)(b);

- (d) to advise Ministers, authorities of the Commonwealth and such other persons as the Minister, by notice in writing given to the Director-General, determines on matters relating to protective security; and
- (e) to obtain within Australia foreign intelligence pursuant to section 27A or 27B of the ASIO Act or section 11A, 11B or 11C of the *Telecommunications (Interception and Access) Act 1979*, and to communicate any such intelligence in accordance with the ASIO Act or the *Telecommunications (Interception and Access) Act 1979*.

2.2 "Security" is defined as:

- (a) The protection of, and of the people of, the Commonwealth and the several States and Territories from:
  - (i) espionage;
  - (ii) sabotage;
  - (iii) politically motivated violence;
  - (iv) promotion of communal violence;
  - (v) attacks on Australia's defence system; or
  - (vi) acts of foreign interference; whether directed from, or committed within, Australia or not; and
- (b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter

mentioned in any of the subparagraphs of paragraph (a).

2.3 Other important statutory provisions include section 17A and section 20 of the ASIO Act:

*Section 17A:*

This Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent, and the exercise of that right shall not by itself, be regarded as prejudicial to security, and the functions of the Organisation shall be construed accordingly.

*Section 20:*

The Director-General shall take all reasonable steps to ensure that:

- (a) the work of the Organisation is limited to what is necessary for the purposes of the discharge of its functions; and
- (b) the Organisation is kept free from any influences or considerations not relevant to its functions and nothing is done that might lend colour to any suggestion that it is concerned to further or protect the interests of any particular section of the community, or with any matters other than the discharge of its functions.

### 3 Governing Principles

3.1 ASIO works to provide timely advice on threats to the security of Australia, the Australian people, and Australian interests, whether in or outside Australia.

3.2 ASIO's security functions are concerned with protection and are anticipatory in nature. ASIO therefore investigates known threats to security, and endeavours to identify persons, groups or entities that may present a risk to security that previously have not been identified.

3.3 ASIO implements measures or arrangements, as far as is reasonably possible, to ensure that the information it relies upon is reliable and accurate.

### 4 Interpretation

4.1 In these guidelines:

- (a) "activities relevant to security" means not only physical acts of the sort specified in the definition of security, but also includes the acts of conspiring, planning, organising, counselling, advising, financing, or otherwise advocating or encouraging the doing of those things;

- (b) "activities prejudicial to security" means activities that are relevant to security and which can reasonably be considered capable of causing damage or harm to Australia, the Australian people, or Australian interests, or to foreign countries to which Australia has responsibilities;
- (c) "subject" means a person, group or other entity;
- (d) "inquiry" means action taken to obtain information:
  - (i) for the purpose of identifying a subject and/ or determining whether the activities of a subject could be relevant to security; or
  - (ii) as part of an investigation; and
- (e) "investigation" means a concerted series of inquiries in relation to a subject where it has been determined that the activities of the subject could be relevant to security.

## 5 Security Assessments

5.1 The furnishing by ASIO of security assessments to Commonwealth agencies is governed by Part IV of the ASIO Act. Where it is necessary to conduct an investigation to obtain new information relevant to a security assessment, such an investigation shall be conducted in accordance with these guidelines.

## 6 Obtaining Intelligence Relevant to Security

6.1 ASIO's functions require it:

- (a) to undertake inquiries to determine whether a particular subject or activity is relevant to security;
- (b) to investigate subjects and activities relevant to security;
- (c) to develop and maintain a broad understanding of the security environment; and
- (d) to analyse and assess information obtained, and to provide intelligence and advice to relevant authorities.

6.2 In performing its functions ASIO may:

- (a) collect, maintain, analyse and assess information related to inquiries and investigations;
- (b) collect and maintain a comprehensive body of reference material to contextualise intelligence derived from inquiries and investigations; and

(c) maintain a broad database, based on the above, against which information obtained in relation to a specific inquiry or investigation can be checked and assessed.

6.3 The Director-General is responsible for deciding ASIO's intelligence collection, analysis and assessment priorities (subject to section 8 of the ASIO Act).

## 7 Investigations

7.1 The Director-General is responsible for determining ASIO's subjects for investigation (subject to section 8 of the ASIO Act).

7.2 ASIO is not required to investigate every instance of activities relevant to security. Decisions to initiate investigations shall be based on a consideration of the extent to which the activities of a subject will, or are likely to, cause harm or damage, ASIO's overall priorities, and the availability of appropriate resources.

## 8 Authorisation of Inquiries and Investigations

8.1 Subject to paragraph 10.4(c), the initiation and continuation of investigations shall be authorised only by the Director-General, or an officer at or above Executive Level 2 authorised by the Director-General for that purpose.

8.2 The Director-General will establish processes to ensure that all requests for information from external agencies are authorised at an appropriate level.

## 9 Bases for Investigations

9.1 In deciding whether to conduct an investigation, and the investigative methods to be used, ASIO shall consider:

- (a) what is already known about the subject's activities, associations and beliefs, and the extent to which those activities, associations and beliefs are, or are likely to be, relevant or prejudicial to security;
- (b) the immediacy and severity of the threat to security;
- (c) the reliability of the sources of the relevant information; and

(d) subject to paragraph 10.4, the investigative techniques that are likely to be most effective.

## 10 Conduct of Inquiries and Investigations

10.1 Information obtained by ASIO is "relevant to security" where it may assist in determining whether:

- (a) there is a connection or possible connection between a subject and activities relevant to security, irrespective of when such activities have occurred or may occur;
- (b) the activities of a subject are not relevant to security; or
- (c) a person, group or entity other than the subject has a connection or possible connection to activities relevant to security.

10.2 The purpose of an ASIO inquiry or investigation should generally be to obtain information concerning the nature of any activities of a person or group which may be relevant to security, including their intentions and capabilities.

10.3 Information collected may include:

- (a) the identity and relevant activities of individuals and groups of interest, including persons associated with the group of interest and of other persons likely to be knowingly concerned in furtherance of its plans or activities; and
- (b) the finances, the geographic dimensions, and the past, present and prospective activities of the individuals or groups.

10.4 Information is to be obtained by ASIO in a lawful, timely and efficient way, and in accordance with the following:

- (a) any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence;
- (b) inquiries and investigations into individuals and groups should be undertaken:
  - (i) using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions; and
  - (ii) with due regard for the cultural values, mores and sensitivities of individuals of particular cultural or racial backgrounds, consistent with the national interest;

- (c) the more intrusive the investigative technique, the higher the level of officer that should be required to approve its use;
- (d) wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques; and
- (e) where a threat is assessed as likely to develop quickly, a greater degree of intrusion may be justified.

## 11 Review of Investigations

11.1 Investigations are to be reviewed no less than annually.

11.2 Where an inquiry or investigation concludes that a subject's activities are not, or are no longer, relevant to security, the records of that inquiry or investigation shall be destroyed under disposal schedules agreed to between ASIO and the National Archives of Australia.

## 12 Advice to the Attorney-General

12.1 The Director-General shall keep the Attorney-General advised, in general terms, of ASIO's investigations and priorities through:

- (a) regular briefings to the Attorney-General on ASIO's investigations, significant developments in relation to important subjects, and the emergence of new subjects; and
- (b) other means as necessary.

Note 1: Under the ASIO Act, and the *Telecommunications (Interception and Access) Act 1979* (the T(I&A) Act), all ASIO warrants (other than questioning warrants issued under Part III, Division 3 of the ASIO Act) are issued by the Attorney-General, and ASIO is required to report to the Attorney-General on the extent to which the action taken under every warrant has assisted the Organisation in carrying out its functions (section 34 of the ASIO Act and section 17 of the T(I&A) Act).

Note 2: Section 21 of the ASIO Act requires the Director-General to consult regularly with the Leader of the Opposition in the House of Representatives for the purpose of keeping him or her informed on matters relating to security.

## 13 Treatment of Personal Information

13.1 ASIO shall only collect, use, handle or disclose personal information for purposes connected with its statutory functions.

13.2 The Director-General shall take all reasonable steps to ensure that personal information shall not be collected, used, handled or disclosed by ASIO unless that collection, use, handling or disclosure is reasonably necessary for the performance of its statutory functions (or as otherwise authorised, or required, by law).

13.3 The Director-General shall ensure that all reasonable steps are taken to ensure that personal information held, used or disclosed by ASIO is accurate and not misleading.

13.4 Appropriate records shall be kept of all requests made by ASIO for access to personal information and all personal information received in response to such requests. Such records shall be open to inspection by the Inspector-General of Intelligence and Security.

13.5 Appropriate records shall be kept of all communication by ASIO of personal information for purposes relevant to security or as otherwise authorised. Such records shall be open to inspection by the Inspector-General of Intelligence and Security.

13.6 The Director-General shall ensure that all personal information collected or held by ASIO is protected by reasonable security measures against loss and unauthorised access, use or modification.

## 14 Politically Motivated Violence (PMV) – legislative definitions

14.1 Key legislative provisions relating to PMV are:

- (a) the definition of "politically motivated violence" in section 4 of the ASIO Act; and
- (b) section 17A which provides that the ASIO Act is not concerned with lawful advocacy, protest, or dissent (paragraph 2.3 above).

14.2 "Politically motivated violence" means:

- (a) acts or threats of violence or unlawful harm that are intended or likely to achieve a political objective, whether in Australia or elsewhere, including acts or threats carried on for the purpose of influencing the policy or acts of a government, whether in Australia or elsewhere; or

- (b) acts that:
  - (i) involve violence or are intended or are likely to involve or lead to violence (whether by the persons who carry on those acts or by other persons); and
  - (ii) are directed to overthrowing or destroying, or assisting in the overthrow or destruction of, the government or the constitutional system of government of the Commonwealth or of a State or Territory; or
- (ba) acts that are terrorism offences; or
- (c) acts that are offences punishable under the *Crimes (Foreign Incursions and Recruitment) Act 1978*, the *Crimes (Hostages) Act 1989* or Division 1 of Part 2, or Part 3, of the *Crimes (Ships and Fixed Platforms) Act 1992* or under Division 1 or 4 of Part 2 of the *Crimes (Aviation) Act 1991*; or
- (d) acts that:
  - (i) are offences punishable under the *Crimes (Internationally Protected Persons) Act 1976*; or
  - (ii) threaten or endanger any person or class of persons specified by the Minister for the purposes of this subparagraph by notice in writing given to the Director-General.

## 15 Interpreting PMV

### Sub-paragraph (a) of the definition of PMV

15.1 The activity comprehended by sub-paragraph (a) of the definition of PMV includes terrorism, and violent protest that has a political objective. In performing its functions in relation to sub-paragraph (a) of the definition of PMV, ASIO should give priority to persons or groups likely to be involved in:

- (a) acts or threats of serious violence or unlawful harm designed to create fear or to incite or provoke violent reaction; or
- (b) the use of tactics that can reasonably be assessed as likely to result in violence;
  - in order to achieve a political objective.

15.2 The above considerations apply whether the object of the violence or threat is the government of the Commonwealth, a State or Territory, or the government of a foreign country with which Australia has responsibilities in relation to security matters, or the people of Australia or Australian interests within Australia and overseas. Where acts or threats occur within a State or Territory and appear wholly designed to influence the policy or acts of the State or Territory government, ASIO is to inform the Attorney-General of any decision taken to investigate such acts or threats.

### Sub-paragraph (b) of the definition of PMV

15.3 In performing its functions in relation to sub-paragraph (b) of the definition of PMV, ASIO is to investigate whether a person or a group actively holds to, advocates or encourages a doctrine, or pursues political objectives in which advocacy of the use of violence is accepted for the purpose of overthrowing, destroying or assisting in the overthrow or destruction of a government or the constitutional system of government of the Commonwealth, or a State or Territory.

15.4 Whether it is probable that the activity will succeed in its purpose, and whether the intent is for imminent or future activity are matters which ASIO should take into account in setting its priorities. However, these considerations of probability of success or imminence of violence are not factors which of themselves determine whether the act is PMV.

15.5 A person or group need not intend to initiate violence in the process of overthrowing constitutional government for their activities to be assessed as PMV under sub-paragraph (b). It is sufficient if the activities could lead to violence. All that is required is there is a reasonable likelihood that the activity will produce violence from others.

15.6 Advocacy of violence may come within sub-paragraph (b) of the definition of PMV even though it is not itself unlawful, or the advocacy is not public. Of their very nature, preparations directed at the overthrow of government are likely to be clandestine and their early manifestations are deceptive.

15.7 If apparently non-violent activities directed at destabilising or undermining constitutional government are associated with what purports to be no more than contemplation of the prospect of the violent overthrow of government, ASIO may investigate those activities to the extent necessary to establish (with some confidence) whether the activities involve a real risk or danger that violence will flow from those activities.

### **Sub-paragraphs (ba) and (c) of the definition of PMV**

15.8 These sub-paragraphs refer to activities that are criminal offences. Any activity which constitutes a criminal offence under the legislation specified is an act of PMV.

### **Sub-paragraph (d) of the definition of PMV**

15.9 Sub-paragraph (d) of the definition of PMV refers to attacks on the persons, official premises and private accommodation of certain defined persons and provides for the Attorney-General to add to those defined persons by notice in writing to the Director-General.

15.10 The categories of persons defined by sub-paragraph (d) of the definition of PMV include internationally protected persons as defined by the *Crimes (Internationally Protected Persons) Act 1976*. Any activity which constitutes a criminal offence under this legislation is an act of PMV.

15.11 Sub-paragraph (d) also provides for the Attorney-General to add other defined persons by notice in writing to the Director-General. That latter category will vary from time to time, but could include:

- (a) Ministers of the Commonwealth Government;
- (b) the Leader of the Opposition in the Commonwealth Parliament;
- (c) Members of the Commonwealth Parliament when travelling as a Parliamentary delegation; and
- (d) the Premiers or Chief Ministers of the States and Territories.

15.12 Investigations into activities that might threaten persons in the categories identified in sub-paragraph (d) of the definition of PMV may require a higher degree of intrusion into the privacy of persons suspected of involvement than would normally be appropriate when based only on information of low reliability. The period of such intrusion should be limited so far as practicable to the period of possible threat.

## **16 Investigations into Demonstrations and other forms of Protest**

16.1 Further to clause 7 above, the following guidance relates specifically to ASIO's investigation of demonstrations and other forms of protest.

16.2 ASIO is not to undertake investigations where the only basis for the investigation is the exercise of a person's right of lawful advocacy, protest or dissent (section 17A of the ASIO Act).

16.3 ASIO is not to investigate demonstrations or other protest activity unless:

- (a) there is a risk of pre-meditated use of violence against persons or property for the purposes of achieving a political objective, or pre-meditated use of tactics that can be reasonably assessed as likely to result in violence; or
- (b) it suspects there is a link between the demonstration or other protest activity and conduct coming otherwise within the definition of security.

16.4 An exception to the above is demonstrations or other protest activity against internationally protected persons or other persons specified by the Attorney-General under sub-paragraph (d) of the definition of PMV.

16.5 Minor acts of violence, such as jostling or defacing or damaging property, are properly matters for investigation by a police force, as are incidental acts of violence or property damage which occur in the course of a demonstration. Where, however, such acts are or are intended to be part of a pattern, and where there is reason to believe that the acts are intended to influence the policy or acts of a government, ASIO may investigate to determine whether there is a potential for the violence to escalate or become more strongly directed at a person or group associated with the policy or acts at issue.

## **17 Assessment of PMV**

17.1 ASIO's threat assessment function is an integral part of national arrangements for the protection of high office holders, internationally protected persons, sites of national significance and critical infrastructure. ASIO may prepare threat assessments in relation to any demonstration or protest activity on the basis of information it already has or which is passed to it by other agencies, for the purpose of advising authorities responsible for law enforcement and the protection of designated persons.

17.2 ASIO is not required to provide an assessment for every event, place, person or instance, that is actually or potentially at threat from PMV. The Director-General shall consider the potential seriousness of any matter or information, the Organisation's priorities, and the availability of appropriate resources.

# index

## A

- Administrative Appeals Tribunal (AAT)
  - appeals against ASIO assessments, 10
- Administrative Review Council (ARC), 28
- Advertising, 74
- Afghanistan, 12, 55
- Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), 43
  - AML/CTF Amendment Act 2007*, 43
- Archives Act 1983*, 46, 67
- Asia-Pacific Economic Cooperation (APEC)
  - Leaders meeting, 13, 37, 43
- ASIO Legislation Amendment (Terrorism) Act 2003*, 42
- Attorney-General
  - ASIO, executive responsibility for, 11
  - replacement, 11
- Auditor-General
  - responsibility for, 9
- Australian Defence Force (ADF)
  - overseas deployments, 12
- Australian Intelligence Community (AIC) agencies
  - acceptance of recommendations, 33
  - agencies comprising, 10
  - change of responsibility for, 11
  - complaints about, 8, 13, 15, 31, 34
  - growth of, 13
  - increased activity, 8
  - presentations at courses, 9
  - psychological assessments, 21
  - responsiveness to issues raised, 33
  - review of activities, 10
  - sharing information with, 13
- Australian National Audit Office (ANAO)
  - report from, 9
- Australian Secret Intelligence Service (ASIS), 49–53
  - AIC, part of, 10
  - assumed identities, 53
  - AUSTRAC data, access to, 50
  - complaints, 53
  - exclusions from new selection arrangements, 12
  - Foreign Affairs Minister's executive responsibility for, 11
  - growth of, 49–50
  - inspection program, 9
  - meetings, 53
  - Ministerial submissions, 51
  - new Minister, 49
  - operational file review activities, 52
  - privacy rules, 52–3
  - proposed inspections for the year ahead, 67
  - review of Ministerial authorisations, 51
  - role of, 49
  - special briefings, 50
  - training, 50
  - visits and contact with staff, 50
  - weapons related authorisations, 51–2
- Australian Security Intelligence Organisation (ASIO)
  - 35–48
  - AIC, part of, 10
  - allegations about, 8
  - approvals to investigate, 42–3
  - archives related complaints, 46
  - assumed identities, use of, 44
  - Attorney-General's executive responsibility, 11
  - Attorney-General's guidelines, 35–6, 117–23
  - AUSTRAC, information obtained from, 43–4
  - community interactions, 45–6
  - complaints regarding, 8, 31, 37, 45–8
  - exclusions from new selection arrangements, 12
  - foreign liaisons, information exchange, 44–5
  - former employees, concerns of, 46–7
  - growth of, 13, 37–8

- immigration related complaints, 47–8
- inspection, 9, 39–48
- interception management systems, 41
- interoperability issues, 43
- links to law enforcement agencies, 43
- litigation and review workload, 37–8
- meetings, 38
- own motion inquiry, 8, 30
- politicians, retention of information regarding, 39
- proposed inspections for the year ahead, 66–7
- questioning and detention warrants, 42
- RCIS papers, release of, 46
- recruitment complaints, 46
- reports of warrant activity, 41
- role of, 35
- security assessment for visas, 8
- security equipment assessment, 47
- taxation information, access to, 44
- telecommunications interception, unauthorised, 41
- training, 38
- Ul-Haquee, Mr Izhar, inquiry regarding, 8, 23, 36–7, 43, 45
- warrant operations, 39–41
- Australian Security Intelligence Organisation Act 1979* (Asio Act), 35
  - Part III, Division 3, 42
  - section 8A, 35
  - section 17(1), 44
  - section 34E, 42
  - section 34G, 42
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
  - ASIS's access to data, 50
  - information obtained by ASIO, 43–4
  - inspection, 9, 51–3
  - memorandum of understanding, 110–16

## B

- 'Balibo Five', 21
- Blick, Mr Bill, 21–2, 52
- Brady, Mr Martin, 43

## C

- Cabinet Secretary
  - administrative responsibility, 9
    - transferred to, 11
  - new selection arrangements, 12
- Clarke, John, QC, 23, 38
- Client legal privilege

- ALRC review of, 28
- Commissioner of Taxation, 44
- Community outreach, 9, 18–19
- Complaints
  - administrative processing, 16
  - AIC agencies, about, 15, 31
  - inquiries triggered by, 8
  - nature of, 32
  - outcome of investigations, 29
  - receipt of, 15
  - statistics, 102
- Consultancy services, 104
- Corporate governance, 70–1
  - business continuity plan, 71
  - corporate and operational planning, 71
  - disaster recovery plan, 71
  - external scrutiny, 71
  - fraud control, 71
  - internal audit, 70
  - organisation structure, 70
  - risk management, 70–1
  - support from PMC and DSD, 71

- Crimes Act 1900* (NSW)

- section 86, 36

- Crimes Act 1914*, 44

- section 15XUA, 44, 53

- CrimTrac, 29

## D

- Defence Imagery and Geospatial Organisation (DIGO), 59–62
  - AIC, part of, 10
  - complaints, 61
  - Defence Minister's executive responsibility for, 11
  - Director DIGO authorisations, 60
  - inspection, 9, 60–1
  - meetings, 61
  - Ministerial authorisations, 60
  - Ministerial directions, 59
  - new Minister, 59
  - own motion inquiry, 30
  - privacy rules, 59, 61
  - proposed inspections for the year ahead, 68
  - role, 59
  - training, 61
  - visits, 61
- Defence Intelligence Organisation (DIO), 63–4
  - AIC, part of, 10
  - analytic integrity, 20, 62–3, 107

- complaints, 63
- Defence Minister's executive responsibility for, 11
- inspection program, 9
- own motion inquiry, 8, 30, 63
- privacy guidelines, 63
- proposed inspections for the year ahead, 68
- role, 62
- training, 63

Defence Minister

- executive responsibilities
  - DIGO, 11
  - DIO, 11
  - DSD, 11
- replacement, 11

Defence Signals Directorate (DSD), 54–8

- AIC, part of, 10
- collection activities, 57
- complaints, 58
- compliance oversight of ADF signals intelligence activities, 55
- counter-terrorism support, 56
- Defence Minister's executive responsibility for, 11
- inspection, 9, 56–7
- meetings, 57
- Ministerial authorisations, 56
- Ministerial directions, 54–5
- new Minister, 54
- own motion inquiry, 31, 58
- Peters, Mr Brian, coronial inquiry, 56
- privacy rules, 55, 57
- proposed inspections for the year ahead, 67–8
- role, 54
- site visits, 57
- spot-checking of databases, 56–7
- support to military, 55
- training, 57

Department of Immigration and Citizenship (DIAC), 37

Department of the Prime Minister and Cabinet (PMC)

- new secretary, 14

Director-General of Security, 38, 39, 46

Disability strategy, 74

## E

East Timor, 21–2

Environmental performance, 74

*Evidence Act 1995*

- section 84, 36
- section 85, 36
- section 138, 36

## F

Faulkner, Senator John. *See* Cabinet Secretary

Federal election, 11

Financial management, 74–5

- consultancy services, 74
- contract services, 74
- legal services, 75
- purchasing, 74

Flood, Mr Philip, 15, 20

Foreign Affairs Minister

- ASIS, executive responsibility for, replacement, 11

Foreign visits, 19

Freedom of information, 74

*Freedom of Information Act 1982*, 74

## G

Georgiou, Mr Petro, 27

## H

Habib, Mamdouh, 24

Haneef, Dr Mohamed, 23, 24, 38

Hicks, David, 24

Homeland and border security review, 28

Human resources, 72–3

- background, 72
- organisation profile, 72–3
- performance management and pay, 73
- personnel guidelines, 73
- training and development, 73
- workplace agreements, 73

*Human Rights and Equal Opportunity Commission Act 1986*, 28

Humphries, Senator Gary, 27

*Independent Reviewer of Terrorism Laws Bill 2008*, 27 (No. 2), 27

## I

Inquiry activities, 10, 15–17

- commenced in 2007–08, 31
- full inquiries, 16–17
- preliminary inquiries, 16

Inspection activities, 15

- program, 17–18
- role, 10

Inspector-General of Intelligence and Security (IGIS)

- acting, 14
- activities, 15–19

- community outreach activities, 9, 18–19
- complaints and inquiries, 15
- corporate activities, 18–19, 69
- functions, 10
- growth of office, 13
- independent statutory office, 10
- inquiry activities, 10, 15–17
- inspection role, 10, 17–18
- new selection arrangements, 12
- outcomes, 30
- presentations at seminars and courses, 9
- Prime Minister’s administrative responsibility, 10, 11
  - transfer of, 11
- recruitment, 9, 12
- relationships with agencies, 9
- role of, 10
- staffing and recruitment, 68
- training, 19
- valedictions, 14
- website, 18

*Inspector-General of Intelligence and Security Act 1986*  
(IGIS Act)

- Division 3, 16
- established by, 10
- possible amendments, 27
- section 8, 10, 15
- section 8(3)(a)(iii), 20, 62
- section 8(3)(c), 20, 63
- section 8(5), 46
- section 8(7), 46
- section 9, 10
- section 9A, 10, 20
- section 11, 15
- section 14, 16
- section 32B, 51
- section 35(2), 20

*Intelligence Services Act 2001* (ISA), 25, 47, 49, 54, 68

- section 6, 49
- section 6B, 59
- section 8, 54
- section 8(1), 51, 55, 59
- section 9(1A), 60
- section 15(1), 52, 55, 59
- Schedule 2, clause 1(5), 51
- Schedule 2, clause 3, 52

- International cooperation, 19
- International Intelligence Review Agencies (IIRA)
  - conference, 19
- Iraq, 12, 55

## K

- Keely, Mr Mick, 43
- Kelly, Ms Robyn, 14
- Key intelligence and security interests, 12–13

## L

- Labor Government
  - continuing the growth of ASIO and other agencies, 13
  - portfolio arrangements, 9, 11
  - sworn in, 11
- Legislative developments, 26–8

## M

- McCrimmon, Professor Les, 27
- McMillan, Professor John
  - acting IGIS, 14
- Memorandums of Understanding (MOUs), 43
- Moran, Mr Terry, 14
- Moroney, Mr Ken, 43

## N

- National Archives of Australia (NAA), 46
- National Security Committee, 11, 49
- National Security Hotline (NSH), 32
- New selection arrangements, 12
- New South Wales Law Enforcement and National Security (Assumed Identities) Act 1998*, 44
- New Zealand, 19

## O

- Occupational health and safety, 73
- Office of National Assessments (ONA), 64–5
  - AIC, part of, 10
  - complaints, 65
  - inspection program, 9
  - new selection arrangements, 12
  - own motion inquiry, 8, 30
  - Prime Minister’s administrative responsibility, 11
  - privacy guidelines, 65
  - proposed inspections for the year ahead, 68
  - report, 105–6
  - role, 64
  - statutory independence, review of, 20, 64–5
  - training, 65
- Office of National Assessments Act 1977*, 64
- Office of the Inspector-General of Intelligence and Security (OIGIS). **See** Inspector-General of Intelligence and Security (IGIS)

Olympic torch relay, 13, 37  
Ombudsman, Commonwealth, 28, 47  
    responsibility for, 9  
*Ombudsman Act 1976*, 28  
Organisational Suitability Assessment (OSA)  
    inquiry into, 8, 20–1, 108–09

## **P**

Parkin, Scott, 24  
Parliamentary accountability, 25  
Parliamentary Joint Committee on Intelligence and Security (PJCS), 25  
Parliamentary Oversight, 25  
Performance, 30–4  
    indicators, 30  
Peters, Mr Brian, 21–2, 56  
Pinch, Magistrate Dorelle, 21–2  
Prime Minister  
    IGIS's relationship with, 10, 12  
    OIGIS, administrative responsibility, 11  
    ONA, administrative responsibility, 11  
*Privacy Act 1988*, 28  
    ALRC review of, 27  
Protective Security Manual (PSM)  
    review of, 29  
Protective Security Policy Committee (PSPC), 29  
*Public Service Act 1999*, 47  
Public Service Commissioner, 29  
    oversight of recruitment process, 12

## **R**

Recommendations, acceptance of, 33  
Royal Commission on Australia's Security and Intelligence Agencies, 16  
Royal Commission on Intelligence and Security (RCIS), 46

## **S**

Security assessments  
    complaints about, 8, 16  
Security Equipment Catalogue (SEC), 47  
Security Legislation Review Committee (SLRC), 27  
Senate Finance and Public Administration Committee, 25  
Sheller, Simon, AO QC, 27  
Shergold, Dr Peter, 14  
Significant issues, 19–23  
Smith, Mr Ric, 28

South Africa, 19  
Street, Sir Laurence, 43  
Street Review, The, 43

## **T**

*Taxation Administration Act 1953*  
    section 3EA, 44  
*Telecommunications (Interception) Act 2007*, 26  
*Telecommunications (Interception and Access) Act 1979*, 26, 41  
*Telecommunications (Interception and Access) Amendment Act*  
    2007 Act, 26  
    2008 Act, 26  
Thomas, Jack, 24  
Timeliness, 32–3  
Troeth, Senator Judith, 27

## **U**

Ul-Haque, Izhar, 8, 23–4, 36–7, 43, 45

## **W**

Workplace Research Associates, 21  
World Youth Day, 13, 37, 43

