

ANNUAL REPORT 2006-2007



Inspector-General of
Intelligence and Security

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

Internet Address

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

© Commonwealth of Australia 2007

ISBN 978-0-9756755-3-3

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 PIRION Pty Limited



INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

2007/577

File Ref: 2007/08

The Hon John Howard MP
Prime Minister
Parliament House
CANBERRA ACT 2600

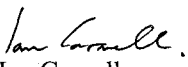
Dear Prime Minister

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 2006 and 30 June 2007.

The report has been prepared in compliance with the *Requirements for Annual Reports*, issued by the Department of the Prime Minister and Cabinet in June 2007.

Each of the agencies within my jurisdiction has confirmed that the components of the report which relate to them will not prejudice the security or defence of Australia, or Australia's relations with other countries. Care has also been taken to protect 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

5 October 2007

Table of contents

Letter of transmittal	3
Glossary of acronyms	5
Key points	6
Role of the Inspector-General	8
Reflections on first term	9
The year in review	13
Parliament and legislation	27
Performance	33
Australian Security Intelligence Organisation	38
Australian Secret Intelligence Service	52
Defence Signals Directorate	59
Defence Imagery and Geospatial Organisation	64
Defence Intelligence Organisation	67
Office of National Assessments	69
The year 2007–08 in prospect	71
Corporate and communication	75
Financial statements	81
Annex 1 – Complaint and inquiry statistics	103
Annex 2 – Consultancy services let during 2006–07	105
Annex 3 – IGIS inquiry into ASIO’s assessment of Mr Rhuheh Ahmed	106
Annex 4 – Statement of procedures – warrants issued under Division 3 of Part III, ASIO Act	109
Annex 5 – IGIS submission to ALRC on legal professional privilege	119
Annex 6 – Report on the statutory independence of ONA – Executive Summary	123
Index	125

Glossary of acronyms used in this report

AAT	Administrative Appeals Tribunal
ACLEI	Australian Commission for Law Enforcement Integrity
ADF	Australian Defence Force
AIC	Australian Intelligence Community
AML/CTF Act	<i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i>
ANAO	Australian National Audit Office
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
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
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
TIA Act	<i>Telecommunications (Interception and Access) Act 1979</i>

Key points

- The office (OIGIS) celebrated its 20th anniversary on 1 February 2007—having conducted 433 formal inquiries as well as extensive inspection activity over those 20 years. The 2004 Flood review had noted that the office performs an important function in the system of accountability of the Australian Intelligence Community (AIC) agencies.
- Proactive inspections of agency records and activities continued to be the major part of the office's workload in 2006–07. The continuing growth of the AIC agencies increased demands in this regard, but I am pleased to say the office met the challenge and extended the program in suitable ways.
- No deficiencies were identified in the course of inspecting agency approaches to significant (and for some controversial) new powers and capabilities which have been introduced in recent years. These included Australian Security Intelligence Organisation (ASIO) questioning warrants and B-party telecommunication interception warrants, and Australian Secret Intelligence Service (ASIS) carriage of weapons for self-defence.
- Presentations at agency seminars and training courses and at common AIC courses saw OIGIS address at least 1,100 staff in the six agencies in 2006–07. Key themes included the importance of the rule of law and having the trust and confidence of the community, the role of this office and the accountability framework generally, and key requirements in relevant legislation. Targeted community outreach was also undertaken and a brochure on how to make a complaint to the office was translated into another 12 languages (making a total of 16 in all).
- The number of formal inquiries triggered by complaints to the office in 2006–07 was 10. This compares to 18 in 2005–06.
- However, there was an increase in the number of complaints concerning delays by ASIO in producing security assessments for immigration purposes. ASIO has some initiatives underway and others planned, and it is important that these be successful in dealing with the challenge which an increasing workload has posed.
- The office completed its first inspection work in relation to the independence and propriety of the assessment work of Office of National Assessments (ONA). Generally analysts did not believe there were attempts to improperly direct or influence assessments, and some processes have been introduced to enhance the integrity of the assessment work. The possibility of “self-censorship” on certain topics was explored—in some instances examination showed that this was not the case, while in others it was inconclusive. With the benefit of this exploration and conscious that the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) specifically refers to formal inquiries being conducted periodically, a formal inquiry was commenced in 2007.

- One inquiry completed in 2006–07 concerned allegations that an ASIO security assessment which resulted in the denial of a visa to Mr Rhuheh Ahmed (one of the UK “Tipton Three” and a subject of the film *“The Road to Guantanamo”*) was politically or otherwise improperly influenced. Upon investigation I found no evidence or indication to support the allegation and concluded that ASIO had acted legally and properly.
- The office increased from a total of seven to 10 people over 2006–07, and we moved to new accommodation which provides necessary additional space and better facilities. I was re-appointed as IGIS for a further four years.
- In summary, none of OIGIS activities in 2006–07 revealed enduring systemic deficiencies that would lead to breaches of the law, propriety, or human rights. I was satisfied that the agencies were committed to acting legally and with propriety and respect for human rights, and that apart from a very small number of genuine errors, had complied with their obligations.

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 IGIS Act and commenced operating on 1 February 1987.

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 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 of the IGIS Act 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 frequently 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 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.

Reflections on first term

OIGIS had been in existence for 17 years when I started and my predecessors had put in place a solid base. Notable in this regard was the mature relationship which had developed over time with the agencies with which it had had regular contact. These agencies had to come to understand the importance of being accountable and OIGIS was conscious that a nuanced relationship—rather than a blunt adversarial one—would best achieve the purposes of the legislation.

My view of the approach the office takes can be summarised as fair, constructive but firm when necessary.

A second valuable element I inherited was an emphasis on the inspection program. This program involves regularly attending agencies, scrutinising key records and activities, and discussing issues with staff. It is an important means of preventing or forestalling issues or problems before they become major ones, and the normative effect is significant.

But the last three years has not been a story of simple continuity. Substantial change in the security environment has also changed the AIC and hence demanded more of OIGIS.

Agency growth

One of the most obvious changes is the growth in the size of the AIC agencies. Some are doubling in size and this flows through to increases in operational activity. This in turn means an increase in inspection and related activities for OIGIS, and hence my staff has grown from four when I arrived in March 2004 to nine as at 30 June 2007.

The office has also had a tradition of seeking additional resources and/or expertise when there

has been specific need and these have been readily provided by Government or agencies. I have used the former IGIS, Mr Bill Blick PSM AM, as a consultant from time to time and have also accessed other expertise when necessary (from outside the agencies I review).

Whether the approved growth of OIGIS proves to be sufficient can only be judged in light of workload trends as they unfold. In part this depends on how well the agencies select, train and guide new staff and the effectiveness of their internal mechanisms to ensure legality, quality, compliance and effective risk assessment and management. With this in mind I have taken, and will continue to take, a keen interest in these processes.

Additionally, in an endeavour to assist the right culture being present, I and my office have sought out and taken a range of opportunities to address staff in the agencies about their obligations and expectations of them. This has spanned new starters, experienced staff and managers. In the last three years we have addressed around 2,500 staff in total in about 110 sessions. Combined with our inspection program I am confident that OIGIS is well known within the AIC and that key messages about legality and propriety have been discussed with agency staff.

Protecting the rule of law and having the trust and confidence of the community have been stressed as essential overarching requirements. Particular points flowing from the legislation which are discussed with agency staff are that the agencies must:

- act only within the scope of their specified charters
- be careful not to inhibit lawful advocacy, protest or dissent

- avoid any suggestion of political partisanship
- exercise good judgement about proportionality in collection activities
- be sensitive to the privacy of Australians, and
- act objectively and with integrity.

Naturally the role of my office and other accountability arrangements have also been covered.

Agency powers and capabilities

At least as notable as the growth in the size of the agencies have been increases in the powers and capabilities available to the AIC agencies in recent years. Where relevant I and my office have contributed to parliamentary committee deliberation on legislation, particularly on safeguards and protections against abuse.

ASIO questioning and detention warrants have been one particular focus. My office plays a central role in monitoring what occurs. I have made it a personal practice to attend on at least the first day of questioning. When so attending, the legislation provides me with the capacity to raise any concerns about the process¹. These concerns must be addressed by the prescribed authority (usually a retired judge, who also monitors the questioning), if necessary by suspending the questioning.

The provisions in the *Australian Security Intelligence Organisation Act 1979* allowing for these warrants and experience with them were carefully reviewed by the PJCIS in 2006² and were extended subject to another sunset clause. While I well appreciate why these provisions are controversial and bear very close monitoring, and I was one of the voices urging that there should still be a sunset clause, some of the public commentary has been disappointing.

Some critics deliberately ignore one of the legal requirements for the issue of such a warrant, namely that “relying on other means of collecting that intelligence would be ineffective”.³ In my view this

makes it a device of last resort and to suggest that a wide range of innocent people could be subject to such warrants is simply wrong. Similarly some critics seem determined to ignore the range of other protections and safeguards that have been put in place.

Other contentious issues which are among the subjects of close attention by OIGIS in inspection activities are the capacity for ASIS officers to carry weapons for self-defence, and changes to telecommunication interception legislation such as the introduction of B-party warrants and proposed authorisations for prospective metadata.

Legislation generally

I have also played a broader role in relation to legislation through membership of the Sheller Committee (the Security Legislation Review Committee) which conducted a review of the terrorism offence provisions in the Criminal Code and related legislation enacted in 2002 and 2003.

The Committee’s report was tabled in Parliament on 15 June 2006⁴ and has been the subject of two subsequent inquiries by the PJCIS⁵. It is to be hoped that the Government takes on board the recommendations which have emerged from these processes given the careful deliberation which has led to their formulation.

I have also been pleased to be a member of the Administrative Review Council⁶ which has a general advisory and monitoring role on the administrative law system in the Commonwealth.

Intelligence assessments

Another distinct development in the work of OIGIS has been in relation to ONA. Following the review in 2004 by Mr Philip Flood AO of the Australian intelligence agencies⁷, amendments to the IGIS Act mean that periodic reviews are to be conducted of the independence and propriety of ONA assessments.

¹ Section 34 Q, *Australian Security Intelligence Organisation Act 1979*.

² Parliamentary Paper No: 454/2005.

³ Sections 34D(4) and 34F(4), *ASIO Act*, op. cit.

⁴ Security Legislation Review Committee 2006, *Report of the Security Legislation Review Committee*, SLRC, Attorney-General’s Department, Canberra.

⁵ Parliamentary Paper No: 423/06. Parliamentary Paper No: 201/07.

⁶ See Part V of the *Administrative Appeals Tribunal Act 1975*.

⁷ P. Flood, *Report of the Inquiry into Australian Intelligence Agencies*, Canberra, July 2004.

For many years the work of OIGIS has been focussed on collection activities for the quite understandable reason that it is collection activities which are most likely to impact on the rights of Australians. However, in light of sensitivities about intelligence assessments, there is a need for processes to provide assurance that ONA assessments are not subject to improper external direction or influence and that generally the process by which assessments are formulated has integrity.

The IGIS model

It is interesting to reflect on how the Australian IGIS model has stood up over time. The recent developments are something of an evolution from what can be described as “the eyes and ears of the ministers”. There is a need for reassurance of the Parliament and the community that agencies are using their expanded powers and capabilities professionally, properly and for the purposes for which they were given. I am conscious that to satisfy this broader expectation the office needs to be better known outside the AIC in a targeted way. There might also be merit in reviewing whether some greater capacity for disclosure in the period between the annual reports to Parliament than the IGIS Act currently permits, would assist in this regard.

Other elements of the IGIS model such as the capacity to call on strong investigative powers, flexibility over how each inquiry is conducted, and having “own motion” capacity to initiate inquiries or inspections as well as being able to respond to complaints and requests from Ministers, continue to be very sound elements of the model.

The independence of the position has been strongly maintained. The IGIS is not subject to general direction on how the inspection program or particular inquiries should be formulated or conducted. The only exception to this is that the Prime Minister can direct the IGIS to inquire into a particular matter, although how the IGIS conducts the inquiry is up to that statutory office holder.

In practice I have found ministers and agencies to be properly respectful of the independence of OIGIS. This has extended to accepting that in applying the Uhrig⁸ templates to agencies, mechanisms such

as ministerial statements of expectation and, in response, agency head statements of intent, are not appropriate for OIGIS.

Scope of jurisdiction

While to some foreign eyes it is unusual that an IGIS should review six agencies rather than focussing on one, I have found being able to compare and contrast useful, as is being able to track something across the agencies.

Indeed, the span of agencies which can be involved in issues such as counter-terrorism can be considerable and this has caused me to reflect on whether there should be some capacity to extend an inquiry under the IGIS Act to include intelligence and security activities of other agencies in special circumstances. This should not be the norm lest there be a diminution of the focus of my office on the AIC, but there are occasions when an intelligence or security issue can only be satisfactorily examined by going outside the AIC.

Another important feature of the IGIS jurisdiction is that the concerns of the office are specified in the IGIS Act as legality, compliance with ministerial directions or guidelines, propriety and respect for human rights.

Propriety is not defined in the Act. The view taken by successive Inspectors-General has been that in the context of this particular legislation “propriety” does not mean efficiency or reasonableness (at least in themselves), but rather conformity with a standard as to what is “proper”. This would seem to be in accord with the view of Justice Madgwick of the Federal Court that when the IGIS reviews an assessment made by ASIO in relation to a visa holder, the review cannot extend to the actual merits of the assessment.⁹

While conscious that there are outer boundaries to the concept of propriety, I have seen it as usefully encompassing issues such as procedural fairness, the integrity of intelligence assessments, and proportionality in intelligence collection activities (i.e. that actions taken and the degree of intrusion must be proportionate to the nature of the threat and its apparent urgency).

⁸ Uhrig, J (2003) Review of the Corporate Governance of Statutory Authorities and Office Holders, Commonwealth of Australia, Canberra.

⁹ See *Leghaei v Director-General of Security* [2005] FCA 1576.

While this flexibility has been generally suitable, that there are outer boundaries to the jurisdiction of this office does arguably raise two broader issues about the accountability of the AIC which are worth comment.

One is quite specific and is whether merits review should be available for certain categories of people who currently are precluded from appealing to the AAT. While people who are Australian citizens or permanent residents can appeal to the AAT on decisions such as the refusal or cancellation of a passport because of an ASIO security assessment, people outside these categories (such as refugee claimants for a visa) do not have resort to the AAT.

My predecessor had recommended that the legislation be changed to provide for AAT review for refugee applicants where appropriate Australian authorities find that the applicants have a well-founded fear of persecution if returned to their country of origin.¹⁰ This was not taken up at the time but I think it would be worthwhile revisiting the proposal. The number would be very small (hence cost should not be a barrier) and there would be greater public assurance that a sensitive group of cases have been carefully examined. As noted earlier, the jurisdiction of my office does not extend to the merits of security assessments, so the extent of review my office can offer is constrained.

The second issue worth comment is a broader one about the best means for reviewing the efficiency and overall effectiveness of the AIC agencies, individually and collectively.

This has been the subject of consideration by the PJICIS¹¹ and by the 2004 Flood review. The approach taken by the latter was that the Department of the Prime Minister and Cabinet (PMC) should advise the National Security Committee annually on the performance of the foreign intelligence community and conduct an annual review of ONA's performance (activities which that Department has subsequently taken up), and additionally that the intelligence community should be subject to periodic external review every five to seven years.¹²

I should also note another limitation to the role of the IGIS. Generally complaints by employees of the AIC agencies which concern their treatment as employees or their conditions of service are outside the legislative remit of this office. The intention is that there be other mechanisms to deal with such matters, and that the focus of IGIS review be squarely on the operational activities of the AIC agencies. I believe this is still a valid approach in respect of individual matters. Importantly, the IGIS Act does not preclude IGIS review of policy, procedures and general practice around human resources processes including those for staff grievances.

Liaison

I have been conscious that however well one devises particular mechanisms, the important issue in public administration is often how different mechanisms fit together. This is particularly important in the accountability area where gaps, overlaps or territorial battles between different watchdogs could defeat the overall effectiveness of arrangements.

With this in mind I have consciously sought to ensure good links with the PJICIS, the Commonwealth Ombudsman, the Privacy Commissioner, the ANAO and the Human Rights Commissioner. All have had the same view about having a suitable relationship and where necessary, alignment.

¹⁰ IGIS Annual Report 1998-1999, p 17.

¹¹ Parliamentary Paper 572/2002; Parliamentary Paper 83/2005.

¹² Flood, op. cit., recommendations 10 and 22.

The year in review

General matters

Although Australia is an island, for practical purposes we live and operate in an increasingly globalised and interconnected world, where distant actions can and do have a direct impact on the way in which we live our lives.

In the period since the 21st century commenced, there has been rising concern about the nuclear and other intentions of certain nation states, the global spread of acts of politically motivated violence by nation states and non-state players, the potential vulnerability of new technologies and critical infrastructure to individuals or groups with hostile intentions, and a developing awareness of the potential for climate change to have an impact on security.

In short the global security environment is not benign to Australia's enduring national interests, it can and does change rapidly, and it is increasingly complex to navigate.

Key intelligence and security interests

During the period 1 July 2006 to 30 June 2007, the AIC focussed on a wide variety of monitoring, collection and assessment activities. It is impossible in any annual report to list the full range of these activities, both for valid security reasons and because they are too numerous to detail, but these interests included:

- the detection and disruption of serious threats to the interests of Australians at home and abroad
- rendering support to various Australian Defence Force (ADF) deployments overseas (including in

hostile operational environments such as Iraq and Afghanistan)

- the regulated sharing of information with other agencies, to gain a better appreciation of potential threats, and to enhance regional and global security
- sharing skills and building capability within our region to deal more effectively with the threat posed by terrorism
- 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
- providing support to the security effort associated with Australia's hosting of the Asia-Pacific Economic Cooperation (APEC) Leaders Forum in September 2007, and various associated meetings in the lead up to this event.

Continuing growth of the AIC

Following the 2004 review by Mr Philip Flood AO and other reviews such as that by Mr Allan Taylor AM into ASIO's resources¹³, the AIC has expanded considerably.

It is not appropriate to provide specific details of the growth and current size of each agency (as to do so could inadvertently provide details of an agencies capabilities and priorities), but the announcement on 16 October 2005 by the Attorney-General, the Hon. Philip Ruddock MP, that ASIO would grow from 980 positions as at that date, to 1860 positions by 30 June 2011, is one indication which has been put in the public domain.

¹³ See IGIS Annual Report 2005-2006, Canberra, October 2006, p. 23.

While each of the AIC agencies has suffered varying degrees of organisational stress associated with rapid growth, from what I have seen the AIC agencies have continued to function at a high level while juggling the competing demands of a complex and dynamic security environment, responding flexibly to new and emerging threats, undergoing significant internal restructuring and accelerating the education and development of new staff.

Consequential growth of OIGIS

When I first commenced as IGIS, the office comprised myself and four staff. This was maintained for approximately 12 months before I obtained funding approval to increase the size of the office, in recognition of the expanded role and functions of the office flowing from changes to the IGIS Act and other intelligence related legislation recommended in the Flood review, and to also match the actual and anticipated growth of the AIC.

The growth of OIGIS over the past two years has been phased, rather than occurring all at once. This has occurred so as to ensure that the changes to the office are digestible, and also due to the length of time it takes for preferred candidates for positions to this office to proceed through the extensive security vetting process.

As at 30 June 2007, OIGIS comprised myself and nine staff, each of whom perform a variety of inspection, inquiry, review, complaints handling and corporate functions. Further details about the composition of the office are provided in the Corporate and Communications chapter of this report.

Summary

It is against the above backdrop of an increasingly complex and dynamic security environment, the rapid growth of the AIC agencies, the extension of new powers to those agencies, and public debate about the potential loss of hard won rights and liberties that I report on the activities of my office for the reporting year 1 July 2006 to 30 June 2007 (hereafter "the reporting period").

OIGIS – 20th anniversary

OIGIS commenced operations on 1 February 1987 and naturally enough celebrated its 20th anniversary on 1 February 2007.

The inaugural IGIS, Mr Neil McInnes AM, commenced operations in premises located at Macarthur House, Lyneham, ACT, but this arrangement lasted for approximately one year only, following which OIGIS accepted an invitation to lodge with PMC, in its building located at 3–5 National Circuit, Barton, ACT.

In the succeeding years OIGIS has been physically located in the PMC building and made significant use of the corporate facilities provided by our portfolio Department.

Despite our close organisational links and physical proximity to PMC, my predecessors and I have always been very conscious to maintain the separate identity of OIGIS. This is important as the IGIS, like the Commonwealth Ombudsman, is an independent statutory office holder and as the head of a watchdog agency must be prepared to be critical of government agencies when and where appropriate.

The effectiveness and utility of the office would be seriously eroded were it to be considered anything other than genuinely independent.

On 19 February 2007, PMC moved to new premises located at One National Circuit, Barton, ACT (i.e. immediately adjacent to their former offices). OIGIS moved at the same time, to the new PMC building. This was no simple exercise due to the security overhead associated with ensuring that the new premises were wholly secure from day one, but I am pleased to advise that this was achieved with little disruption to our day to day activities.

So as to mark the dual occasion of the 20th anniversary of the creation of the office, and our move to new facilities, I hosted a small function at our new offices on 9 March 2007, to which I invited my four predecessors as IGIS.

A brief pen portrait of each of the previous Inspectors-General is provided on the opposite page.

Mr N D (Neil) McInnes AM

(1 February 1987– 27 September 1989)

The inaugural Inspector-General was selected to establish OIGIS in late 1986, following a lengthy career observing and commenting on international relations and several subsequent senior level appointments within government.

In the course of a lengthy stint as a journalist based in Paris (1955-1978), Mr McInnes wrote four respected books which provided an in depth analysis on the development and theoretical underpinnings of the Communist parties of western Europe.

Following his return to Australia, Mr McInnes filled the position of the Deputy Director-General of ONA (1978–1982), before being promoted as a Division head within the Department of Defence (1982–1983), and then as a Deputy Secretary in PMC (1983–1986).

Mr J R (Roger) Holdich AM

(28 September 1989 – 5 April 1995)

Like the inaugural IGIS, Mr Holdich was another foreign affairs specialist. After commencing his career in the South Australian Department of Trade, Mr Holdich gave many years of distinguished service to the Department of Foreign Affairs (1959–1976), during which time he rose to Ambassadorial rank (to the Republic of Korea 1975–1976).

Following his return to Australia, Mr Holdich headed up the International Division of PMC (1976–1983), before appointments at the Deputy Secretary level in the then Departments of Special Minister of State (1983–1987), and Administrative Services (1987–1989).

Mr R N (Ron) McLeod AM

(6 April 1995 – 18 February 1998)

Mr McLeod took up as Inspector-General following a long and distinguished career at the then Public Service Board and the Department of Defence.

In his time at the Public Service Board, Mr McLeod held positions at the Branch and Division head level (1971-1984), before being promoted to become the Deputy Secretary Budget and Management, in the Department of Defence (1984-1995).

In 1994, Mr McLeod was seconded to head a major review of the *Public Service Act 1922*, and made a series of recommendations which ultimately lead to the Act being wholly revamped in the form of the *Public Service Act 1999*.

Towards the completion of his first term as Inspector-General, the Government appointed Mr McLeod as the Commonwealth Ombudsman (1998-2003).

Mr W J (Bill) Blick AM, PSM

(19 February 1998 – 22 March 2004)

Mr Blick commenced as the fourth Inspector-General in February 1998 immediately upon Mr McLeod's appointment as Commonwealth Ombudsman.

Prior to his appointment, Mr Blick spent the majority of his career at various levels within the Department of the Prime Minister and Cabinet, ultimately heading up that department's Government Division, before being promoted to the Deputy Secretary level (1996-1998).

While in the later position, Mr Blick took a leading role in organising the Federal constitutional convention of February 1998 at which delegates were asked whether or not Australia should become a republic, and following a majority vote to this effect, which model for a republic they preferred.

In the midst of his career within PMC, Mr Blick served as the Deputy Commonwealth Ombudsman (1984-1986).



L to R: Mr Ron McLeod AM, Mr Ian Carnell, Mr Neil McInnes AM, Mr Roger Holdich AM, Mr Bill Blick AM, PSM



L to R: Mr Ron McLeod AM, Mr Philip Moss, Professor John McMillan, Mr Bill Blick AM PSM

Also present at the 20th anniversary event was Mr Philip Moss, who holds the singular distinction of being the inaugural and thus far only Assistant Inspector-General of Intelligence and Security (1987–1997).

I additionally invited the Commonwealth Ombudsman, Professor John McMillan, in recognition of the close links between our respective agencies and because Professor McMillan holds a standing appointment to serve as the acting IGIS, whenever I am overseas, on extended leave, or otherwise unable to discharge the functions of the office.

I am pleased that this small but distinguished group was able to join with me, current OIGIS staff, and several other friends of the office, to mark 20 years of dedicated service to the principles upon which the office was founded.

Reappointment as IGIS

Mechanics and duration of re-appointment

The arrangements for appointing an individual as IGIS are set out in sections 6 and 26 of the IGIS Act.

Such appointments are made by the Governor-General, on the recommendation of the Prime Minister, following consultation with the Leader of the Opposition in the House of Representatives.

The IGIS may hold office for a period not exceeding five years, as specified in the instrument of appointment, but is eligible for reappointment, excepting that a person is not eligible to hold the office more than twice.

I was first appointed as IGIS for a period of three years, with effect from 23 March 2004. My first term as IGIS, therefore expired at the end of 22 March 2007.

I have provided some brief reflections on my first term elsewhere in this report.

Considerations for filling the position had not been completed by early March 2007, and the Prime Minister issued an instrument (pursuant to section 6A of the IGIS Act), appointing me acting IGIS for the period 23 March to 30 April 2007.

I was subsequently appointed as IGIS on a full time basis for a period of four years, commencing from 27 April 2007.

Instruments appointing Prof John McMillan as acting IGIS

It has been the practice of this office over several years to rely on the good offices of the Commonwealth Ombudsman to act as IGIS, in a personal capacity, to cover situations where the IGIS is on duty overseas, on extended personal leave, or on occasions when the IGIS is otherwise unable to discharge the functions of the office.

This arrangement has developed because the office has not had a need for an Assistant Inspector-General since the departure of Mr Moss in 1997, and there is too big a gap in work classification levels between the IGIS and the next most senior persons in the office (who are at the Executive Level 2 classification).

A standing instrument first appointing Professor McMillan as acting IGIS was issued by the Prime Minister on 8 October 2005.

As mentioned earlier, it was necessary for me to be appointed as acting IGIS between 23 March and 27 April 2007. The instrument appointing me as acting IGIS, voided all other instruments appointing persons to act in the office of IGIS (including the standing instrument appointing Professor McMillan).

Following confirmation of my reappointment in late April 2007, the Prime Minister made a new standing instrument, in accordance with section 6A(1) of the IGIS Act, appointing Professor McMillan to act as IGIS as required. This instrument was signed on 28 May 2007.

AIC leadership changes

New Secretary of the Department of Defence

In a press release dated 2 November 2006, the Prime Minister, the Hon. John Howard MP, advised of the proposed retirement of the then Secretary of the Department of Defence, Mr Richard (Ric) Smith AO, and his replacement by Mr Nick Warner with effect from 4 December 2006.

I had cause to meet with Mr Smith several times during my first term as IGIS, and found him to be at all times very willing to discuss issues falling within his bailiwick, to provide resources and facilities where necessary to assist my work, committed to accountability, and to be genuinely responsive to the needs of my office.

New Deputy Secretary Intelligence and Security in Defence

As indicated in my previous annual report Mr Shane Carmody replaced Mr Ron Bonighton AM, as the Deputy Secretary Intelligence and Security (DepSec I&S) in the Department of Defence, following Mr Bonighton's retirement in November 2005.

In October 2006, Mr Carmody accepted an appointment as the Deputy CEO Strategy and Support, with the Civil Aviation Safety Authority.

The then Director of DSD, Mr Stephen Merchant commenced as acting Deputy Secretary I&S upon Mr Carmody's departure, and was confirmed in that position in February 2007. Subsequent to his appointment, Mr Merchant has also assumed functional responsibility for the International Policy Division of the Department of Defence.

New Director DSD

The short term movement of Mr Merchant to fill the vacancy created by Mr Carmody's departure, and his subsequent confirmation as DepSec I&S, left a consequential vacancy in the position of Director of DSD.

It was announced in early May 2007 that Mr Ian McKenzie was the successful applicant for this position.

Mr McKenzie has spent many years working in various positions within DSD, and has also had extensive experience in a variety of senior level

positions elsewhere within Defence, including as Director DIGO (2003-2006).

New Director DIGO

The filling of the Director DSD by Mr McKenzie naturally left the position of Director DIGO vacant. A senior DSD manager, Mr Clive Lines, accepted an invitation from the Secretary of the Department of Defence to transfer to this position.

Mr Lines has had extensive senior level experience in a variety of positions within the Department of Defence, including DIO and DSD.

Valedictions

Mr Allan Taylor AM

It is with sadness that I note the passing of a former Director-General of ASIS, Mr Allan Taylor AM, who died on 19 June 2007.

Although my term as IGIS did not overlap with Mr Taylor's time as Director-General of ASIS, I nonetheless had interactions with him in various forums over the years, and developed a very healthy respect for his intellect, his sense of fair play, and his humanity.

Based on the work of my office, I know that Mr Taylor devoted considerable efforts to modernising various management and work practices within ASIS, and making it a more forward looking and responsive agency.

Mr Hadyn Strang

It is extremely unusual for current or former ASIO officers to be publicly identified, whether it be for praise or criticism. Indeed, section 92(1) of the ASIO Act, specifically prohibits the publication of the identity of current or former ASIO officers, without the written consent of the relevant Minister, or the Director-General of Security.

I am therefore grateful to the Director-General of Security for allowing me to briefly highlight the contribution of Mr Hadyn Strang, who sadly passed away on 24 January 2007.

Mr Strang served as ASIO's principal legal adviser from 1988 until his retirement several years ago, following which he continued to provide legal consultancy services to ASIO.

As the principal legal adviser to various Directors-General of Security, Mr Strang made a huge contribution to ensuring that ASIO's various legal obligations were being met, and developing guidance and advice on the myriad legal issues which an organisation such as ASIO must confront.

Honours and awards

Dr Peter Shergold AC

The Secretary of PMC, Dr Peter Shergold, was made a Companion of the Order of Australia in the Australia Day honours list, which was announced on 26 January 2007.

By virtue of his position Dr Shergold regularly attends meetings of the National Security Committee of Cabinet as an adviser, and also chairs the Secretaries Committee on National Security. As such, Dr Shergold is vitally involved in guiding the work of the AIC.

Mr Ian Cousins PSM

With the approval of the Director-General of Security, I would like to congratulate Mr Ian Cousins on the awarding to him of a Public Service Medal (PSM), in the Australia Day honours list, which was announced on 26 January 2007.

Mr Cousins has served as Deputy Director-General of Security for many years and has made a very significant contribution to ASIO over very many years. Mr Cousins has received his award for outstanding public service in the delivery of Australia's security policy framework and critical infrastructure initiatives.

Dr Paul Taloni PSM

Dr Paul Taloni was also awarded a Public Service Medal in the Australia Day honours list, which was announced on 26 January 2007. Dr Taloni received his award for outstanding public service as Deputy Director of the DIO.

Prior to the award being announced Dr Taloni accepted another senior level appointment elsewhere in the Department of Defence. I wish Dr Taloni well in his new position and congratulate him on his award.



Neville Bryan receiving his PSM

Mr Neville Bryan PSM

It gives me special pleasure to advise that one of my own staff, Mr Neville Bryan, was also awarded a Public Service Medal in the Australia Day honours list, which was announced on 26 January 2007.

Mr Bryan was officially recognised for outstanding public service in the monitoring of the AIC. My two immediate predecessors and I have all found Mr Bryan's commitment, insights and sustained endeavours immensely valuable.

IGIS activities

The functions of the IGIS are set out in detail in the IGIS Act. Broadly speaking the business of my office can be divided into three parts, namely:

- inquiry activities, under which heading complaints are received and processed, matters can be referred by responsible ministers for examination, and the IGIS can initiate 'own motion' inquiries (as provided for under section 8 of the Act)
- inspection activities, which involve the IGIS proactively monitoring and/or reviewing the activities of the AIC agencies, with the purpose of giving effect to the objectives of the IGIS Act (as provided for under section 9A of the IGIS Act), and
- corporate activities, which involve the IGIS complying with all reporting and other obligations imposed on all independent government agencies, and where possible, contributing to good governance arrangements across the public service.

Complaints and inquiries

The IGIS Act generally empowers my office to receive complaints about the AIC agencies, and also provides a framework against which they can be processed or inquired into.

If my office receives a complaint which does not fall within our jurisdiction, we will promptly inform the complainant of this fact and whether or not there are any other avenues available to them for consideration of their concerns.

Section 11 of the IGIS Act provides the IGIS 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, the IGIS will not pursue an inquiry where a complainant has exercised or exercises a right to cause the action to which a complaint relates to be reviewed by a court or tribunal, unless the IGIS is 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, the IGIS has three options on how next to handle a complaint, namely administratively, as a preliminary inquiry, or as a full inquiry.

The bulk of complaints made to the office are handled administratively and the majority of the complaints in the reporting period related to purported delays by ASIO in processing security assessments for applicants for different classes of visa. I will comment separately on the processing of these complaints elsewhere in this report.

Of the remaining complaints which we receive and process administratively, the majority are dealt with in the office 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 that the

complainant holds genuine but misconceived ideas about the role and functions of the AIC agencies, or the complainant has put forward suggestions which are highly unlikely (i.e. conspiracy theories) or manifestly impossible (i.e. purported new mind control or related technologies).

Notwithstanding that quick judgements can sometimes be made about a number of these complaints, all complaints are taken seriously with complainants being treated with courtesy and respect.

The next means by which a complaint can be processed is by way of a preliminary inquiry. Such inquiries are provided for under section 14 of the IGIS Act, and are ordinarily pursued if there is a question about jurisdiction or if the IGIS requires further information 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.

The final means of investigating a complaint is by means of an inquiry, as provided for under Division 3 of the IGIS Act (such inquiries are colloquially referred to a “full inquiries” in our office, so as to distinguish them from “preliminary inquiries”).

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

These powers, which are roughly 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 the IGIS to answer questions relevant to the matter under inquiry, and to administer an oath or affirmation.

During the reporting period the office initiated 13 new full or preliminary inquiries. This compares with 20 such new inquiries initiated in the previous reporting period.

The decline in the number of matters which I judged required a full or preliminary inquiry is an encouraging trend, especially when considered against the substantial growth of the AIC, the numbers of newly trained officers who are now operating in the AIC, and an increasing operational tempo.

During the previous reporting period we received 53 complaints about AIC agencies which did not relate to the processing of security assessments by ASIO. In this reporting period this figure was 65. As can be seen this figure is relatively stable.

During this reporting period my office received 74 complaints about alleged delays by ASIO in preparing security assessments on applicants for various visa categories, which I chose to handle administratively. This represents a very substantial increase on the 26 such complaints OIGIS processed administratively during the previous year.

There are several reasons why the number of immigration related complaints has increased substantially, and these are separately addressed in the chapter on ASIO. Having said that, an increase of this kind is nonetheless disappointing, and certainly an issue which I will be paying close attention to in the year ahead.

A fuller examination of the level of complaints made to this office, and the timeliness with which they were dealt is explored in the 'Performance' chapter of this report.

Inspection program

The origins of this office lay in a recommendation made by Justice Robert Hope, in the final report of his Royal Commission on Australia's Security and Intelligence Agencies, in December 1984.¹⁴

Justice Hope had a clear conception of the role of this office, when he suggested that a new body should be established with the proposed title of Inspector-General of Intelligence and Security, rather than another formulation such as Intelligence Ombudsman or Security Commissioner.

"My own preference for the title of such an office is 'Inspector-General of Security' (or if, as I recommend in the General Report, the work of the office extends to other agencies, 'Inspector-General of Security and Intelligence')¹⁵. I believe the title 'Inspector-General' is more descriptive of

the intended role of the office and is less likely to connote executive responsibilities than the title 'Security Commissioner.'¹⁶

In suggesting the title for the recommended new office, Justice Hope clearly conceived that much of the focus of the office would be on inspection activities rather than dealing with complaints.

The underlying rationale for this was that, without undercutting the management prerogatives and responsibilities of responsible agency heads, there would be utility in a body such as IGIS actively monitoring the intelligence agencies to identify issues and trends of potential concern as they arise, rather than trying to deal with such concerns after they have become systematised or major concerns.

The need for such a focus was reaffirmed and emphasised by Justice Gordon J Samuels AC QC, and Mr Michael H Codd AC, in their Report of their Commission of Inquiry into ASIS, which was published in March 1995.¹⁷

During the reporting period the resources of the office (apart from what was necessary for corporate and administrative matters) were allocated so that approximately two thirds of the efforts of the office was spent on inspection activities.

As I have stated previously, I firmly believe in the positive effect OIGIS inspection activities have on influencing normative behaviour within the agencies.

The strength of the inspection program is indeed that it is proactive and attempts to influence the culture of the intelligence and security agencies and assists to prevent or forestall problems of illegality or impropriety.

If combined with professional leadership and governance in the agencies, the outcome should mean few, if any, genuine "scandals" and only a very modest rate of the sort of errors which are bound to occur in even the best organisations. It should also mean only a modest number of formal inquiries need be undertaken by this office.

¹⁴ Justice R. M. Hope, *Royal Commission on Australia's Security and Intelligence Agencies*, General Report, AGPS, Canberra, December 1984, p. 25, paragraph 3.26.

¹⁵ Elsewhere in the General Report, and in his report on ASIO, Justice Hope reformulated the title of the proposed office as the 'Inspector-General of Intelligence and Security'.

¹⁶ Justice R. M. Hope, *Royal Commission on Australia's Security and Intelligence Agencies, Report on the Australian Security Intelligence Organization*, AGPS, Canberra, December 1984, p. 330, paragraph 16.85.

¹⁷ Justice G. J. Samuels, and M. H. Codd, *Report on the Australian Secret Intelligence Service*, Public Edition, AGPS Canberra, March 1995, p. 94, paragraph 9.4.

Fuller details of the inspection activities of the office are provided in the individual chapters on each of the agencies, but the activities have included:

- reviewing relevant documentation 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
- actively reviewing exchanges of information about Australians by AIC agencies with their counterparts to ensure that this activity is properly authorised and regulated
- regularly reviewing the application of privacy rules to products/ records generated by ASIS, 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 the application of relevant weapons guidelines and approval processes in respect of ASIS personnel
- regularly speaking to AIC staff at an expanding range of training courses to promote awareness of the importance of accountability and acting legally and with propriety
- regularly visiting AIC offices and sites around Australia (to reinforce that all AIC staff are accountable not only those based in each agency headquarters), and
- visiting AIC staff and their offices in overseas locations on an occasional basis, as circumstances and opportunity permits.

Notwithstanding the broad nature of our existing inspection program, there is always scope for it to be varied (so that it does not become stale), and to add new inspection tasks as new powers and functions are provided to the various agencies.

With the recent growth in the size of OIGIS, I also intend to initiate further pilot projects to see if particular extensions to the inspection program would be useful.

Liaison with other Commonwealth accountability bodies

Commonwealth Ombudsman

As detailed in my previous annual report, the Ombudsman and I formally entered into a Memorandum of Understanding (MOU) on 14 December 2005, to provide a framework within which complaints which might overlap our respective jurisdictions might be most effectively handled and unnecessary duplication be avoided.

I was very happy with the manner in which our two offices interacted during the reporting period. While I do not see any current or pressing need to alter the terms of the MOU, I will review its operation periodically, in consultation with the Ombudsman, to ensure that it continues to meet our common objectives.

Australian National Audit Office

Another key Commonwealth accountability agency with which this office has occasional dealings is the ANAO.

Section 16 of the IGIS Act requires that before commencing an inquiry into a matter relating to an agency, the IGIS should have regard to the functions of the Auditor-General in relation to that agency with a view to avoiding inquiries being conducted into the same matter by both agencies.

Although I did not initiate any inquiries in this reporting period which were likely to overlap with the Auditor-General's role and functions, I have met periodically with the senior executive within ANAO with responsibilities for the AIC agencies to discuss matters of mutual interest or concern.

Australian Commission for Law Enforcement Integrity

The Australian Commission for Law Enforcement Integrity (ACLEI) was established on 30 December 2006 with the coming into effect of the *Law Enforcement Integrity Commissioner Act 2006*. This Act also established the new statutory office position of the Integrity Commissioner as the head of ACLEI.

Professor John McMillan served as the Acting Integrity Commissioner, for the first six months of ACLEI's existence, before the Attorney-General announced via a media release dated 22 June 2007,

his intention to appoint Mr Philip Moss as Integrity Commissioner, with effect from 23 July 2007. As advised elsewhere in this chapter, Mr Moss spent 10 years in OIGIS between 1987 and 1997, rising to become the inaugural and thus far only Assistant Inspector-General.

Although I expect that there will be little overlap between our respective offices, I welcome ACLEI to the ranks of Commonwealth accountability agencies, and congratulate Mr Moss on his appointment.

Community outreach

Although OIGIS is quite a small office it is important for the existence of the office to be known to as many people as possible. To this end, my staff and I contributed to, or participated in, a number of targeted outreach activities during the reporting period to raise awareness of the office within the community.

One means by which this was achieved was through our contribution to a small but important publication coordinated by ONA entitled *The Australian Intelligence Community: Agencies, functions, accountability and oversight*¹⁸, which was publicly launched by the heads of the AIC agencies and myself on 20 October 2006.

The brochure is the first occasion on which the AIC has attempted to simply set out in a public document its role and functions, the inter-relationship of the agencies with the higher-level intelligence setting and coordination committees, and the accountability and oversight framework in which the AIC operates.

In addition to the above initiative, my office arranged for the brochure explaining the role and functions of the IGIS to be translated into another 12 community languages, bringing the total to 16. Hard copies of these brochures have been circulated to relevant government offices and to interested community groups, and are also freely available electronically on our website at <<http://www.igis.gov.au/>>.

I additionally spoke about the role and functions of the office, or participated in panel discussions, at the following forums during the reporting period:

- Equal Opportunity Commission of Victoria forum on anti-terrorism legislation (27 September 2006)
- Australian Financial Review National Security & Counter Terrorism Conference, Melbourne (24 October 2006)
- Strategic and Defence Studies Centre, Australian National University, Canberra (1 May 2007), and
- the 'Above Board Public Accountability Forum', Australian National University, Canberra (12 May 2007).

Training

As the AIC continues to recruit heavily, and more persons become engaged in intelligence related activities, I believe it is vitally important for the underlying rationale for existence of my office, its role and functions, to be explained and for my staff and I to be as visible as possible.

As a consequence I and members of my staff have actively sought to make presentations at suitable agency training courses and seminars as often as possible. In this reporting period OIGIS made at least 48 such presentations to at least 1,100 staff from across the six AIC agencies, at different locations across Australia.

The presentations are suitably 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 the need for accountability and community confidence in their use of special powers and capabilities.

In addition to delivering presentations on the role and functions of the IGIS, members of my staff and I have also attended several agency training courses either as participants or observers.

¹⁸ This publication can be accessed at <<http://www.ona.gov.au/publications/aic.htm>> (as at 10 August 2007).

International cooperation

During the reporting period, we again received a number of international visitors. Notable among these were visits from individuals in the senior ranks of the United Kingdom and Canadian governments who have responsibilities for intelligence and security arrangements in those countries.

IIRA Conference 2006

In October 2006, I attended the fifth International Intelligence Review Agencies (IIRA) conference, which was held in Cape Town, South Africa. The rest of the Australian delegation to the conference comprised the Hon. David Jull MP (Chair of the PJCS), Senator the Hon Robert Ray and Mr Stewart McArthur MP (also members of the PJCS), my Principal Investigation Officer, Mr Neville Bryan PSM, and the then Secretary to the PJCS, Ms Margaret Swieringa.

The first meeting of what has subsequently come to be known as the IIRA conference occurred in October 1997, and was organised by the then IGIS, Mr Ron McLeod AM, to mark the 10th anniversary of the creation of this office.

The IIRA conferences have occurred approximately every two years since the inaugural gathering, rotating between the six nations which attended the first meeting (i.e. Australia, Canada, New Zealand, South Africa, United Kingdom and United States of America).

The theme of the conference in South Africa was *'Balancing National Security and Constitutional Principles within a Democracy.'*

As well as the inaugural members of the group, participants were also drawn from Belgium, Ghana, Namibia, the Netherlands, Norway, Poland and Tanzania.

Due to our historical, cultural and constitutional development Australia is naturally more likely to share views with countries with whom we have been traditionally aligned, however, it was an extremely useful and worthwhile exercise to hear the perspectives of delegates from outside of this realm and to learn more about the approaches of their countries to issues of intelligence oversight and accountability.

I wish to sincerely thank the co-hosts of the conference, the Hon. Dr Siyabonga Cwele (Chairperson of the South African Joint Standing Committee on Intelligence) and the Hon. Zolile Ngcakani (South African Inspector-General of Intelligence), and their hard-working staff, for putting together a most interesting and thought provoking program, for making all delegates so very welcome, and for organising what was a first class conference.

The sixth IIRA conference is to be hosted by New Zealand in 2008, following which hosting responsibilities will fall once more to Australia, at a date and venue to be determined, some time in 2010.

Other foreign visits

In April 2007 I visited some regional countries. The purpose of these visits was to meet with AIC staff, to gain some insight into their activities and to examine the various formal liaison arrangements which exist with local authorities.

In June 2007 I made a presentation to the *Administration of Justice and National Security in Democracies* conference, which was held in Ottawa, Canada, having been invited to do so by the conference organiser, the Hon. Allan Lufty, Chief Justice of the Canadian Federal Court.

The conference, which featured papers from, and round table discussion with, high ranking jurists from several jurisdictions, provided me with new insights into Canadian and United States approaches to issues with which we are also grappling.

The accountability of law enforcement and intelligence agencies is an issue to the fore in Canada following the release of two reports of a major public inquiry into the case of a Canadian citizen, Mr Maher Arar, who was rendered from the United States to Syria where he was imprisoned for one year and suffered degrading and abusive treatment.

The reports by Justice O'Connor (Associate Chief Justice of Ontario and Commissioner of the Inquiry) examined both Mr Arar's individual case and the adequacy of existing policing and intelligence oversight arrangements in Canada.

I also took the opportunity of my visit to Canada to meet with members and staff of the Canadian Security Intelligence Review Committee, the Inspector-General of the Canadian Security Intelligence Service, the Commissioner of the Communications Security Establishment and his office, as well as a range of government officials operating in areas in which I have a functional interest.

Significant issues

In this reporting period my office either had a direct involvement in or monitored a number of issues of public interest or significance. A brief summary of these issues is provided in this section, with a fuller discussion of some of these matters provided in relevant chapters elsewhere in this report.

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 IGIS should conduct periodic reviews of ONA's statutory independence.¹⁹

Mr Flood explained the rationale for this recommendation in the following terms:

*"Given the nature of the assessment business, where individuals' judgements are a key factor in the final product, and ONA's direct line of responsibility to the Prime Minister, with the consequent potential for charges of political interference, there is a need for some external process to ensure independence is preserved, and is seen to be so. This relates to the content of what is reported, and to what is not reported."*²⁰

The Flood report also emphasised that "...while intelligence priorities should be driven by policy needs, intelligence judgements must be uninfluenced by policy or political considerations."²¹

So as to give practical effect to Mr Flood's recommendation, the IGIS Act was amended, with effect from 2 December 2005, by the inclusion of subsection s8(3)(c). This subsection 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).

In the second part of the previous reporting period I initiated a review of ONA's statutory independence, using as my authority the general inspection powers afforded to the IGIS under section 9A of the IGIS Act.

This inspection activity involved reviewing various lines of ONA assessed products, surveying and interviewing ONA analysts and senior managers, interviewing customers of ONA products, and interviewing senior ministerial staff members.

I concluded this activity with the presentation of a report of my findings to the Prime Minister on 15 December 2006.

A fuller description of these processes and a general summary of my findings is provided in the chapter on ONA and at Annex 6.

While I do not believe that it is necessary or appropriate to continually conduct review of ONA's statutory independence, I was keen to build on the work done via my first review, and therefore decided in January 2007, to initiate a follow up review, which would be undertaken as a formal inquiry, as provided for under subsection 8(3)(c) of the IGIS Act. I did so to enable a more in-depth analysis of issues associated with ONA's statutory independence.

This inquiry into ONA's statutory independence was on-going at the conclusion of this reporting period.

Security assessment of UK citizen Mr Rhuhel Ahmed

In October 2006 I was alerted by media reporting of claims that a former Guantanamo Bay detainee, Mr Rhuhel (sometimes rendered as Ruhel) Ahmed, had been denied an entry visa into Australia, allegedly on advice from ASIO, thereby denying him the opportunity to speak to audiences in Australia about

¹⁹ Flood, op. cit., p.106 and p. 180.

²⁰ *ibid.*, p. 105.

²¹ *ibid.*, p. 9.

his experiences, and to promote a related film, of which he was a subject.²²

Shortly afterwards I received 37 letters, expressed in nearly identical terms, from members of the public expressing concern that Mr Ahmed had been denied a visa to enter Australia. Each of these correspondents asked me to investigate what role ASIO had played in this decision, and whether the decision was politically or otherwise improperly influenced.

Having separately reflected on the merits or otherwise of formally pursuing the matter, I initiated a formal inquiry on 28 November 2006.

The inquiry I conducted involved a review of all relevant documentation associated with this matter, consideration of the legal and administrative framework in which the decision to refuse Mr Ahmed a visa was made, the conduct of interviews/discussions with relevant ASIO personnel, and also obtaining statutory declarations from several ASIO officers with a connection to the matters under review.

I concluded my inquiry and provided a full report of my findings to the Attorney-General and the Director-General of Security on 12 March 2007.

I subsequently wrote to each person who made a complaint to my office (where we had sufficient contact details) on 2 April 2007 attaching an unclassified version of the report I had provided to the Attorney-General.

The conclusion I reached was that ASIO had been involved in making a security assessment of Mr Ahmed, in response to his application for a Business (Short Stay) Visa, and that in doing so it had acted legally and properly. There was no evidence or indication that the assessment had been the subject of improper influence.

A copy of my unclassified report into this matter is provided as Annex 3 to this annual report.

NSW coronial inquiry into the late Mr Brian Peters

As advised in last year's annual report²³ the NSW Coroner has been conducting an inquest into the death of Mr Brian Peters in East Timor, in October 1975. Mr Peters was one of five newsmen killed at that time who have come to be collectively known as the 'Balibo Five'.

My predecessor, Mr Blick, 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.²⁴

After at least one year of preparatory investigations, the NSW Deputy Coroner, Ms Dorelle Pinch, began a series of public hearings in February 2007, taking evidence in relation to a wide range of matters associated with the death of Mr Peters. These hearings were conducted over a number of weeks between February and June 2007, and involved a wide variety of witnesses including a number of former employees of the ADF/Department of Defence, including several who were associated through their work with DSD.

In his summary of the evidence which had been adduced before the inquest, the senior Crown counsel assisting the inquest, Mr Mark Tedeschi QC, was reported as saying that despite the historical record of intelligence records relating to the Balibo incident being incomplete, there was no sign of any conspiracy by the government to withhold relevant intelligence from the inquest.²⁵

²² See for example, 'ASIO thwarts film promotion' by Mr Garry Maddox, *The Sydney Morning Herald*, 28 October 2006.

²³ IGIS Annual Report 2005–2006, Canberra, October 2006 pp. 8–9.

²⁴ An unclassified version of Mr Blick's report was published at Annex 3 to the 2001–2002 IGIS Annual Report, pp. 82–90.

²⁵ 'MP's dupes' in game of deceit' by Hamish McDonald, *The Age*, 31 May 2007.

Mr Stephen Merchant (Deputy Secretary Intelligence, Security and International Policy, Department of Defence) also sought to set the record straight, as he saw it, on a report in *The Age* newspaper that quoted the senior Crown counsel assisting the inquest as saying “seven intercepts of Indonesian military signals relating to Balibo (were) evidently lost, misplaced or destroyed...”.

In a letter which was subsequently published in *The Age*²⁶, Mr Merchant said that the words attributed to Mr Tedeschi about records being lost, misplaced or destroyed, were not actually used by him in his final oral submission to the coroner. Mr Merchant referred to the possibility that references to missing intercepts may simply be a reflection of the fact that in some instances, 32 years after the event, witnesses’ recollections did not exactly match the document trail.

Mr Merchant concluded his letter by stating that:

“I can assure the public that the Defence Signals Directorate has gone to great lengths to ensure that all documentation it holds regarding the deaths of the newsmen in Balibo in 1975 has been made available to the inquest.”²⁷

In early June 2007, the NSW Deputy Coroner adjourned the inquest until a date to be fixed, at which time she would deliver the report of her findings. It is expected that this will be sometime in the first half of the 2007–08 reporting period.

It would be inappropriate for me to comment on matters which are still before the Coroner, other than to state that I have naturally been following these proceedings closely.

The Cole ‘Oil-for-Food’ Commission

On 10 November 2005 the Hon. Terrence Cole AO RFD QC was appointed to conduct an inquiry into and report on whether decisions, actions, conduct

or payments by various Australian companies mentioned in the Final Report of the Independent Inquiry Committee into the United Nations Oil-for-Food Programme breached any Federal, State or Territory law.

Commissioner Cole conducted a series of investigations and public hearings relevant to his terms of reference, before ultimately presenting the Report of his Inquiry to the Governor-General on 24 November 2006.

I advised in my previous annual report that I had not felt it necessary for me to initiate an inquiry into the conduct of any of the AIC agencies in relation to these matters while Commissioner Cole’s inquiry was in progress, but would consider this again when Commissioner Cole’s report was finalised.²⁸

Having now had the opportunity to read and reflect upon Commissioner Cole’s report, having regard to the detailed and forensic nature of Commissioner Cole’s investigations, and the fact that no adverse findings or imputations were made about the AIC in general, or any AIC agency in particular, I am not minded to initiate an ‘own motion’ inquiry into any AIC agency, in relation to these matters.

²⁶ Letters to the Editor, ‘For the record’ by Mr Stephen Merchant, Department of Defence, published in *The Age* on 6 June 2007, p. 20.

²⁷ *ibid.*

²⁸ IGIS Annual Report 2005–2006, op.cit. p. 9.

Parliament and legislation

Overview

The level of public and parliamentary interest in matters pertaining to intelligence and security and the rate of associated legislative development has risen dramatically in the period since the 11 September 2001 terrorist attacks on the United States.

In keeping with this trend, this reporting period saw high levels of public and parliamentary scrutiny of the activities of the AIC, the development, passage and implementation of various laws which extend the powers of the AIC agencies (and therefore have an impact upon this office), and a series of formal reviews being conducted which will also be influential in shaping the future legislative framework in which the AIC operates.

The following chapter briefly sets out my interactions with parliamentary bodies during the reporting period, summarises legislative developments affecting the AIC in which I have an interest, and briefly details input I have made to several legislative reviews.

Parliamentary oversight

PJCIS

The Chair of the PJCIS for the duration of the reporting period was the Hon David Jull MP, while the position of Deputy Chair was filled by Mr Anthony Byrne MP.

Mr Jull has announced that it is his intention not to contest his seat in the forthcoming Federal election, meaning that a new person will fill this position when the new Parliament is convened. Mr Jull has consistently shown a thoughtful and considered

approach to the leadership of the PJCIS during his tenure as Chair of the committee, and I must thank him for the courtesy which he has always shown to this office in our appearances before the PJCIS.

During this reporting period I appeared before or met with the PJCIS on four occasions, as follows:

- 31 July 2006, as a part of the PJCIS's *Review of Security and Counter Terrorism Legislation* which among other things considered the report of the Security Legislation Review Committee (the Sheller Committee) of which I was an *ex-officio* member
- 14 September 2006, a general update on the activities of OIGIS
- 3 April 2007, with Justice Sheller, in respect of the PJCIS's *Inquiry into the Terrorist Organisation Listing Provisions of the Criminal Code Act 1995*, and
- 10 May 2007, a general update on the activities of OIGIS.

My staff and I also met with members of the Secretariat which supports the PJCIS on two occasions during the reporting period, to discuss matters of mutual interest.

Senate Finance and Public Administration Committee

I prepared for and was available to appear before the Senate Finance and Public Administration committee during its consideration of Supplementary Budget Estimates in October 2006, Additional Estimates in February 2007, and Budget Estimates in May 2007, but was not called upon on any of these occasions.

Legislative developments

AML/CTF Act 2006

The Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 was introduced to Parliament on 1 November 2006 with the purpose of:

- improving Australia's existing anti-money laundering and counter-terrorism financing arrangements
- meeting higher international standards to protect Australian businesses from being used for money laundering and terrorism financing, and
- making it harder for criminals to use the profits of crime and for individuals or groups to receive money to carry out terrorist acts.

After a period of debate the above Bill was passed by both houses of Parliament and came into force on 12 December 2006, as the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act).

The AML/CTF Act imposes new obligations on reporting entities in respect of identification, verification and ongoing monitoring of customers, reporting suspicious matters and financial transactions above a set threshold, ensuring customer information accompanies international funds transfer instructions, and record keeping obligations.

These requirements will be progressively phased in over a two year period, so as to allow affected businesses sufficient time to implement necessary compliance and reporting measures.

In addition to putting in place a legislative framework to give effect to these objectives, the AML/CTF Act also formally recognised a range of government bodies as being 'designated agencies' with strictly limited and controlled access to data which is gathered by the Australian Transaction Reports and Analysis Centre (AUSTRAC).

AUSTRAC is Australia's AML/CTF regulator and financial intelligence unit and by virtue of the function it performs is a pivotal player in identifying and suppressing the financing of terrorism.

While AUSTRAC is not a member of the AIC per se it has developed linkages with some elements of the AIC, most notably ASIO, given their common interest

in identifying and suppressing terrorist related financing.

The fact that AUSTRAC has a relationship with ASIO is a matter of public record and the exchange of information between the two bodies is regulated by a long-standing MOU. ASIO's compliance with the requirements of its MOU with AUSTRAC is monitored by my office.

ASIO and IGIS were each listed as being a 'designated agency' in the AML/CTF Act.

AML/CTF Amendment Act 2007

The introduction and passage of the AML/CTF Act was a large undertaking, and not all that was proposed to be done could be achieved by the passage of that Act.

As a consequence, the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2007, was introduced to Parliament on 15 February 2007, for the purpose of making technical amendments to the AML/CTF Act and six other Acts.

One of the more significant amendments made as a consequence of the *AML/CTF Amendment Act 2007* (AML/CTF Amendment Act) being passed was to make ASIS a 'designated agency' with access to financial transaction records maintained by AUSTRAC, and to enable ASIS to communicate such information to foreign intelligence agencies where appropriate.

This amendment brought ASIS into line with ASIO which, as described above, has had a long standing formal relationship with AUSTRAC.

As a consequence of the passage of the AML/CTF Act and the AML/CTF Amendment Act, ASIO is presently reviewing the terms of its MOU with AUSTRAC, while ASIS is developing a MOU.

I will review the terms of my existing arrangements with AUSTRAC, and the inspection activities conducted by this office, in the light of these developments.

Inspector-General of Intelligence and Security Act 1986

The AML/CTF Act and the AML/CTF Amendment Act made amendments to section 22 and section 25A of the IGIS Act. These were essentially technical amendments designed to ensure that appropriate

reporting of inquiry and inspection activities could be carried out.

I also began discussions with PMC (as the Department of State for the portfolio), about possible further amendments to the IGIS Act.

The amendments I have proposed are intended to plug minor gaps in my jurisdiction, correct minor drafting anomalies, or provide me with additional flexibility in certain circumstances.

The changes I have in mind are technical and minor in nature, do not unduly hinder me in achieving the objectives of my office pending amendment action, and I expect they will go forward in a portfolio bill in due course.

I am also contemplating whether to recommend some other, more substantive amendments to the IGIS Act. These possible amendments, which have been informed by my experiences during my first term as IGIS, require further thought, research and development before they are brought forward for formal policy consideration and approval.

Privacy Legislation Amendment (Emergencies and Disasters) Act 2006

The Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006 was introduced to Parliament on 13 September 2006, passed through both Houses on 28 November 2006 and was assented to on 6 December 2006.

The Act was developed in the wake of the 2004 Boxing Day tsunami disaster, to overcome concerns that a too strict application of the *Privacy Act 1988* (the Privacy Act) inhibited the capacity of some agencies to respond quickly and flexibly in the face of a crisis involving mass casualties and missing persons.

The Act provides for the readier flow of personal information by and between government agencies when an emergency declaration has been made by either the Prime Minister or the Attorney-General, by temporarily relaxing statutory confidentiality or secrecy provisions, excepting where a 'designated secrecy provision' is binding upon the IGIS and/or the intelligence agencies.

Relevant legislation applying to the IGIS and the intelligence agencies already provides the agency heads with a measure of discretion about the release of information in emergency situations, although

this Act made some minor amendments to section 18 of the ASIO Act to ensure the Director-General of Security has similar flexibility.

Crimes Legislation Amendment (National Investigative Powers and Witness Protection) Bill 2006

In addition to being affected by legislation which passes through the Parliament, my office is frequently consulted on, or pays close attention to, draft legislation which may affect the office or the AIC.

One such bill upon which I was consulted as it was being developed was the Crimes Legislation Amendment (National Investigative Powers and Witness Protection) Bill 2006, which was introduced into Parliament on 29 November 2006.

One of the purposes of this Bill is to expand existing national model legislation to protect the identity of covert operatives who give evidence in court, by extending the scheme to include protection for security and intelligence officers and other authorised persons (such as foreign law enforcement officers) granted an assumed identity.

The Bill further proposes that ASIO and ASIS be required to make an annual report to the IGIS, as soon as practicable after the end of each financial year, on the extent to which they have authorised the use of assumed identities and or used witness identity protection certificates, and cognate information relevant to their use.

The requirement to make a report on the use of witness protection certificates is naturally a new requirement, but reflects the existing procedure set out in section 15XUA of the *Crimes Act 1914* in relation to assumed identities.

This Bill was still under consideration at the conclusion of the reporting period.

Human Services (Enhanced Service Delivery) Bill 2007

Another bill upon which I have been consulted and in which I have a potential functional interest is the Human Services (Enhanced Service Delivery) Bill 2007.

The genesis of this Bill lies in an announcement made by the Australian Government on 26 April 2006 that it planned to introduce a new access card for use in the administration and payment of

various health and social service benefits, that the card would utilise smartcard technology and that the card was expected to replace up to 17 cards that are currently used to access Australian Government health, social service and veteran's benefits.

The Government introduced a Bill in February 2007 which detailed those matters which needed to be included in the first tranche of legislation to introduce the access card. On 15 March 2007, the Minister for Human Services accepted a recommendation from the Senate Finance and Public Administration Committee to consolidate all proposed tranches of the access card legislation into a single consolidated Bill. In the period since, the Department of Human Services has been working assiduously to develop a successor to the original bill.

My interest in the access card principally lies with what access, if any, agencies such as ASIO or ASIS should have to information which is collected for, or contained on, the proposed access card, and if access is to be provided, how this access is to be regulated and monitored.

Development of a replacement Bill to create the proposed access card was on-going at the completion of this reporting period.

Telecommunications (Interception and Access) Amendment Bill 2007

In my annual report for 2004–05, I provided some basic background information on a review of the then *Telecommunications (Interception) Act 1979* (T(I) Act), which was conducted by Mr A S Blunn AO.²⁹

The purpose of the Blunn Review was to examine the adequacy of the regulation of communications which was provided for under the then T(I) Act, balanced against:

- the objective of protecting the privacy of users of the Australian telecommunications system
- the assistance that access to the content of telecommunications offers in the investigation of serious crime and threats to security, and

- the objective of providing certainty to agencies seeking access to the content of communications for investigative purposes and for users of the Australian telecommunications system.

The Government responded to Mr Blunn's recommendations by introducing a first tranche of changes via the *Telecommunications (Interception) Legislation Amendment Act 2006*, with the intention of introducing a second tranche at a later date.

This first tranche of legislative changes covered such matters as stored communication warrants and B-Party intercepts and were summarised in my previous annual report.³⁰

The Telecommunications (Interception and Access) Amendment Bill 2007 was introduced to Parliament in June 2007, to give legislative effect to those of Mr Blunn's recommendations which were not dealt with in the earlier legislation.

The Senate referred the provisions of this Bill to the Senate Standing Legal and Constitutional Affairs Committee on 21 June 2007 for inquiry and report by 1 August 2007.

I made a submission to this Committee on 11 July 2007, but as this submission was sent following the conclusion of this reporting period I have not included it in this report, but it is accessible via the Committee website.³¹

Statement of Procedures – warrants issued under Division 3 of Part III of the ASIO Act 1979

The Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2002 inserted a new Division into Part III of the ASIO Act 1979, which provided for questioning, and questioning and detention warrants.

Several sections of the amending Act required the development of a written statement of procedures (namely a 'protocol') to be followed in the exercise of such warrants and provided that no warrant of this kind could be issued until the protocol was tabled in Parliament.

²⁹ IGIS Annual Report 2004–2005, Canberra, October 2005 p. 5.

³⁰ IGIS Annual Report 2005–2006, Canberra, October 2006 p. 14.

³¹ The submission is located at the following website (as at 14 August 2007) <http://www.aph.gov.au/senate/committee/legcon_ctte/telecommunications_interception/submissions/sub14.pdf>.

The background to the development of the protocol and a copy of the protocol were included in my first annual report as IGIS.³²

Due to a technical oversight this protocol lapsed in September 2006 and had to be remade. The remade protocol is substantially the same as the previous protocol but has been retitled as a "Statement of Procedures" and incorporates clearer headings and a slightly revised internal numbering system (to permit for some introductory remarks about the commencement of the procedures and the revocation of the previous protocol).

The new 'Statement of Procedures' was issued by the Attorney-General on 16 October 2006, and has been added to the Federal Register of Legislative Instruments. I have attached a copy of the 'Statement of Procedures' as Annex 4 to this report.

Contributions to public sector governance

Membership of the Security Legislation Review Committee

In October 2005 the Attorney-General established the SLRC, under the chairmanship of a retired judge of the NSW Supreme Court, the Hon Simon Sheller AO QC, to review the operation, effectiveness and implications of six pieces of legislation relating to terrorism which were introduced or amended in 2002 and 2003. I was appointed to the SLRC as an *ex-officio* member.

While the work of the SLRC itself was completed during the previous reporting period, as discussed elsewhere in this chapter I appeared before PJCS inquiries in July 2006 and April 2007 to discuss the findings of the SLRC.

I continue to closely monitor developments relating to the recommendations of the SLRC and will continue to contribute my thoughts to appropriate forums, on cognate issues, as appropriate.

Membership of the Administrative Review Council

The Attorney-General 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. While the announcement coincided with my reappointment as IGIS, the appointment has been made to me in a personal rather than official capacity.

During the reporting period I participated in a seminar to mark the 30th anniversary of the founding of the ARC, attended four ARC meetings, and participated in two ARC related teleconferences. Although not all matters considered by the ARC relate directly to the AIC, many issues under consideration do, and there are advantages to my role as IGIS from my participation in ARC meetings and functions.

Providing advice on the outcome of complaints investigations

In the early part of 2006 I informally canvassed the views of the Australian Public Service Commissioner, the Privacy Commissioner, and the Commonwealth Ombudsman as to whether a too strict interpretation/ application of the Privacy Act was inhibiting the capacity of various public sector agencies to provide comprehensive 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.

I had raised this issue in the light of a particular IGIS investigation but as IGIS Act inquiries are not typical of those conducted across the public service (due to the frequent interplay of security as well as privacy issues), thought it best to informally seek the views of experts in this field, as to whether this was an area of actual or potential concern.

These informal soundings led to the creation of a small working group to which my office contributed during this reporting period, which is examining this issue.

ALRC review of the Privacy Act 1988

On 31 January 2006 the Attorney-General provided a reference to the ALRC for an inquiry into the extent to which the Privacy Act and related laws continue to provide an effective framework for the protection of privacy in Australia. This inquiry is being led by ALRC Commissioner, Associate Professor Les McCrimmon.

³² IGIS Annual Report 2003-2004, Canberra, October 2004, pp. 5-6, and Annex 2.

I met with Professor McCrimmon on 15 March 2007, to discuss a range of privacy related issues pertaining to the AIC, with a focus on how the privacy rules and guidelines which exist in the AIC are interpreted and applied.

The ALRC plans to release a discussion paper on this review in September 2007, with the final report and recommendations due to be delivered to the Attorney-General by 31 March 2008.

ALRC review of Client Legal Privilege and Coercive Investigative Powers

On 29 November 2006, the Attorney-General asked the ALRC to inquire into the application of legal professional privilege to the coercive information gathering powers of a number of specified Commonwealth bodies.

Although the OIGIS was not one of the Commonwealth agencies specified in the terms of reference provided to the ALRC, my office does possess strong coercive powers, and this being so, the President of the ALRC, Professor David Weisbrot AM, invited a submission on this subject from my office.

I provided a submission in response to Professor Weisbrot's invitation (see Annex 5 of this report) and also visited the ALRC offices in Sydney on 26 June 2006, where I spoke to the contents of my submission.

Performance

Resource allocation

As the AIC grows in size and complexity, the demands which are being placed on OIGIS are also increasing in number and difficulty. While there has been appropriate budgetary recognition in recent years that if the AIC grows, OIGIS should also grow, the challenge is to ensure that the additional resources are being used in a way which best meets the objectives of the office.

In the very early years of OIGIS's existence, significant resources were devoted to processing complaints and less time and effort was spent on inspection activities. There was a pent up demand from aggrieved individuals who wished to safely ventilate their concerns, and OIGIS provided a forum for these concerns. It was also the case that some of the intelligence agencies, not having had any previous experience in dealing with an external oversight body were wary of providing ready access to their records and methods until the relationship had developed and matured.

The Commission of Inquiry into ASIS conducted by the Hon. Gordon J. Samuels AC, QC and Mr Michael H Codd AC, in 1994-95, took evidence from the then Inspector-General, Mr Roger Holdich AM, on the allocation of resources within OIGIS and the focus of his work. At the time of his giving evidence, Mr Holdich estimated that handling complaints had come to occupy 75-80% of his time.³³

The Commissioners were critical of this, especially the amount of time then being devoted to handling what amounted to AIC agency staff grievances:

*"The amount of time IGIS has devoted in recent years to his function in relation to inquiries into staff grievances has, in our view, distracted him from the general monitoring and oversight functions, and unduly reduced the attention which should have been given to these functions. We regard this as a matter of concern."*³⁴

The Commissioners then proposed that the IGIS's capacity to review staff grievances be limited:

*"... to allow IGIS to concentrate most of the energies of the office on the monitoring and oversight functions which we will be recommending be expanded in their coverage."*³⁵

Subsequent to the Commissioners making their report, all Inspectors-General have sought to give effect to this recommendation and ensure there is focus on regular and targeted inspection activities.

In the last five years, more of the time of the office has been directed towards assisting in the development of legislation affecting the AIC, and subsequently reviewing the impact of that legislation.

During this reporting period the resources of the office (apart from those necessary for corporate tasks associated with being a separate agency) were allocated roughly as follows:

- 60% monitoring the day-to-day activities of the intelligence community
- 35% devoted to handling complaints or inquiry related activities, and

³³ Quoted in the Report of the Commission of Inquiry into ASIS (Public Edition), Australian Government Printing Service, Canberra, March 1995, paragraph 9.18.

³⁴ *Ibid.*, paragraph 9.21

³⁵ *Ibid.*, paragraph 9.21.

- 5% on policy development, legislative review and presentations.

I can assure readers that, while I take the complaints and inquiry functions of the office very seriously, I will continue to focus the work of OIGIS on conducting regular monitoring and inspection activities.

Outcomes and outputs

In program budgeting terms, OIGIS has one outcome and one output. The fact that the office has only one outcome and output reflects its small size and the relatively narrow focus of our activities (i.e. 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”.³⁶

This outcome is achieved through a single output which is to “inspect, inquire into, and report on, the activities of the intelligence and security agencies.”³⁷

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 unique role and functions of the OIGIS:

- 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 commencement of the reporting period four preliminary inquiries remained open. Two of these inquiries related to the activities of ASIO, and two were concerned with ASIS. Three of these four preliminary inquiries were finalised in the early months of the reporting period, while the fourth was concluded early in 2007.

In addition to the four matters referred to above which were carried over into the reporting period, OIGIS received 149 approaches from individuals with new or continuing complaints against a nominated agency³⁸. I also commenced three own motion inquiries. This global figure of 152 compares with 99 complaints/inquiries in the previous reporting period.

The 152 approaches described above can be broken down as follows:

- 3 own motion inquiries, compared to two in the previous reporting period
- 10 new complaints leading to preliminary or full inquiries. Of these inquiries three remained open as at 30 June 2007. In the previous reporting period 18 complaints led to preliminary or full inquiries³⁹
- 28 approaches seeking a previous complaint be reviewed or a new inquiry be conducted, compared to 19 in the previous reporting period
- 37 new complaints where an agency was specifically identified, which were dealt with administratively. There were 34 such complaints in the previous reporting period,⁴⁰ and
- 74 complaints about alleged delays by ASIO in conducting immigration related security assessments that were handled administratively rather than as preliminary or full inquiries. This compares to only 17 complaints in the 2004–2005 reporting period and 26 such complaints in 2005–2006.⁴¹

³⁶ PM&C Portfolio Budget Statement 2007–08 – Office of the Inspector-General of Intelligence and Security, p. 169, (available at <<http://www.pmc.gov.au/accountability/budget/2007-08/pbs/oigis.pdf>> accessed on 12 September 2007).

³⁷ *Ibid.*, p. 169.

³⁸ For the purposes of this analysis I have construed the 37 form-letters we received in respect of the security assessment of Mr Rhuheh Ahmed as comprising one complaint rather than 37 separate complaints.

³⁹ Tabular information relevant to these two dot points is provided at Annex 1, Table 1.

⁴⁰ Summary information relevant to these two dot points is provided at Annex 1, Table 2.

⁴¹ Summary information relevant to this dot point is provided at Annex 1, Table 3.

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

Since the creation of the office in 1986–87, the average number of new matters or complaints which were formally pursued as preliminary or full inquiries averages 20.75 per annum.

In the five year period between 2001–2002 and 2005–2006, the average was 26.2 per annum.

In this reporting period I pursued 13 matters as preliminary or full inquiries (i.e. 3 own motion inquiries and 10 complaints).

The decline in the number of preliminary and full inquiries I conducted in 2006–2007 is linked to how I have chosen to handle an upsurge in complaints I have received about the timeliness with which ASIO is conducting security assessments on applicants for various forms of visas.

In the 2004–2005 reporting period, I received a total of 31 complaints on immigration related matters. I pursued 14 of these as preliminary inquiries and processed 17 complaints administratively.

In the 2005–2006 reporting period, I received a total of 34 complaints on immigration related matters. I pursued 6 of these as preliminary inquiries, 2 as full inquiries, and processed 26 complaints administratively.

In the 2006–2007 reporting period, I received a total of 76 complaints on immigration related matters. I pursued two of these as preliminary inquiries and processed 74 complaints administratively.

As has been explained elsewhere in this report, there are a number of reasons why we are receiving an increasing number of immigration related complaints. One is the pressure which workload increases have placed on ASIO. Another is that it seems an increasing number of migration agents or networks are now aware of the existence of our office and will contact us directly if they believe there is an unreasonable delay in the processing of their client's visa application.

When our office first experienced an upsurge in immigration related complaints in the 2004–05 reporting period, I pursued 14 of these complaints as preliminary inquiries. Going through this formal process, while appropriate, was time consuming as in each case the Director-General of Security needed to be briefed and respond to my request for information.

In consequence of the time being taken, I decided to handle all such complaints administratively in the first instance, unless there is a clear need to pursue the complaints more formally. This is usually to the benefit of the complainants, as administrative inquiries can be addressed in a speedier manner.

I will continue to closely 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 65 other 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 we try to process complaints about AIC agencies which do not proceed to preliminary or full inquiry within a few days.

In addition to the 156 cases identified above (i.e. four preliminary inquiries carried over from the 2005–06 reporting period, 149 new or resumed complaints and three new own motion inquiries), 30 other individuals contacted the office with concerns which did not directly refer to or involve an AIC agency (compared to 61 in 2005–06). Each of these contacts was handled administratively.

It is sadly the case that a significant proportion of these 30 contacts were from individuals who were clearly suffering from delusional or imaginary concerns.

In addition to persons with manifestly delusional concerns we also received contact from persons who wished to raise matters which fell outside of our jurisdiction, or otherwise sought to provide "tip-off" information.

In the case of matters falling outside of our 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).

All tip-off information we receive which may be at all credible is 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 ph. **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 this office.

Timeliness

It is not 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 a complaint is disposed of.

Such factors include but are not limited to, the complexity and range of issues raised by the complainant, the accessibility of relevant files and documents to be reviewed, the availability of agency staff, and fulfilling other requirements associated with procedural fairness. Notwithstanding the above, it is our objective to minimise the time taken to complete inquiries.

In the five years between 1 July 2002 and 30 June 2007, the average time taken for inquiries to be completed was 108.95 days.

The average time taken to finalise preliminary and full inquiries in the 2006–07 reporting period was 95 days, compared to 81 days for the previous year.

While I am naturally disappointed that the time taken to finalise preliminary and full inquiries increased, on average, by 14 days per case, these delays were frequently caused by factors over which this office had no direct control. Notwithstanding this, I will strive to improve our timeliness in the 2007–08 reporting period, to the maximum extent possible.

Acceptance of recommendations

It is most uncommon for an agency to reject recommendations of the Inspector-General. This is because recommendations for change are not made lightly, generally involve prior consultation and hopefully reflect a common sense response to a particular issue or concern.

In all instances where the Inspector-General made formal recommendations in reports of inquiries which were concluded during the 2006–07 reporting period, these were accepted by the relevant agency.

Responsiveness to issues raised

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

During 2006–07, I made a number of suggestions for procedural changes and reforms. These suggestions were generally accepted and acted upon.

I can also advise that the intelligence and security agencies continued to seek the views of my office on draft policies and procedures.

Where I have an interest or a concern about a particular activity, I do not hesitate to seek a 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 continue to be encouraged by the willingness of the agencies to seek and accept input from this office and believe that it demonstrates a commitment on their part to conduct their activities legally and with propriety.

Level of assurance

The number of persons contacting my office is probably greater now than at any time during which OIGIS has existed.

This does not mean that the AIC agencies are running out of control, or that their activities are causing more offence, but is most likely a by product of the AIC's increasing size, its greater visible engagement with the community, and its increasing operational tempo as it seeks to respond to new challenges. It may also reflect greater knowledge of the existence of my office.

Certainly I do not believe that the decline in the number of matters which I pursued as preliminary or full inquiries is the result of lack of awareness about this office. 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 naturally sit outside the AIC.

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 presence on the Internet 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. We are currently redesigning our website to make it even more accessible and user-friendly.

As I have noted previously, as various community groups achieve a greater understanding of the role of this office and hopefully achieve greater comfort levels in approaching a government office on matters affecting security, it is possible that complaints to my office will rise rather than decrease.

Summary

As a result of the various inspection and inquiry activities conducted by this office during the 2006–07 reporting period a small number of instances were found where the agencies acted beyond their authority.

While any instance where an intelligence agency has acted without authority is a matter for concern, the instances detected were almost invariably due to technical or human error and appropriate remedial action was either already initiated by the affected agency, or put in train immediately an agency was made aware of a problem. There was no evidence that the intelligence and security agencies, or individual members of the agencies, have knowingly acted, or wish to act, beyond their authority.

Based on the various monitoring, inspection and inquiry activities undertaken by my office during 2006–07, I am satisfied that there is no evidence of enduring systemic deficiencies that would lead to breaches of propriety, the law, or the human rights of Australians.

I was also satisfied that the agencies were committed to acting legally and with propriety and respect for human rights, and that apart from a very small number of genuine errors, had complied with their obligations.

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.

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 cooperate with Australian law enforcement agencies to assist with criminal investigations that have a national security dimension.

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

Continued growth and expansion

In recognition of the complexity and unpredictability of the threat environment and the continued increase in the volume and pace of information flows, the Government has provided substantially increased resources to ASIO over a number of years, so that it might respond effectively to the challenging security environment in which it operates.

The significant boost to ASIO's funding in respect of its core business activities has been directed towards enhancing its capability to respond to threats from various forms of extremism, espionage, foreign interference, the proliferation of weapons of mass destruction, and other forms of politically motivated violence which threaten Australians and Australian interests. The means by which ASIO is doing this are many and varied but include:

- the recruitment and training of significant numbers of new staff, with skill sets appropriate to ASIO's current and future needs

- adopting strategies to retain valued staff and minimise churn
- internal organisational restructuring, so that appropriate management focus and oversight is directed to enduring interests, as well as to new areas of interest or concern
- placing more functional activities on a 24/7 basis, so as to facilitate better monitoring and improved responsiveness
- increasing intelligence collection and assessment capability
- further increasing surveillance capability
- managing a continuing rise in border security related activities, and
- bolstering technical capabilities (through the upgrading of its information and communications technologies and improving connectivity with various customer agencies).

New Headquarters

A logical corollary of the growth in the number of persons employed by ASIO is that this has placed significant stress on its existing accommodation and facilities.

In recognition of these pressures, the Government announced in the 2006–07 Commonwealth Budget papers that in principle approval had been granted for a new building to be constructed in Canberra to house ASIO's central office, as well as their current co-tenants ONA.⁴²

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 2005–06.⁴³

My position remains that either I or a senior OIGIS staff member 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.

However, as indicated in the ASIO Annual Report for 2006–07, no warrants were issued under either section 34E (questioning) or section 34G (questioning and detention) of the ASIO Act during the reporting period.

Attorney-General's Guidelines

Section 8A(1) of the ASIO Act provides that the Attorney-General may, from time to time, issue to the Director-General of Security written guidelines which are to be observed in the performance by ASIO of its functions or the exercise of its powers.

In late 1992 the then Attorney-General, the Hon. Michael Duffy, issued two guidelines to the Director-General of Security concerning the performance by ASIO of its functions relating to:

- obtaining intelligence relevant to security, and
- politically motivated violence.⁴⁴

These guidelines are extant and have not been amended since they were issued.

My immediate predecessor and I have periodically suggested that there would be merit in reviewing these guidelines, to bring them up to date, and so that the current Attorney-General might have the opportunity to endorse them.

During this reporting period ASIO devoted resources to this task, with a view to rolling the existing guidelines into a single more user friendly document, which reflects contemporary practice within ASIO.

I have been consulted as a part of this review process and discussion was on-going as at the completion of the reporting period.

Special briefings

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. This is a natural by-product of the work

⁴² *Budget Funds Enhanced Resourcing for ASIO*, press release 075/2006 dated 9 May 2006 issued by the Attorney-General, the Hon Philip Ruddock MP.

⁴³ IGIS Annual Report 2003-2004, Canberra, October 2004 pp. 15-18; 2005-2006, Canberra, October 2006 pp. 11-12.

⁴⁴ These guidelines can be accessed via the ASIO website <<http://www.asio.gov.au>> (accessed 15 August 2007).

we perform and should not be read as suggesting that information is being deliberately kept from me or my staff.

On those occasions when I require special or additional briefing on a particular subject I will write to the Director-General of Security seeking his assistance, or if the issue is more pressing, directly contact the relevant senior manager.

Mr Paul O'Sullivan has not placed any restrictions on who I might seek briefings from, or to whom I might speak within ASIO. Indeed, I am pleased to advise that Mr O'Sullivan has actively encouraged his staff to take the initiative to brief me on topical issues, rather than waiting for my request.

Although it is not appropriate for me to detail every such briefing, during this reporting period I met with senior ASIO officers on at least 28 separate occasions to discuss issues such as the long term retention and management of electronic records, inter-agency relations, internal audit procedures, the likely impact of proposed legislation, 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 staff 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 as IGIS. 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 15 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.

I also met on several occasions with senior ASIO training staff to discuss the curriculum they have developed for trainee intelligence officers, and to identify opportunities for myself or OIGIS staff to observe or participate in relevant training opportunities.

Inspection activities

General scope

ASIO has a strong domestic focus and is the AIC agency which is most likely to directly interact with members of the Australian public.

Given that ASIO devotes significant resources to activities which have a domestic focus, it is logical and appropriate that ASIO's intelligence collection activities should be subjected to more intensive and more frequent review by my office than the other members of the intelligence community.

During this reporting period we conducted 56 inspection visits to ASIO's various offices compared to 48 separate inspections in the previous reporting period.

It has been my practice since becoming IGIS to write to AIC agency heads towards the end of each calendar year, with a proposed visits and inspections schedule for the following calendar year. In advising the agency heads of this schedule, I set out each inspection activity which we plan to undertake but retain the flexibility to alter the schedule as need dictates.

I also write to the relevant agency head following each inspection, so that they have a record of our visit and that I have an additional vehicle by which I can raise any issues or concerns.

The responsiveness of the Director-General of Security to my various letters was slower in 2006–07 than in previous years but the replies I received were generally detailed and considered.

I do not read anything sinister into the increased length of time taken for the Director-General to respond to some of my correspondence, accepting that he is an extremely busy person with a large number of staff and activities to administer and that his responses sometimes need to be drawn from disparate parts of ASIO prior to finalisation and dispatch.

I will nonetheless have regard in the coming year to the timeliness with which responses to my queries are received as one indicator of the on-going health of ASIO, and more specifically the health of the relationship between our respective agencies.

Range of current and new inspection activities

As with previous years this 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, use of assumed identities and liaison with law enforcement agencies.

In addition to these regular tasks we also instituted two new inspection activities, one relating to the exchange of information about Australian persons to foreign liaisons, and the second involved reviewing the operational activities of a particular section in ASIO. I also set the wheels in motion to set up a monthly meeting with senior ASIO officers.

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

Project to review the exchange of information with foreign liaisons

In an age of high speed modern communications and relatively easy international travel there is a very clear need for agencies such as ASIO to share information with their international counterparts, so that they might keep tabs on persons of security interest.

In order for ASIO to meet its charter obligations in respect of security there will be occasions when it needs to respond to requests for information about Australian persons made by foreign intelligence services or law enforcement agencies, and equally there will be occasions when it is appropriate and reasonable for it to proactively release information of this kind to their foreign counterparts, seeking information in return.

In mid-2006, I wrote to the Director-General of Security proposing to inspect ASIO's records relating to the release of information about Australian persons to foreign liaison services.

No specific Australian case prompted me to explore this subject, but it is an area where conceivably some sensitive issues could arise.

Prior to commencement of this pilot project, the relevant functional area in ASIO with responsibilities in this area internally reviewed their procedures and determined that they could be improved. Following this internal review development work was commissioned on an electronic template to ensure

a consistent approach to the release of information about Australian persons to foreign liaisons. I was invited to provide any thoughts or input to the proposed new processes.

During the reporting period, my staff examined relevant records from some of ASIO's liaison offices. We found that the new measures introduced by ASIO were working well.

I am appreciative of the open and proactive manner in which ASIO responded to this proposed inspection activity, and the speed of ASIO's response when they realised that their record keeping practices in the area could and should be improved.

I propose to conduct a further review in the second half of the next reporting period to check that standards are being maintained.

Review of operational activities

During this reporting period I utilised the services of a former Inspector-General, Mr Bill Blick on a consultancy basis to supplement our various inspection activities.

One of the activities I asked Mr Blick to undertake was to conduct a thorough review of the operational activities of a particular section within ASIO. No particular incident served as a catalyst for this activity, rather I judged it timely and prudent that the activities of this section be subject to external review.

I was satisfied with the detailed responses provided to the various queries we posed as a result of this inspection work.

Proposed introduction of monthly meetings

As indicated above, towards the later part of this reporting period I began moves to set up monthly meetings with senior ASIO personnel (at the Deputy Director-General/Division Head level).

The purpose of these meetings will be for me and these officers to meet regularly to discuss significant findings or issues arising out of our inquiry and inspection activities, to exchange views on other issues in which we have a common interest, and to be briefed on new projects. These meetings will also provide a mechanism for me to receive updates on outstanding correspondence, should there be a need to do so, and for me to respond to any requests for feedback or comment levied on my office.

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)
- postal and delivery service articles

As the exercise of these special powers will not ordinarily 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, and this objective was achieved in 2006–07.

Our inspections go beyond simply seeing and ticking off each warrant. We also 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 am pleased to report that the quality of the warrant requests which go to the Attorney-General have been of a consistently high standard.

I am also satisfied that in each case where a special powers warrant was issued in 2006–07 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 an accurate, objective and timely manner, and
- maintained the key accountability documents on the relevant files for examination by OIGIS staff.

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

B-Party warrants

As detailed elsewhere in this and my previous annual report⁴⁵, Parliament passed the *Telecommunications (Interception) Amendment Act 2006*, to give effect to a tranche of recommendations contained in the Blunn Review of the legislation. One change was to rename the Act as the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

One substantive change brought about by the passage of this Amendment Act was the insertion of provisions which enable ASIO to seek telecommunications interception warrants in relation to so-called “B-Party” services.

A “B-Party” service is a telecommunications service not owned by a person of security interest but which the person of security interest is likely to be in contact with.

A “B-Party” telecommunications interception warrant can only be sought where all other practical methods of identifying the telecommunications services of a person of interest have been exhausted, or it is not possible to intercept the services of a person of interest.

The use of “B-Party” warrants is contentious because it inherently involves a potential for greater privacy intrusion into the activities of persons who may not be involved in matters of security interest, or the commission of an offence.

Finding an appropriate balance between individual liberties and protecting the country from potential security threats is not easy. In recognition

of the extra sensitivity of intercepting the telecommunications of individuals who are at one remove from a person of specific security interest, the Parliament determined that “B-Party” warrants should only be available for a maximum of 90 days rather than 180 days, as is the case with the other types of telecommunications interception warrants for which ASIO has access.

In addition to “B-Party” telecommunications interception warrants being of shorter duration (and thus subject to more regular review should they be renewed), I expressly stated in my previous annual report that:

“We will be particularly vigilant in monitoring the use of so-called “B-Party” warrants which have been provided for as a result of recent amendments to the TIA Act.”⁴⁶

I can advise that ASIO did utilise these new provisions during this reporting period, and that my staff had access to all relevant associated documentation when conducting our regular warrants inspections.

Precise figures of the number of occasions which recourse was made to B-Party warrants cannot be included in this report (for security reasons), but I can say that this type of warrant was used sparingly, and on those occasions when such warrants were sought, my staff and I were 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.

Unauthorised telecommunications interception

A review of our inspection records reveals that during this reporting period there was one instance where an error or fault which was within ASIO’s control led to unauthorised telecommunications interceptions occurring. This compares with three such instances during the previous reporting period.

In addition to the singular instance referred to above, my staff identified, or had brought to their attention, three other instances where technical or human error within ASIO’s control had the potential to cause unauthorised collection to occur, but such

⁴⁵ IGIS Annual Report 2005-2006, Canberra, October 2006 p. 14.

⁴⁶ *ibid.*, 55.

collection did not eventuate. This compares with 10 such instances of this occurring during the previous reporting period.

While any instance where unauthorised interception occurs, or has the potential to occur, is serious I am very pleased with the improvement which was achieved during the reporting period.

This achievement is even more commendable when one considers that the overall number of services intercepted under telecommunications interception warrants each year is rising, and the legal framework under which warrants are issued is more complex.

In addition to the above cases we also identified or had brought to our attention five instances where the actions of bodies external to ASIO resulted in, or could potentially have resulted in, unauthorised collection occurring. This is the same rate as occurred in the previous reporting period.

The five cases identified were the product of simple human error or minor technical glitches which led or could have led to an undesirable outcome.

In each instance where human or technical failure led to unauthorised collection (either by ASIO or an external body), the intercepted data was destroyed and all related records purged from ASIO's databases.

In those cases which arose from a technical failure of some sort, appropriate technical solutions were identified by ASIO and/or the external service provider with which ASIO had dealings.

While any instance where unauthorised interception has occurred, or has the potential to occur, is a serious thing, the incidence of detected error is extremely low when considered against the number of services for which special powers warrants have been granted.

ASIO is very ready to devote resources to effecting technical solutions in cases where telecommunications interception errors arise. This is because ASIO is particularly conscious of the consequences which would flow were it to collect and use intercept without lawful authority, and because of the potential for valuable intelligence to be lost, if a "wrong" number or service is being intercepted.

Interception management systems

In addition to our very regular review of ASIO's warrant documentation files, we also periodically interrogate ASIO's interception management systems.

We undertake these checks to independently satisfy ourselves that collection is only occurring against telecommunications services which are listed on properly authorised warrants, and within the specified collection period.

I am pleased to advise that none of the checks we conducted during this reporting period revealed any instances of inappropriate or otherwise unauthorised collection.

Other issues arising from warrant reviews

In the course of our regular warrant inspections we identified a small number of minor administrative errors or inconsistencies. These errors included the accidental incorrect dating of warrant requests or authorisation lists but not the warrants themselves. These errors or inconsistencies had no effect on the legality or validity of the warrants in question.

In past years where we have identified dating inconsistencies which could give rise to confusion as to when a warrant was actually signed, ASIO's practice has been to err on the side of caution and chose the earliest date on which such a request could have been submitted (even if no special powers were actually exercised on the day in question), and use that as the basis for calculating the expiry date for the warrant. This is a prudent approach which I strongly support.

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 TIA Act, 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 our attention one instance where the outcome of a telecommunications interception warrant was not provided to the Attorney-General within the requisite timeframe. ASIO provided a full explanation as to why this had occurred, indicating that it was a one off administrative error which was caused by an unusual confluence of events, and that relevant staff had been reminded to be more vigilant in the future. I accepted the explanation provided to me as both plausible and reasonable.

Over and above this it is noteworthy that ASIO brought this error to our attention rather than leaving us 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.

Approval to investigate – procedures

Staff employed within ASIO cannot commence an investigation into a person or organisation simply on a whim, or because their curiosity has somehow been piqued. Rather, a formal and auditable process must be followed.

The Attorney-General's Guidelines (referred to earlier in this chapter) set out in general terms the circumstances in which ASIO can go about obtaining 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 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 37 days. These inspections were conducted in Canberra and at ASIO's various interstate based collection offices.

During these ATI inspections we checked to see:

- 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.

Approvals to investigate – inspection results

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

Early in the reporting period I wrote to the Director-General of Security setting out in a single page those elements of the approval process which my staff and I pay close attention to when we conduct our inspections. The comments I made were linked back to specific references to the Attorney-General's Guidelines.

In writing to the Director-General I acknowledged that while many, if not most, of the approvals we review are of a high standard, I nonetheless thought it would be useful to set out my thoughts on several matters so as to encourage improvement in standards and consistency in approach across ASIO.

Overall, I was quite happy with the manner in which the approval process worked during this reporting period.

In previous years we noted a number of instances where ASIO's internal policy requirement that warrant operations be supported by a certain type of approval, or a different type of higher level approval, had not been met. I am happy to advise that the incidence of this occurring dropped markedly during the reporting period.

In the course of our inspections we had brought to our attention an instance where the Attorney-General had written to the Minister for Defence, in accordance with section 9(1A)(b) of the *Intelligence Services Act 2001* (ISA), seeking the issue of a ministerial authorisation (MA) to permit the collection of the foreign communications of an Australian person, on the grounds that the person in question is, or is likely to be, involved in an activity or activities that are, or are likely to be, a threat to security.

Even though there is no legal or policy requirement specifying that ASIO must also have in place an investigation approval, I advised the Director-General of Security that I thought that ASIO should do so in all such cases, as the issue of an MA conferred similar powers to a domestic telecommunications interception warrant, and all warrants are required to be supported by an investigative approval.

In a subsequent inspection we came across evidence of differing views within the AIC on the way in which section 9(1A) of the ISA should be interpreted and applied. Further discussion of this subject is provided elsewhere in this report.

In several inspections we noted that some officers were using the same form of words when putting limits on particular investigative activities. We actively seek to discourage the use of such 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.

We also noted several 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) but these were very much the exception and did not point to any systemic concerns.

The Attorney-General's Guidelines requires 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.

We found that in almost all cases reviews were completed prior to an approval being renewed, or within a reasonable period following their expiry.

ASIO and law enforcement agencies

ASIO naturally has quite close links to law enforcement agencies in all Australian jurisdictions.

These links are necessary to assist with security planning for major events such as APEC where Australia has obligations with respect to the protection of foreign dignitaries who visit Australia, and because there is often an overlap between persons who are planning for or engaged in criminal activities, and persons of security interest.

As has been the case for many years, whenever we visit any of ASIO's state offices we closely review ASIO's files which detail their interactions with locally based law enforcement agencies.

On the basis of the materials available during our inspection visits, I am satisfied that ASIO is committed to working cooperatively with local law enforcement, within the constraints imposed by the ASIO Act.

I am also satisfied that appropriate control measures exist to ensure that personal information on persons of security interest is only exchanged where there is a demonstrable need for this to occur.

Information obtained from AUSTRAC

As touched on in an earlier chapter of this report which reviewed significant legislative developments during the reporting period, the AML/CTF Act was passed by the Parliament in late 2006, received Royal Assent on 12 December 2006, and its provisions are being progressively introduced over a two year period.

The AML/CTF Act forms part of a legislative package which aims to improve Australia's anti-money laundering and counter-terrorism financing system to meet higher international standards, and to make it harder for criminals to use the profits of crime and for terrorists to receive money to carry out terrorist acts.

The AML/CTF Act provides a legal framework in which “designated agencies” are able to access information which is held by AUSTRAC, in strictly controlled circumstances.

ASIO and IGIS have both been made “designated agencies” for the purposes of the AML/CTF Act.

In ASIO’s case, access to AUSTRAC information assists the Director-General of Security to fully discharge his responsibilities consistent with the functions prescribed for ASIO under section 17 of the ASIO Act, whereas my office requires access to AUSTRAC information so that we might monitor that ASIO is complying with the conditions under which access to this information has been granted to it.

Prior to the AML/CTF Act coming into effect, ASIO sought and obtained access to AUSTRAC information within the legal framework established by the *Financial Transactions Reports Act 1988* (FTR Act).

In accordance with the terms of the standing MOU which exists between this office and AUSTRAC, I provided a certificate to the Attorney-General on 8 December 2006, stating that ASIO had complied with the requirements of the Attorney-General’s Guidelines, the FTR Act and the ASIO-AUSTRAC MOU during the 2005–06 reporting period.

During the current reporting period my staff conducted nine AUSTRAC related inspections at ASIO’s central office compared to six such inspections during the previous reporting period. My staff also reviewed relevant records in ASIO state offices whenever the opportunity presented itself.

In the course of the above inspections we identified a small number of minor procedural issues none of which were of material effect.

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.

Despite the understandable reserve ASIO has shown to date, I am nonetheless satisfied that ASIO should continue to have access to taxation information in strictly limited circumstances, as an investigative tool and/or as an aid to understanding the activities of persons of security interest.

Use of assumed identities

As has been our practice for many years, my office also periodically reviews ASIO’s assumed identity registers.

In conducting this review activity my staff and I review approximately 10% of all authorisations, variations and revocations, relating to assumed identities which had been processed during the reporting period.

The registers we review 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.

During this reporting period we conducted two inspections of the assumed identity registers, which was the same number as conducted during the previous reporting period.

On the basis of these inspections I am satisfied 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.

Archives

The Director-General of Security continues to provide my office with quarterly progress reports on ASIO’s performance in meeting its obligations under the *Archives Act 1983*.

These reports provide an indication of any trends which might be developing in relation to requested material, or possible difficulties in meeting high volume requests.

On the basis of the reports I have received from the Director-General, I am satisfied that ASIO's performance in meeting its obligations continues to be satisfactory.

Complaints and inquiries

As at 30 June 2006 I had two preliminary inquiries in train into complaints about ASIO, which I carried over into this reporting period. Both of these inquiries were concluded early in the reporting period.

The office conducted preliminary inquiries into five new complaints about ASIO in the reporting period compared to 11 in the previous period, and initiated full inquiries into three new matters, which is the same number as in the previous reporting period.

It should be noted that one of the full inquiries I conducted was prompted, in part, by the receipt of 37 letters of complaint. For statistical purposes I have counted this as being one inquiry/complaint rather than 37.

In addition to the preliminary and full inquiries briefly described above, the office received 119 other complaints specifically about ASIO, from individuals seeking to reopen former complaints, or making new complaints raising specific concerns (compared to 50 in 2004–05, and 71 in 2005–06).

Of these 119 complaints 74 were concerned with the timeliness with which ASIO processed immigration related security checks. My handling of these complaints is discussed below, followed by brief summaries of several other complaints I addressed during the reporting period.

Immigration related complaints handled administratively

There has been a noticeable increase in the reporting period in the number of complaints about the timeliness with which ASIO processes security assessments for immigration applications.

A total of 74 complaints were received in relation to 72 complainants in this reporting period. This compares with 32 complaints received in the previous reporting period. The complainants varied from permanent protection visa applicants to skilled migrant and spouse visa applicants. These complaints were lodged either by the complainants themselves, migration agents acting on their behalf,

or following a referral by another government agency.

Each of these 74 complaints received were, in the first instance, handled administratively, with two progressed further as preliminary inquiries. Matters handled administratively are actioned by making an informal inquiry of ASIO to verify that the case has actually been referred to ASIO by the Department of Immigration and Citizenship (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.

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.

A 100% increase over the past 12 months in complaints about ASIO's handling of immigration related matters has caused me to question ASIO regarding the timeliness of its processing of security assessments.

The time taken to complete a security assessment varies depending on the individual circumstances of the case. Some cases are more complex than others and therefore take longer to process than would otherwise be the case. Notwithstanding this, such a significant increase in complaints about timeliness has highlighted an issue which requires my continuing close attention.

ASIO has advised me that it is acutely aware of this issue and is taking remedial steps to address it by allocating additional resources and upgrading IT systems to improve timeliness.

Although it falls just outside the reporting period, it should be noted that on 8 July 2007 the Prime Minister announced a project to enhance the accuracy and speed of information passing between ASIO and DIAC which should lead to a significant improvement in processing timeframes.

Alleged delays in security assessments for Commonwealth employment

During the reporting period I received two complaints from members of the public who raised concerns about alleged delays by ASIO in the

processing of security assessments in respect of themselves.

The security assessments in each case were required as the complainants were applicants for designated security assessment positions within different Commonwealth agencies which each required the successful candidate to hold higher level security clearances.

The security assessment process is an integral part of the selection process for designated security assessment positions, and even if an individual is the preferred candidate after a merit based selection exercise, a formal offer of employment cannot be made until the security assessment process has been completed and the candidate meets all mandatory requirements (i.e. they are the holder of an appropriate level security clearance).

The complainants to my office suggested that they suffered disadvantage due to the length of time allegedly taken by ASIO to undertake and complete their security assessments.

Subsection 8(8)(c) of the IGIS Act, generally prohibits the IGIS from reviewing matters which fall within the jurisdiction of the Security Appeals Division (SAD) of the AAT. The SAD is empowered to review adverse and qualified security assessments which are made by ASIO, in respect of applicants for Commonwealth employment.

In each of the cases brought to my office, ASIO had not made an adverse or qualified assessment but was still going through the assessment process.

I therefore determined that I could reasonably initiate preliminary inquiries into each complaint, with a focus on the timeliness with which ASIO had handled each case, so long as I did not attempt to conduct a merits based review (which would fall squarely outside of my jurisdiction).

I concluded my inquiries into the first of these complaints in late 2006, and advised the complainant that I was satisfied that ASIO had accorded their case serious consideration and appropriate priority.

I received the second of these complaints in the second half of the reporting period and it was still on foot as at 30 June 2007 (but finalised early in the 2007–08 reporting period).

Security assessment of UK citizen Mr Rhuheh Ahmed

In the later part of 2006 various media outlets published stories claiming that a former Guantanamo Bay detainee, Mr Rhuheh Ahmed, had been denied an entry visa into Australia, allegedly on advice from ASIO.

Shortly afterwards I received 37 letters from members of the public expressing concern that Mr Ahmed had been denied a visa to enter Australia. Each of these correspondents asked me to investigate what role ASIO had played in this decision, and whether the decision was politically influenced.

I initiated a formal inquiry on 28 November 2006 and provided a full report of my findings to the Attorney-General and the Director-General of Security on 12 March 2007.

The conclusion I reached was that ASIO had been involved in making a security assessment of Mr Ahmed, in response to his application for a Business (Short Stay) Visa, and that in doing so it had acted legally and properly. There was no evidence or indication that the assessment had been the subject of improper influence.

A copy of my unclassified report into this matter is provided as Annex 3 to this annual report.

Migration related security assessments

As reported elsewhere in this chapter there was a marked spike in the number of complaints or referrals made to this office by persons expressing concern about the timeliness with which ASIO is processing security assessments for applications for short and long term visas across a wide spectrum of visa categories.

As I have explained, I chose to handle the bulk of these complaints administratively, but there were a small number of complaints during the reporting period which I pursued as preliminary inquiries.

In each of these instances there was a special circumstance which impelled me to take this course (and thereby bring the specifics of that case to the attention of the Director-General of Security).

In one of these cases I was able to advise the complainant that while there had been some delay in the processing of his visa application the clearance process had been completed and that

following completion of the assessment, a visa had then been swiftly issued.

In the other new case which I pursued as a preliminary inquiry, I advised the complainant (via his migration agent) that while the time taken to conduct the assessment was regrettable the assessment was not straightforward, and that the reasons for the delays which had been experienced were understandable.

ASIO career information

In my previous annual report I provided some general background information about a complaint which was initially handled by my predecessor as Inspector-General, Mr Blick, which I had cause to further examine during the 2005–06 reporting period.⁴⁷

Briefly restated, the complainant claimed that unfounded and/or malicious information about his former career in ASIO had been disclosed to a state police force for whom he worked and that the use of this information in an assessment of him had ultimately contributed to his loss of employment.

In March 2005 I was contacted by a person who was upset that he had been named in civil proceedings which the complainant had initiated. The person who contacted me had become aware of my predecessor's inquiry and report through the court proceedings and felt he had been denied natural justice.

I reviewed the papers and then wrote to three people with an interest in this matter seeking their views as to whether they wished me to reopen the inquiry which had been concluded by Mr Blick.

In doing this I pointed out that subsection 11(3) of the IGIS Act requires that the IGIS can only inquire, or inquire further, into a matter which is also before the courts or a tribunal if there are "special reasons" for the IGIS to do so.

Following receipt of responses from the persons I had written to, I judged that no such "special reasons" existed for me to make further inquiries while the matter was before the courts.

The matter rested there until late in the 2005–06 reporting period, when I ascertained that the

complainant's civil action had been dismissed, as the complainant had not been present when the matter had been called. I also learnt that shortly after this event the complainant had died in apparently tragic circumstances.

As there was now no possibility that these matters would be considered by a court, and therefore no impediment to an IGIS inquiry, I advised the Attorney-General in July 2006 that I intended to inquire further into various matters associated with this case.

In the course of my inquiry, I took sworn evidence from one person Mr Blick had interviewed, and interviewed another person under oath. I also formally required the provision of information in writing from a third person.

I concluded this inquiry late in 2006, and in early 2007 provided a copy of the report of my inquiry to the Attorney-General. My conclusion was that Mr Blick's original conclusions were all soundly based.

Claim for assistance arising from activities undertaken for ASIO

In June 2006 I was contacted by an individual who claimed to have had a long association with ASIO which had ceased in the 1970s.

The complainant claimed that the activities he had undertaken for ASIO and the circumstances under which he ultimately ceased to assist ASIO, was having a serious adverse impact on his current state of health.

I handled this complaint administratively in the first instance, to establish the complainant's *bona fides*.

Shortly afterwards I wrote to the Attorney-General, advising that I thought the matters raised by the complainant should be inquired into, but as these matters preceded the establishment of this office, I was required by subsection 8(8)(a) of the IGIS Act to obtain his permission before I commenced such an inquiry. The Attorney-General provided approval for this inquiry to proceed.

Following a close examination of relevant documents and files, discussions with relevant ASIO staff, and with the benefit of a legal opinion, I concluded my inquiry in April 2007.

⁴⁷ IGIS Annual Report 2005–2006, Canberra, October 2006, p. 34.

I advised the complainant that he appeared to have standing to make a claim under the *Safety, Rehabilitation and Compensation Act 1988* (SRC Act), at least in respect of some of the time in which he actively assisted ASIO, and that should he choose to do so, it was open to him to lodge a claim with the Commonwealth agency which processes claims made under the SRC Act, namely Comcare.

I encouraged the complainant to pursue this course, as Comcare is a specialist body with the competence and expertise to inquire into the basis for claims of ill health.

I advised the complainant that as this course was available to him, I had decided to conclude my inquiry.

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 government decision-makers.

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

Growth and expansion

ASIS, like the other AIC agencies, has experienced a period of rapid and continuing growth in the period since the 11 September 2001 terrorist attacks on the United States and subsequent attacks on Australian and western interests around the world.

One measure of the significant growth which ASIS has recently experienced is budgetary. The total appropriation granted to ASIS from all sources in the 2006–07 Commonwealth Budget was \$131.4 million⁴⁸, while this figure had grown to \$162.5 million⁴⁹ when the 2007–08 Commonwealth Budget was brought down in May 2007.

Rapid and continuing growth will pose issues for any organisation and ASIS is not immune from this general rule, excepting that the secretive work it undertakes means that these issues can be made more difficult to manage by the needs of security.

I have sought and received regular updates on how the additional funds allocated to ASIS are being spent, the consequential rebalancing of organisational structures and priorities within ASIS, and on recruitment, training, accommodation and facilities issues.

⁴⁸ DFAT Portfolio Budget Statement 2006-2007, ASIS statement available at <http://www.dfat.gov.au/dept/budget/2006_2007_pbs/pbs_2006_2007_asis.pdf> (accessed 22 August 2007).

⁴⁹ 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> (accessed 22 August 2007).

I have also sought and received feedback on the use of internal grievance mechanisms and the results of staff surveys, as a guide to the current organisational health of ASIS.

While the continuing expansion of ASIS provides it with new opportunities, the Director-General is fully seized of the risks associated with growing rapidly and is concerned to ensure that the process of change is managed effectively.

From what I have seen the rapid expansion of ASIS has been managed in a considered and sensible manner, with appropriate regard shown to the interests of individuals, as well as ASIS as a whole.

Ethical issues

The collection and other operational activities undertaken by ASIS are frequently challenging and potentially quite dangerous. There are many reasons for this not the least being that the intelligence information ASIS is charged with obtaining would clearly be of little value if it could be obtained freely, and without risk, by other means.

In order for ASIS to fulfil its functions some of its staff will necessarily be required to work in hostile or harsh operational environments, a long way from the usual support systems which are available to individuals who work in more unusual fields.

Many ASIS staff will also be subject to special pressures associated with the kind of work they perform, must adapt psychologically to the risk and possible consequences of exposure, and deal regularly with individuals who might otherwise be regarded as ethically challenged, without letting this corrode their own moral code.

It is not surprising that this type of work throws up ethical quandaries and we become aware of such issues from time to time, either through direct contacts made with our office, or through our regular inspection activities.

My experience is that ASIS management are well attuned to the sensitivities and nuances of the work with which they are engaged. In their discussions with me and in responses to correspondence posing questions, I have found the responses to be thoughtful and considered.

Special briefings

In discharging my duties I have regular and frequent contact with the Director-General of ASIS, Mr David Irvine AO, his senior managers, and a range of less senior officers who hold key positions.

In addition to our regularly scheduled inspection visits, I met with senior ASIS officers on at least 20 separate occasions during this reporting period, either where I specifically sought a briefing on a particular subject, or where a senior ASIS manager has wished to bring something to my attention.

These briefings covered a wide variety of issues ranging from internal structures and processes to particular operational activities. Due to the inherent sensitivity of the subject matters discussed, I am not able to make further comment in this report.

I am appreciative of the responsiveness of ASIS to my requests for briefings, the willingness of ASIS to proactively bring matters to my attention, and the candour which is displayed in these meetings, all of which I view as positive signs of ASIS's attitude to external oversight.

Visits and contact with staff

As has been the case since I first became IGIS, I try to personally meet with the more senior ASIS officers prior to the commencement of their overseas postings. The purpose of these meetings is to remind ASIS representatives of the role and functions of this office and the expectations of them.

I consider these meetings to be an important means of reinforcing with ASIS personnel 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.

These are important messages to send and to reinforce because, for the most part, I will not be in a position to visit or meet with ASIS staff in the field.

Notwithstanding this, I did call on some ASIS personnel in the course of a brief overseas visit I made during the reporting period.

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

Training

Members of my staff and I regularly make presentations to ASIS officers at ASIS training courses, and we also incidentally address ASIS staff when we present 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 appropriate given the respective sizes of these agencies.

As a minimum, I meet with each new intake of intelligence officer trainees to explain the role and functions of my office.

It is my intention in 2007–08 that my staff and I will also attend various ASIS training sessions as observers, so that we can view the training methods to which trainees are subject.

Access to AUSTRAC data

ASIS was little touched by legislative changes during the reporting period but, as detailed elsewhere in this report, following the passage of the *Anti-Money Laundering/Counter-Terrorism Financing Amendment Act 2007*, ASIS will for the first time be able to directly access various financial transaction records maintained by AUSTRAC, and to communicate such information to foreign intelligence agencies, subject to certain conditions being met.

This legislation has brought ASIS into line with ASIO which has had a long standing formal relationship with AUSTRAC.

As a consequence of the passage of the above Act, ASIS is developing an MOU with AUSTRAC which will set out the terms and conditions under which it can obtain access to AUSTRAC's records.

Once this MOU has been developed and I have revised my own MOU with AUSTRAC, I will institute regular inspections of ASIS to ensure that it complies with the terms and conditions under which access to financial transaction reporting information has been provided to it.

Work on the above was continuing as at the conclusion of this reporting period.

Inspection activities

Range and scope

As ASIS continues to grow in size, it follows logically that the volume of operational activities and records which need to be considered or reviewed also grows. It also follows that as ASIS expands the scope of its activities and refocuses its priorities, that I will incorporate new elements into my inspection program.

The inspection activities conducted by my office in respect of ASIS therefore reflect a mixture of continuity and change.

During the reporting period, we maintained many of the features of our usual inspection program, but also added some new features or activities. 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. Such a Ministerial Direction was issued to the Director-General of ASIS in late 2001, to coincide with the commencement of the ISA.

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.

We conducted six such inspections during this reporting period, and generally found the authorisations to have been properly made and in conformity with all obligations.

We noted the first instance we had seen of the use of section 9A of the ISA, under which authority the Prime Minister, the Minister for Defence or the Attorney-General, may issue a MA to ASIS in an emergency situation, should the Minister for Foreign Affairs not be available.

In the case in question the Minister for Foreign Affairs was in transit when a time critical operational opportunity presented itself which required an MA. The authorisation was granted in conformity with the requirements of section 9A, and did not cause me any concerns, rather it revealed that the processes put in place to deal with such a circumstance had worked well.

We also pointed to a minor dating anomaly on the face of one authorisation. Although we did not believe that this anomaly was of any legal consequence (as the intention of the Minister was very clear), ASIS nonetheless immediately took action to have the error corrected, thus removing any doubt.

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 unfettered 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. My confidence in making this statement is based on:

- our regular examination of all submissions made by the Director-General to the Minister for Foreign Affairs
- the receipt by me of each approval which specifically dealt with training in the use of weapons for self-defence purposes, the provision of weapons for self-defence purposes, and/or the delivery of training in other self-defence techniques (cross referenced against the ministerial submission files we examine)
- independent access to the internal ASIS database recording such authorisations, and
- a full reconciliation of these records following the completion of the reporting period.

While I am not in a position to report the precise number of authorisations which were issued I can nonetheless 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 have also spoken at length with the officers responsible for maintaining the above records, other ASIS staff with functional oversight of this process, and ASIS officers who have received training and/or were authorised to carry a weapon for self-defence purposes should circumstances require it.

Based on these discussions and our other review activities I am satisfied that the powers afforded to ASIS under Schedule 2 of the ISA are being used professionally and as intended, and not being misused.

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). I received no such notifications during the reporting period.

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

Since becoming IGIS in 2004 I have placed considerable store on regularly reviewing ASIS's operational case files, either directly or at one remove. This was again the case in this reporting period.

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 staff 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 therefore continued the consultancy arrangement I have with my predecessor, Mr Bill Blick, whereby he spends between two and three days per month reviewing ASIS's operational case files and reporting his findings back to me at the completion of each inspection.⁵⁰

The task of reviewing ASIS's operational files, like painting the Sydney Harbour Bridge, is never complete, but I am keen to cycle through as many files as possible each year.

To this end Mr Blick has been assisted during his inspections by one of my senior staff and I anticipate involving another member of staff in this activity in the future. I also intend to personally conduct more inspections of this kind, as my schedule permits.

While not able to go into specific operational details in a public report I can provide assurance 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 searching questions relevant to the conduct of the operations under review.

The Director-General has provided written replies in all instances where I have required a response.

Some of these responses have resulted in a further exchange of correspondence or briefings to clarify issues we have raised.

I am appreciative of the efforts of those ASIS staff who have assisted us during these inspections, have provided briefings, or been involved in the preparation of responses to our various queries.

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 Minister for Foreign Affairs issued such rules in October 2001 to coincide with the coming into effect of the ISA and they have not been varied since. A copy of the ASIS privacy rules were published in the IGIS Annual Report 2001–02⁵¹ and can also be accessed via the ASIS website⁵².

The ASIS privacy rules are important because in discharging its functions ASIS generates and receives a significant amount of secret intelligence information. Information reaching this threshold is put into reports which are then circulated to appropriately cleared addressees with a demonstrated need to know this information.

My office regularly reviews this reporting to ensure that, so far as we are able to ascertain, it was collected in accordance with the requirements of the ISA, and then reported/disseminated in accordance with the requirements of the ASIS privacy rules.

The total number of reports which are circulated run into many thousands each year, but the instances when it is felt necessary or appropriate to refer to Australian persons in this reporting is relatively low.

So as to ensure that we have full visibility of every instance where intelligence on or about an Australian is included in an ASIS report, relevant ASIS staff are required to complete a privacy cover sheet, highlighting the reference, citing justification under the privacy rules for the inclusion of this information, and giving an explanation of how the relevant provision is applicable.

All of these reports and their accompanying privacy coversheets are provided to my office approximately every two weeks for consideration and comment.

Following our review of the reporting we provide written comments to the head of the relevant section within ASIS which coordinates the publication and distribution of this reporting.

⁵⁰ Details of this arrangement were advised in IGIS Annual Report 2005-2006, Canberra, October 2006, p. 38-39, and p. 60.

⁵¹ IGIS Annual Report 2001-2002, Canberra, October 2002, Annex 4, pp. 91-92.

⁵² See <http://www.asis.gov.au/rules_to_privacy.html> (accessed on 24 August 2007).

This a labour and time intensive inspection and review task but I believe that it is worth the effort, given the marked improvement we have noted over several years in the manner in which ASIS is fulfilling its obligations.

I am pleased to say that I have seen no privacy abuses in the material we have access to, and that there is a commitment within ASIS to the rigorous application of the privacy rules.

Periodic roundtable meetings

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, rather than reflexively exchanging correspondence.

In ASIS we conduct roundtable meetings of this kind approximately every six weeks. Our ordinary practice is to circulate an agenda approximately a week before each meeting and invite staff along who are involved in policy development, legal affairs and intelligence production. 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 the IGIS 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 carried over two unfinished preliminary inquiries into this reporting period each of which have now been finalised. I also received two new complaints about ASIS which led me to initiate preliminary inquiries.

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

The above rate of complaint about ASIS is relatively stable when considered against the number of complaints received in the past few years.

A summary of some of the inquiries my office conducted is provided below.

Recruitment related complaints

One of the complaints I carried over, and one of the new complaints I received concerned recruitment related issues.

The recruitment related complaints we have received in the past have tended to be concerned with procedural issues (such as the timeliness of the selection process), restrictions imposed on persons who have difficult to verify or uncheckable backgrounds, and what feedback can or should be provided to unsuccessful candidates. All three of these themes relate in some way to the special security requirements that attach to employment with ASIS.

The two recruitment complaints referred to above primarily concerned process issues and the provision of feedback.

Obtaining employment with an intelligence agency is, of course, not similar in every respect to gaining employment elsewhere in the public or private sector, as it is necessary for candidates for such positions to be the subject of psychological testing procedures, and other intrusive and time consuming background checks.

This testing is designed to help ensure that there is a close correlation between an applicant's skills and attributes and the requirements of particular positions within the agency.

Psychological testing also serves the purpose of identifying candidates who do not have the aptitude or psychological characteristics necessary to be successfully employed in a high security

environment, or who might, in some circumstances, present as a potential security risk.

It is also sometimes the case that there is a genuine mismatch in how a candidate views their own strengths and attributes, compared to how this is judged in an external assessment, and the gulf between these positions cannot always be bridged or reconciled.

The issue of providing meaningful feedback is more problematic. As detailed in last year's annual report⁵³ ASIS's standard position has been that it does not provide performance feedback to unsuccessful job applicants.

The justification for this is that ASIS does not wish to reveal too much of its selection methods, for fear that possible weaknesses might be exploited and unsuitable persons selected for employment with ASIS.

While ASIS generally holds to this position, it recognises that unsuccessful candidates who are already employed elsewhere in the AIC fall into a different category than do unsuccessful candidates from elsewhere.

In recognition of this ASIS has decided to be slightly more forthcoming in providing feedback to such candidates, with a view to assuaging any concerns these candidates might have about the effect of an unsuccessful application on their security status, future job prospects and so on.

Overall, given the rate at which ASIS has grown and continues to expand, the number of recruitment related complaints received by this office continues to be very small.

Grievance process issues

In June 2006 I received a complaint from a current employee of ASIS alleging a flawed and unjust investigation of a formal grievance he had lodged regarding aspects of his employment. The complainant also raised other issues which were not dealt with as a part of the grievance review process.

On the basis of the information provided to me I decided to initiate a preliminary inquiry. The purpose of the inquiry was to determine whether I had jurisdiction to review certain aspects of this case,

and to also examine certain other aspects which appeared not to have been the subject of prior consideration and determine whether I could or should investigate them.

I devoted significant time and effort to reviewing relevant papers, meeting with the complainant and subsequently speaking to him at length, and also meeting with senior ASIS management.

At the end of this process I determined that certain employment related decisions were management prerogatives which I was not properly placed to second guess, and that while there were certain things ASIS could have perhaps handled differently, the complainant had been properly heard and his concerns were taken seriously.

I also determined that there were certain other issues raised by the complainant which were outside of my jurisdiction.

⁵³ IGIS Annual Report 2005–06, Canberra, October 2006 p.41.

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, MAs and privacy rules which are made pursuant to the ISA.

Intelligence priorities for the Australian intelligence community 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.

DSD's infosec role is not security classified, and 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 Director DSD

As discussed in 'The year in review – general matters' Mr Stephen Merchant, was promoted to the position of Deputy Secretary Intelligence and Security (DepSec I&S) in the Department of Defence, and in early May 2007 the then Director DIGO, Mr Ian McKenzie was announced as Mr Merchant's successor as Director DSD.

Support to military operations

DSD naturally 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 the completion of this reporting period up to 3500 ADF personnel were variously deployed to locations including the Solomon Islands, East Timor, Sinai, Sudan, Iraq and Afghanistan.

As can be deduced from this list, the operational environments into which our service personnel are deployed can range up 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 is not compromised, DSD is being increasingly called upon to provide high-quality and timely sigint products and services to the ADF. DSD also contributes to the security of ADF missions abroad by ensuring that sensitive electronic information systems are sufficiently robust to deflect attempts at unauthorised access, compromise or disruption.

As has been the case for several years now, the number and variety of ADF deployments continues to impose significant demands on DSD. I received several briefings throughout 2006–07 on the support provided to the ADF by DSD, and 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 relating to terrorism-related targets.

Obtaining and sharing information of this kind directly assists 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

As discussed in 'The year in review – general matters' chapter the NSW Coroner has been conducting an inquest into the death of Mr Brian Peters in East Timor, in October 1975.

My predecessor, Mr Blick, 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 deaths of Mr Peters and four of his colleagues could have been averted.

While Mr Blick ultimately concluded that intelligence material meeting the above description did not exist, DSD naturally has a very considerable interest in the matters currently being inquired into by the NSW Coroner.

Although Mr Blick's inquiry had a completely different focus to the inquest (one being focussed on whether the Australian government had forewarning and the other concerned with the circumstances of Mr Peters' death), I have been monitoring developments in this matter.

Through out the second half of the reporting period, I sought regular updates from DSD on the progress of the inquest, and the efforts they were making to respond to requests from the Coroner.

I was satisfied, based on these briefings, that DSD was very genuine in providing materials and responding to other requests, notwithstanding the very significant costs in terms of time and resources associated with servicing the Coroner's requirements.

Public hearings associated with the inquest concluded in June 2007, with a report of the outcome of the inquest likely to be finalised and made public in the first half of the 2007–08 reporting period.

Inspection activities

During 2007 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 monthly meetings with relevant DSD staff 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 Director needs to satisfy the Minister for

Defence 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.⁵⁴

In order to obtain an MA, the Director DSD provides a comprehensive written submission to the Minister in respect of each individual on which 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.

We became aware through our various inspection activities, that differing views existed about how subsection 9(1A)(b) of the ISA should be interpreted and applied, and discussed the implications of this with various DSD seniors.

The provision in question requires that before a responsible Minister issues an MA in respect of an Australian person, the Minister needs to be satisfied of certain things. If the MA application is justified on the grounds that the subject is believed to engaged in activities that are, or are likely to be, a threat to security, the agreement of the Attorney-General must first be obtained.

A slightly more detailed discussion of this issue is provided in the DIGO chapter, but this matter was ultimately resolved by a definitive legal opinion on the subject being obtained from the Australian Government Solicitor, which is accepted by all parties with an interest in this matter.

Although it occurs relatively infrequently, DSD has a potential role to play in assisting other government authorities in respect of Australians who are overseas who get caught up in hostage situations, particularly if there is a genuine fear or apprehension about their safety.

During the course of the year, we discussed with DSD the applicability of section 9(1A) of the ISA to the communications of persons in such situations.

Spot checking of databases

As detailed in my previous annual report⁵⁵, in the first half of 2006 I had a member of my staff conduct a series of spot checks 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 that such collection only occurred during the period specified in the authorisation.

These checks, which concluded in the second half of the 2006 calendar year, revealed that the requirements of each MA were being complied with.

This pilot project did reveal several data entry errors relating to expiry dates, but steps have been taken to ensure improved data integrity into the future.

I propose to conduct similar checks in the first half of 2008 to check on the efficacy of these measures.

Monthly meetings

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

The style and form of these various meetings all have their genesis in the regular meetings we have been holding with DSD for very many years.

The meetings we hold with DSD usually involve a very senior DSD manager, as well as drawing staff from the compliance and reporting standards 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, ministerial authorisations, legislative and parliamentary reviews, and current legal issues, as well as any topical issues which may have featured in the media.

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

⁵⁴ Section 9(1A) of the *Intelligence Services Act 2001*.

⁵⁵ IGIS Annual Report 2005-2006, Canberra, October 2006 pp. 44-45.

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 very pleased with the candour and quality of discussion in these meetings, and find them very helpful in gaining a better understanding of the important work which DSD undertakes.

Privacy rules

Section 15(1) of the ISA requires the Minister for Defence to make written rules regulating the communication and retention of intelligence information concerning Australians. The then Minister for Defence issued privacy rules to DSD in late October 2001 to coincide with the commencement of the ISA.

The DSD privacy rules enable DSD to include references to Australian persons in their reporting, in limited circumstances, 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 since becoming IGIS 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 very 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 projects with these objectives and we discuss any aspects that might involve legality or propriety.

I was pleased that DSD briefed me on several such projects during the reporting period and seriously addressed the various queries which I raised.

Site visits

DSD maintains a number of facilities around Australia which are integral to its collection activities.

During the reporting period my staff visited one such facility, as well as an ADF unit 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.

In this reporting period my office delivered 10 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 primary business 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.

Appropriateness of OSA procedures/security related issues

During this reporting period I received one complaint specifically about DSD which I decided to pursue as a preliminary inquiry.

The complaint, which was from an unsuccessful applicant for a position with DSD, revolved around the appropriateness or otherwise of an Organisational Suitability Assessment (OSA) process and also raised several related security issues.

I advised the complainant at the conclusion of my inquiry, that I was satisfied that they had not been disadvantaged because of any of the factors which they had identified as purported defects.

Wider review of OSA policy and procedures

Quite unrelated to the above matter, I decided towards the end of this reporting period to initiate an 'own motion' inquiry into OSA policy, procedures and practices across the three AIC agencies which operate within the Department of Defence. This naturally includes DSD.

The purpose of this inquiry is to examine existing policies, procedures and practices in each of the Defence Intelligence Group intelligence agencies, to identify and consider any inconsistencies which might exist, and to comment on practice across the Group against considerations of fairness and "propriety" generally. This inquiry was on-going at the completion of the reporting period.

Matters handled administratively

In addition to this formal inquiry, I also received one other complaint about DSD which, because of its nature, I decided to handle administratively.

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, 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 Director DIGO

As discussed elsewhere in this report, the Director of DIGO for most of this reporting period was Mr Ian McKenzie. Towards the end of the period he was appointed Director DSD and was succeeded at DIGO by Mr Clive Lines.

Growth and expansion

When DIGO commenced on the path of becoming an AIC agency in its own right in the late 1990s, its managers were confronted with a series of challenges arising out of the fusion of sometimes disparate elements.

These issues have now been largely resolved, through the combined effects of a committed workforce, strong but sensitive management, and by the infusion of a large number of recruits who do not know DIGO as being anything other than the agency which it is today.

While these issues were important and required significant management attention, DIGO has also rightly focussed on establishing and then consolidating its role as Australia's leading imagery/geospatial agency.

Having to my mind achieved this objective, DIGO is now able to fully direct its focus towards:

- further developing and exploiting its collection and analytical capabilities

- forging close links with similarly focussed international agencies
- forging closer links with its domestic customers, and
- contributing to a ‘whole of government’ approach to various issues through the provision of unique products and services.

While the creation of a new agency from many parts is no easy task, and DIGO has experienced some growing pains, DIGO’s future is bright, and it is now well placed to make a significant and growing contribution.

Inspection activities

DIGO privacy rules

Section 15(1) of the ISA requires the Minister for Defence to make written rules regulating the communication and retention by DIGO of intelligence information concerning Australian persons.

On 2 November 2005, the then Minister for Defence endorsed a document entitled the *Rules Governing DIGO’s Activities in Respect of Australia and Australians*. I included a copy of these rules as an annex in my previous annual report.⁵⁶

My staff and I visit DIGO headquarters every two months to review materials relating to DIGO’s collection activities. In the course of these visits we closely examine all tasking requests DIGO receives which might impact upon Australian persons or interests, for compliance with the DIGO privacy rules.

For all practical purposes DIGO’s privacy rules are essentially the same as the privacy rules under which the other ISA agencies (i.e. ASIS and DSD) operate.

While there is much to commend in having a uniform approach to the handling of privacy related matters across our foreign intelligence collection agencies, it does pose certain issues for DIGO.

The foremost challenge DIGO faces in applying their privacy rules is that they are predicated on the assumption that the privacy of “Australian persons” will be protected, unless there is appropriate justification provided to enable the reporting

of intelligence information to clients with an established need to know.

The term “Australian persons” has a broader meaning than living human beings, and is 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 it is for ASIS and DSD. This is because ASIS and DSD reporting is largely text based and references to Australian persons are normally to living persons, whereas DIGO’s reporting is primarily image-based and not focussed on persons per se but on property or premises which may fall within the definition of being an “Australian person”.

In making the above observations, I should state that the vast majority of DIGO’s reporting has an off-shore focus, and that the privacy rules come into play relatively infrequently.

DIGO is committed to applying the privacy rules, and if anything inclined to take a cautious and conservative approach rather than to disregard the requirements of the rules.

Ministerial authorisations

Whenever my staff and I conduct a privacy rules inspection, we also review every MA which has been issued by the Minister for Defence in the period since our previous visit, and also examine any approvals given by the Director DIGO in the same period.

In the course of one of these reviews, early in 2007, I queried whether every legal requirement for the granting of a particular MA had been met.

In the case in question a customer agency had requested DIGO as a matter of urgency to obtain some imagery relevant to an ongoing inquiry. As the request appeared to relate to activities which might be construed as posing a threat to security, I queried whether the approval of the Attorney-General had been obtained, as required by section 9(1A)(b) of the ISA.

⁵⁶ IGIS Annual Report 2005-2006, Canberra, October 2006, Annex 5, pp.103-104

In the circumstances of the case DIGO did not believe that such an approval was necessary, and prior to seeking the authorisation had obtained advice supporting this view.

Following my questioning of the basis for the authorisation in question, DIGO placed an immediate internal 'stop' on their collection activity, pending the resolution of the legal questions raised by my query.

There followed several intra-agency meetings involving discussion of what is required to trigger the operation of section 9(1A)(b) of the ISA, and ultimately the production of what is accepted by all interested parties as a definitive legal opinion by the Australian Government Solicitor on the subject.

As that opinion is classified, I am not able to directly discuss its contents but I am glad that there is now a clear understanding by all parties of the requirements of this provision.

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 review our privacy rules/ministerial authorisation inspections.

On each occasion I met with the Director DIGO or Acting Director, DIGO's legal adviser, and a representative from the policy and compliance area of the Organisation. I am grateful to all for giving freely of their time to participate in these meetings

Training

I did not make any specific presentations to DIGO staff during the reporting period but did incidentally speak to those DIGO staff who attended the cross-AIC induction and senior officer courses at which I spoke.

Complaints and inquiries

The office received one complaint about DIGO during the reporting period, which was handled administratively.

The above complaint was from an unsuccessful candidate for a position with DIGO, who also raised queries about Organisational Suitability Assessment (OSA) processes. I suggested to the complainant that they should seek feedback or redress from within the Department of Defence.

Wider review of OSA policy and procedures

As noted in the DSD chapter, I decided towards the end of this reporting period to initiate an 'own motion' inquiry into OSA policy, procedures and practices across the three AIC agencies which operate within the Department of Defence. The above inquiry naturally includes DIGO.

The purpose of this inquiry is to examine existing policies, procedures and practices in each of the DIG intelligence agencies, to identify and consider any inconsistencies which might exist, and to comment on practice across the Group against considerations of fairness and "propriety" generally. This inquiry was on-going at the completion of the reporting period.

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 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/>.

Privacy guidelines

The DIO privacy guidelines, endorsed by the then Minister for Defence Senator the Hon Robert Hill on 2 December 2005, govern the use of references to personal information about Australians in external communications – including reports, briefings, emails and advice – emanating from DIO.

After the introduction of privacy guidelines at DIO, I was able to conduct one inspection in April 2006 and forecast in my last annual report that I intended to conduct inspections every three months during this reporting period.

I conducted five inspections of DIO's use of the privacy guidelines during the reporting period.

Overall I was pleased with the quality and level of detail contained in the documentation. The implementation of privacy guidelines at DIO has been conducted thoroughly and it is clear that DIO staff take seriously the responsibility to document application of the guidelines. I have also noticed that during the reporting period DIO staff have developed a more nuanced appreciation of the privacy guidelines and, for the most part, appear to understand the process and the importance of meeting the requirements of the guidelines.

DIO has continued its organisation-wide programs and training to educate analysts on applying the guidelines and reporting on compliance with the guidelines. DIO is making good progress in this regard with a high percentage of staff having undertaken training. I will continue to monitor DIO's commitment to ensuring that privacy guidelines training is regularly undertaken by all analysts.

I intend to continue conducting inspections relating to DIO's use of the privacy guidelines every three months.

Analytical Integrity

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. This means that of my own motion I can inquire into matters which include:

- the compliance by DIO with the laws of the Commonwealth and of the states and territories
- the propriety of particular activities of DIO, or
- the effectiveness and appropriateness of the procedures of DIO relating to the legality or propriety of the activities of DIO.

As mentioned in the chapter on ONA, the legislative amendments also specifically required me to inquire into the statutory independence of ONA. There is no equivalent provision in respect of DIO, not least because DIO does not have a statutory basis.

However, I consider that the concept of propriety clearly covers notions that DIO assessments must be formulated in an objective manner and without improper external pressure or self-censorship to conform with policy positions. Another way of expressing this is to refer to the “integrity” of the assessment process.

I am certainly not suggesting that the sort of review undertaken by my office in respect of ONA is readily transferable to DIO. Obviously a key difference is the statutory independence of the Director-General of ONA compared to the DIO Director’s position in the Defence management structure.

I have sought a detailed briefing on how DIO ensure the integrity of its assessment process and look forward to receiving this in the next reporting period.

Training

I made two presentations to staff at DIO during the reporting period.

Complaints and inquiries

I received no complaints about DIO which required inquiry action during this reporting period. Three matters were handled administratively.

As mentioned in the DSD and DIGO chapters, I have commenced an own motion inquiry into the OSA process in these three Defence agencies.

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 – 2006 Inspection

In my 2005–06 annual report I outlined my new role and responsibilities in relation to conducting periodic reviews of the statutory independence of ONA.

By way of background, the *Intelligence Services Legislation Amendment Act 2005* which came into effect on 2 December 2005 inserted a new provision – s8(3)(c) – into the IGIS Act which requires the IGIS:

“(c) At the request of the responsible Minister or of the Inspector-General's own motion, to inquire into any matter in relation to the statutory independence of ONA.”

There has also been an amendment to s35(2) of the IGIS Act so that the IGIS is required to include in his or her annual report, comments on any inquiry conducted in accordance with the new s8(3)(c).

In order to fulfil my new responsibilities, I began planning and undertaking inspection activity relating to ONA's statutory independence in the last reporting period. This work essentially covered ONA's assessments in the period December 2005 until October 2006. It involved examination of ONA's formal assessment products, interviews with key ONA clients, a survey of ONA analysts and confidential interviews with selected analysts to explore survey responses and related issues.

I concluded this inspection activity in October 2006 and the report of my findings was sent to the Prime Minister, the Director-General of ONA and the Secretary of PMC on 15 December 2006. In March 2007 I addressed an ONA all-staff meeting on the findings of my first review of ONA's statutory independence.

I found that the general view of analysts was that ONA judgements are not shaped to suit the political concerns of government ministers. There were no suggestions to me of improper pressure and/or attempted direction from ministers and their offices.

Analysts believed ONA assessments are not biased towards desired policy outcomes, although there

were a number of analysts (but not a majority) who believed or were ambivalent about whether there may be some subjects with policy/political sensitivity on which ONA might self-censor (ie. touch on in a limited manner only). Examination of ONA products in the small number of areas nominated did not support this in some instances, but was inconclusive in others.

A copy of the complete executive summary of the report is at Annex 6.

Statutory Independence – Inquiry 2007

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 review.

While the inspection results were 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. On 15 February 2007 I advised the Prime Minister and the Director-General of ONA of my intention to conduct such an inquiry.

The methodology used in conducting this inquiry, while largely consistent with the methodology used in undertaking the 2006 inspection activity, has been more wide-reaching. As well as undertaking the same review activities as in 2006, I requested:

- documentation on endnoting
- internal ONA reviews of key judgements
- documentation on dissent, and
- drafts of ONA product and documentation indicating changes made to drafts.

At the end of this reporting period my office was undertaking the analysis of this documentation and progressing with this inquiry. My findings will be reported in the next annual report.

Privacy guidelines

As mentioned in the previous chapter on DIO, ONA has also developed privacy guidelines that outline the handling, use, and further dissemination of information about Australian persons. The guidelines apply to references to personal information about Australians in external communications _ including

reports, briefings, emails and advice _ emanating from ONA.

During this reporting period I conducted five inspections of ONA's use of the privacy guidelines. I was satisfied with ONA's application of, and compliance with, the privacy guidelines and was pleased with the quality and care taken in the documentation.

ONA continues to educate analysts on applying the guidelines and reporting on compliance with the guidelines. The implementation of the privacy guidelines at ONA has been conducted in a thorough manner and I was satisfied with the level of awareness of the privacy guidelines among analysts. I would emphasise the importance of refresher training to ensure that analysts maintain an awareness of their responsibilities.

I will continue to conduct inspections relating to ONA's use of the privacy guidelines every three months.

Training

Following from my new roles and responsibilities in respect of ONA, 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 course, to which ONA staff are regularly allocated places. In March 2007 I addressed an all-staff meeting which covered my role in relation to ONA, a comparison of the roles and responsibilities of other Inspectors-General from around the world, and the findings from the 2006 review of ONA's statutory independence. I believe that ONA staff have a well-formed appreciation of my role in reviewing the statutory independence of ONA.

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.

As mentioned above, I launched an own motion inquiry into the statutory independence of ONA (Section 8(3)(c) of the IGIS Act) in February 2007. I will report the findings of this inquiry in my next annual report.

The year 2007–08 in prospect

The following is a summary of the main activities planned for the 2007–08 reporting period.

Continuation of final term as Inspector-General

As noted earlier in this report, I was reappointed as IGIS on 27 April 2007 for a period of four years.

Section 26 of the IGIS Act provides that persons holding the office of IGIS may not be appointed to the office more than twice. I think that it is entirely appropriate and desirable for the position of IGIS to be term limited. Equally it is important to have a sufficient time in the position so as to obtain a good grasp of the inner workings of the AIC agencies but without becoming captive to their institutional interests, or becoming identified in the public mind as an “intelligence insider”.

The following plans reflect my current short term intentions but will be supplemented as necessary, as the new reporting year progresses and my thinking develops further.

Staffing and recruitment

During this reporting period I recruited two full time officers and one part time officer. One of these positions was filled in anticipation of the impending retirement of a long serving OIGIS officer early in the 2007–08 reporting period. It is my current intention to engage at least one additional member of staff in 2007–08.

The anticipated increase in resources detailed above means that I will be able to improve 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.

Inspection activity

ASIO – new powers

In 2005 the ASIO Act was amended to provide ASIO with the power to compel airline and vessel operators to provide information (see section 23). In the coming period I propose to conduct inspection activity which examines the requests made and how the data is handled.

As indicated elsewhere in this report, ASIO used “B-party” telecommunications interception warrants for the first time during this reporting period. We will continue to be especially vigilant in monitoring all aspects of the use of “B-Party” warrants during the 2007–08 reporting period.

It is my intention in the 2007–08 reporting period to conduct periodic meetings with senior ASIO personnel, along similar lines to meetings which I already conduct with the other intelligence collection agencies.

The purpose of these meetings will be to provide a regular forum in which I can be briefed on emerging trends or developments, candidly exchange views on issues of mutual interest, and to monitor progress on matters in which my office has a direct interest.

As indicated in the chapter of this report dealing with legislative developments, the Telecommunications (Interception and Access) Amendment Bill 2007 was introduced to Parliament in June 2007, to give legislative effect to those recommendations contained in the Blunn Review which were not dealt with in earlier legislation.

The Senate referred the provisions of this Bill to the Senate Standing Legal and Constitutional Affairs Committee on 21 June 2007 for inquiry.

In my submission to this review I observed that one of the proposals contained in the Bill is that very senior officers within ASIO will be able to issue authorisations requiring telecommunications carriers or carriage service providers to provide prospective telecommunications data to ASIO for the duration of the authorisation (i.e. up to 90 days).

In commenting on this provision I stated that:

"While this requirement for more senior level approval is appropriate, I believe that it is also a process which should be examined as a part of my office's inspection program. This would involve periodic visits by my staff during which they would review all of the authorisations granted in the preceding period to ensure that there was sufficient justification and that the requirements imposed by the Communications Access Coordinator under the proposed section 183 were met."⁵⁷

The Senate Standing Legal and Constitutional Affairs Committee discussed this suggestion in their report and formally recommended that such inspection activities occur.⁵⁸

Should this Bill be passed and given effect during the 2007–08 reporting period, I will implement this recommendation.

ASIO - warrants

My office will continue to pay very close attention to the granting of special powers warrants to ASIO and the execution of these warrants.

These warrants are, for the most part, issued by the Attorney-General rather than by a judicial officer. It is therefore appropriate that these warrants be subject to some form of external scrutiny, even if it is necessarily ex post facto.

Another reason why this office seeks to review 100% of ASIO's special powers warrants is that they are, by their very nature, inherently intrusive into the personal affairs of the subject of the warrant, and

this is perhaps doubly true when these powers are exercised covertly.

In light of this it is my intention to inspect all requests for warrants which are made by ASIO during 2007–08, and to review associated documentation.

It is also my intention that, in selected cases, we will seek full details of the investigations which are carried out under warrant authority, including examining relevant operational case files and, if necessary, discussing operations with the responsible ASIO officers.

We 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 2007–08, should any questioning, or questioning and detention warrants be granted to ASIO.

ASIO – other reviews

We will examine all approvals to investigate generated in ASIO's central office and as many approvals generated by ASIO's State and Territory offices as we can access during our periodic visits. The files on which actions resulting from the authorities are recorded will also be examined.

We will continue monitoring ASIO's access to, and use of, AUSTRAC and taxation records, to ensure compliance with the legislation and the MOU under which this access is provided.

We will continue to monitor ASIO's procedures for controlling the use of alternative documentation associated with assumed identities.

We will also continue to monitor ASIO's performance with regard to its obligations under the *Archives Act 1983*.

⁵⁷ My submission is submission number 14, which is located at the following web address: <http://www.aph.gov.au/senate/committee/legcon_ctte/telecommunications_interception/submissions/sub14.pdf> (accessed on 29 August 2007).

⁵⁸ Report of the Senate Standing Committee on Legal and Constitutional Affairs on the Telecommunications (Interception and Access) Amendment Bill 2007, 1 August 2007, p. 33-36.

Later in the reporting year we will revisit ASIO procedures and practice in the exchange of information with foreign liaisons, to check that standards are being maintained.

My office will continue to make presentations to ASIO training courses on ethics and accountability. We also intend to observe, participate in and otherwise support 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.

ASIS

During the 2007–08 reporting period my office will review any instance where ASIS has used its new status as a “designated agency” to access any financial transaction records which are held by AUSTRAC, or to communicate any information of this kind to other parties.

This is necessarily a new inspection activity and how we go about this task will be informed by experience, but as a minimum, we will be checking that ASIS is acting in compliance with its legal obligations under the AML/CTF Act 2006, and any MOU it enters into with AUSTRAC.

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 reviewing all MAs which are sought by ASIS under the terms of the ISA.

We will continue to very 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.

If it is feasible, I propose that either I or a senior member of my staff will attend a weapons training course, as an observer, to gain a first hand appreciation of what is involved.

We will continue to closely inspect operational files having regard to the legality and propriety of the conduct of ASIS officers. It is my intention to continue to engage former Inspector-General, Mr Bill Blick, to assist in this task until at least the end of 2007, at which time I will review this arrangement.

I intend to maintain our close scrutiny of records relevant to ASIS's compliance with the privacy rules.

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

I will complete the inquiry into OSA policy, procedures and practices in DSD (as well as DIGO and DIO).

My office will continue to access and review each DSD submission to the Minister for Defence seeking an MA under the ISA.

We will continue to monitor DSD's compliance with its obligations under the DSD privacy rules.

We 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.

I will continue to address DSD training courses and other forums on accountability.

It is my intention to visit DSD or DSD related sites in Australia, as the opportunity presents.

DIGO

I will complete the inquiry into OSA policy, procedures and practices in DIGO (as well as DSD and DIO).

My office will review all submissions made by DIGO to the Minister for Defence seeking an MA under the ISA.

We will review internal submissions made to Director DIGO specifically seeking authorisation in respect of Australian territory or Australian interests.

We will closely monitor compliance with the DIGO privacy rules.

We will conduct meetings approximately every two months at DIGO Headquarters to discuss issues arising out of the above inspection activities, and to discuss matters of common interest with relevant DIGO senior managers.

ONA

I intend to complete the inquiry I commenced in the second half of this reporting period into the independence and propriety of ONA's assessment work.

I will meet with Director-General ONA on an occasional basis, to discuss matters affecting his agency, or the wider AIC, as circumstance dictates.

We will also closely monitor the application of ONA's privacy guidelines.

DIO

I will complete the inquiry into OSA policy, procedures and practices in DIO (as well as DSD and DIGO).

Following a foreshadowed briefing on the framework for ensuring the integrity of DIO assessments, I will contemplate whether any further activity on my part is warranted.

My office will regularly review DIO's compliance with the recently issued DIO privacy guidelines. It is my intention to meet with DIO senior management either prior to, or after, each privacy guidelines related visit we undertake to DIO headquarters.

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 during the first half of the new reporting period.

Corporate and communication

Support from PMC and DSD

My office relies on the assistance of PMC in handling staff and other administration issues and in providing general support. This support is provided on the basis that we are a very small portfolio agency and collocated with PMC.

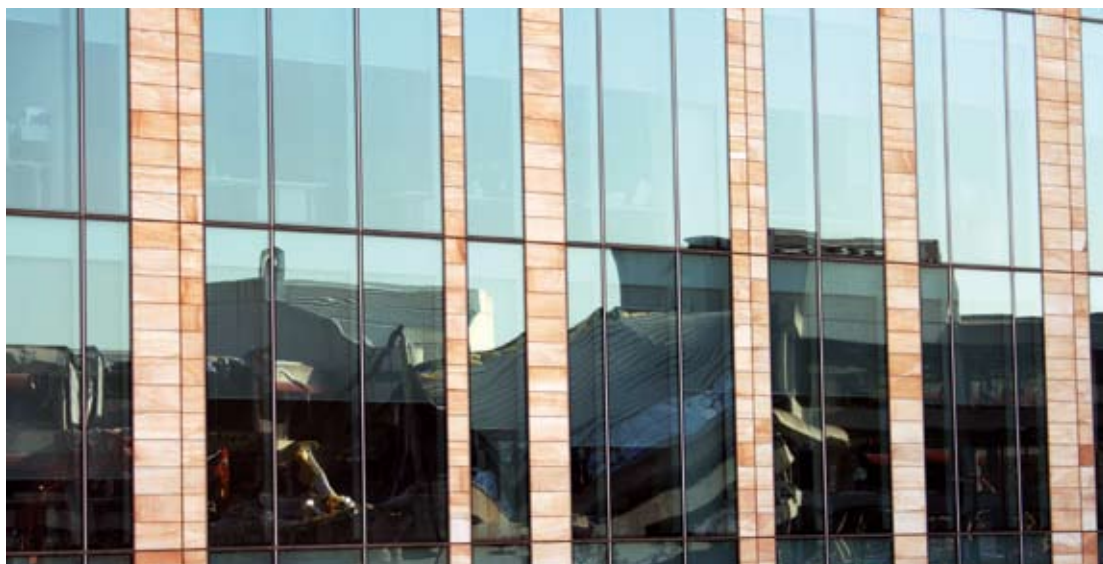
In 2006–07 the office made a \$45 000 (GST exclusive) payment to the PMC in recognition of the increasing costs associated with the support provided to the office. The current arrangement works well and I am appreciative of PMC's continued support.

On 16 February 2007 my office relocated with PMC to its new premises at One National Circuit Barton. In recognition of the additional costs associated with relocating our office, a one-off payment of \$29 934 (GST exclusive) was made to PMC.

The other major provider of 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.

Corporate governance

The office has an Audit Committee chaired by me and which also includes an external member from PMC. The committee considers corporate governance issues such as financial compliance, internal and external audit findings, fraud and risk management, occupational health and safety, and significant financial issues.



Demolition of the old PM&C Building reflected in the windows of the new Building

The expansion of the office has allowed me to engage an additional staff member who assists me in the overall corporate management of the office.

The small size of the office lends itself to a collegiate approach to dealing with workplace issues. Whole of agency meetings are held frequently and all staff have direct access to me on a daily basis.

Disaster recovery plan/business continuity plan

The office has its own disaster recovery/business continuity plan to ensure the continued operation of the office in the event of a disaster. This plan is reviewed periodically to ensure its currency.

The office has also been included in the PMC Pandemic Plan.

Fraud control

I am satisfied that OIGIS has in place appropriate fraud control mechanisms that meet the needs of the agency and comply with the Commonwealth Fraud Control Guidelines. The office has a current Fraud Control Plan 2006-2008.

Staffing and resources

There were a number of changes to the staffing composition of the office during the reporting period, relating to the staffing of three newly created positions.

Salary ranges are aligned with those under the PMC collective agreement. Salaries are formally reviewed in June each year.

Composition of the office

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 (from 4 June 2007)

- Senior Investigation Officers
 - Ms Jane Trevor
 - Ms Samantha Clark
- Senior Review Officer
 - Ms Lisa Buckingham
- Office Accountant
 - Ms Jackie McRae (from 2 April 2007)
- Personal Assistant to the Inspector-General
 - Ms Jodie Williams
- Office Manager and Monitoring Officer
 - Ms Robyn Kelly
- Administration Officer
 - Mrs Jocelyn Yosef (from 12 June 2007)

Performance pay

OIGIS staff have indicated that they do not wish to participate in a performance based pay scheme. Accordingly, no staff members were allocated performance based pay during the reporting period.

Workplace agreements

The *Workplace Relations Act 1996* established a framework in which agencies are required to directly negotiate agreements on pay and conditions matters with their staff.

All staff have entered into individual Australian Workplace Agreements. These agreements are subject to periodic review.

Workplace diversity

In such a small workplace the background, skills, talents and viewpoints of each employee are recognised and highly valued.

The main objective of the office is to provide assurance that the intelligence and security agencies act legally, ethically and with propriety. As such each member of my staff and I are committed to fostering and demonstrating such values within our own workplace.

Disability strategy

The office is committed to its responsibilities under the *Disability Discrimination Act 1992* and the Commonwealth Disability Strategy.

Occupational health and safety

SRC Solutions Pty Ltd facilitated workplace inspections and prior to our office's relocation, work space audits. While a work space inspection of the new premises did not take place during the reporting period, staff were encouraged to identify any occupational health and safety matters. As a result PMC were notified of a small number of matters. There was one outstanding item at the end of the reporting period. The issue related to a building fitting and PMC instigated a trial to ascertain the best long term solution. At the time of writing this report it is anticipated that the issue will be resolved shortly. No directions or notices were issued to my office under the *Occupational Health and Safety (Commonwealth Employment) Act 1991* (as amended).

The results of workplace inspections were reported to the office Audit Committee.

There were no incidents reported to Comcare Australia under the reporting requirements of section 68 of the OH&S Act.

Under the SRC Solutions contract provisions, members of the office are able to participate in health week activities and the influenza vaccination program.

From time to time, PMC offers organised exercise classes for staff which are also available to my office.

Management of human resources

The small size of the office necessitates that all staff be exposed to a variety of work and developmental activities. There are also annual staff performance assessment meetings at which development needs and how they can be met, are discussed. Staff attend relevant courses and information sessions in line with these performance assessment discussions.

Purchasing

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

Consultancy services and contract services

The office has only a small need for consultancies and contracts each year. Information on expenditure on contracts and consultancies is available on the AusTender website <<http://www.tenders.gov.au>>.

Consultancies

Generally a small number of consultants are engaged each year by the office on an as needed 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 2006–07 one new consultancy contract was entered into. The end date for this contract is 30 June 2007 but that contract was extended for a further three months on 28 August 2007.

There was also an ongoing consultancy contract which operated from 2005–06 into 2006–07. Payments under these contracts for the 2006–07 financial year (including superannuation) totalled \$42 292.

The same consultant was engaged for the above two contracts to conduct specialist operational audits and special project work. The selection method was direct sourcing with the consultant selected on the basis of experience, independence and specialist expertise in conducting similar audits.

In summary, there was \$42 292 in consultancy expenditure in 2006–07. Note this expenditure included superannuation payments required under legislation.

A consultancy services table is at Annex 2. The office policy is set out above.

Contract services

Nexis Accountants was engaged to provide financial services in 2006–07 at a total value of \$17 325 (GST inclusive). In 2005–06 accountancy services were purchased to the value of \$19 580. These services included the production of monthly and annual financial statements on actuals and bi-annual financial estimates.

Legal services

Legal advice is obtained from the Australian Government Solicitor (AGS). In 2006–07 OIGIS paid for four separate AGS legal advices at a combined cost of \$3 339 GST inclusive (2005–06: \$40 006). My office did not engage any other solicitors or any counsel during the reporting period, and there are no internal legal services.

Energy saving measures

The office through its collocation with PMC continues to benefit from that Department's commitment to energy saving measures. 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 addressed in this report. The new premises incorporate many energy efficiencies. Details of these measures are contained in PMC's 2006–07 annual report.

The office uses an 80–20 (80 per cent recycled–20 per cent new/virgin paper) for photocopying, facsimile report and document printing and purchases recycled paper writing pads. Where possible documents are printed or reproduced double-sided (that is, using both sides of the paper). The empty toner cartridges from the unclassified facsimile are recycled. The office uses PMC waste recycling services for plastic, glass and unclassified paper waste.

During the reporting period the office leased a fleet vehicle with an overall green vehicle rating of three and a half stars (out of a possible five star rating).

Social justice: access and equity

As stated earlier, the OIGIS seeks to provide assurance that each of Australia's intelligence and security agencies act legally, ethically and with propriety. Respect for these fundamental principles fosters an awareness and appreciation of social justice issues.

The office brochure is now available in 16 languages (Arabic, Chinese – simplified, Chinese – traditional, English, Farsi, Filipino, Greek, Hindi, Indonesian, Italian, Pushto, Sinhalese, Spanish, Turkish, Urdu and Vietnamese).

Copies of these brochures are available on request from our office (individual and community group requests are welcomed), via the office's website <<http://www.igis.gov.au>> and through some community centres. In addition the office accepts calls from members of the public accessing the Translation and Interpreting Service (through the Department of Immigration and Citizenship).

During the reporting period planning commenced to make the office's website more user friendly, more user focused and offer better access to information.

Internet presence

The IGIS website <<http://www.igis.gov.au>> provides information about the office, including copies of previous annual reports which include as annexes, publicly released reports on inquiries conducted and occasional statements about current activities.

Numerous inquiries about the work of the office are received via our

e-mail facility <info@igis.gov.au>.

Occasionally members of the public use this facility to provide 'tip-off' information regarding suspicious persons and the like. In such cases we ordinarily pass this information on to the National Security Hotline (NSH).

The NSH is the appropriate body to process and handle such information in the first instance. The NSH can be reached by phoning 1800 123 400. This is a freecall for any person calling from within Australia. E-mail messages to NSH can be sent to <hotline@nationalsecurity.gov.au>.

The office also occasionally receives concerns about, or requests to investigate, suspect e-mails soliciting

personal information or banking details. In most cases we advise that the e-mails in question are obviously part of a hoax or scam and can safely be ignored. In some cases the offending e-mail will be referred to the AFP's High Tech Crime Centre.

Media

Intelligence matters continued to be very much to the fore during the period covered by this report. Not surprisingly there was intense media interest in some subjects in which the IGIS played a part or otherwise has a direct interest.

In cases where the fact that the IGIS is conducting an inquiry has been made public, in accordance with the IGIS Act the practice is not to discuss the particulars of that inquiry beyond process issues and the formal requirements of the IGIS Act.

Advertising and market research

OIGIS incurred no expenditure on general advertising or advertising campaigns during the reporting period.

Freedom of information

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

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 – General Matters' and the 'Parliament and Legislation' chapters of this report.

Summary of the office's financial performance and resources for outcomes.

The office has one outcome and one output.

	2006–07 Outcome 1	2006–07 Output 1
Revenue and Expenses	\$	\$
Operating revenues		
Revenues from government (Budget and Additional Estimates Appropriations)	1 485 000	1 485 000
Other income (Resources received free of charge)	93 000	93 000
Total operating revenues	1 578 000	1 578 000
Operating expenses		
Employees	905 112	905 112
Suppliers	432 873	432 873
Assets written-off	-	-
Net losses from sale of assets	9 676	9 676
Equipment depreciation	28 743	28 743
Total operating expenses	1 376 404	1 376 404
OPERATING RESULT	201 596	201 596

In 2006–07, the office received an operating appropriation of \$1.485 million as shown in the previous table. The major components of 2006–07 expenditure were:

- 66% employee expenses
- 32% supplier expenses, and
- 2% depreciation expense.

The 32% supplier expenses outlined above consist of:

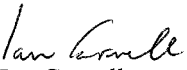
- 69% other goods and services
- 20% resources received free of charge
- 10% payment to PMC, and
- 1% Comcare premium.

The office realised an operating surplus of \$201 596 in 2006–07.

Financial statements

STATEMENT BY THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2007 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

4 September 2007



INDEPENDENT AUDITOR'S REPORT

To the Prime Minister

Matters relating to the Electronic Presentation of the Audited Financial Statements

This auditor's report relates to the financial statements published on the website of the Office of the Inspector-General of Intelligence and Security for the year ended 30 June 2007. The Inspector-General of Intelligence and Security is responsible for the integrity of the web site.

This auditor's report refers only to the primary statements, schedules and notes named below. It does not provide an opinion on any other information which may have been hyperlinked to/from the audited financial statements.

If users of this report are concerned with the inherent risks arising from electronic data communications they are advised to refer to the hard copy of the audited financial statements in the Office of the Inspector-General of Intelligence and Security's annual report.

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 2007, which comprise: a Statement by the Inspector-General of Intelligence and Security; income statement; balance sheet; statement of changes in equity; cash flow statement; schedules of commitments, contingencies and a summary of significant accounting policies; and other explanatory notes.

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* and the Australian Accounting Standards (including 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 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

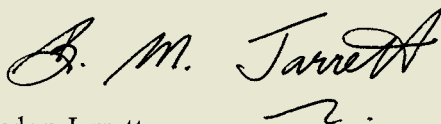
In conducting the audit, I have followed the independence requirements of the Australian National Audit Office, which incorporate the ethical requirements of the Australian accounting profession.

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 Order under the *Financial Management and Accountability Act 1997*, and the Accounting Standards (including the Australian Accounting Interpretation);
- (b) give a true and fair view of the matters required by the Finance Minister's Order, including the Office of the Inspector-General of Intelligence and Security's position as at 30 June 2007 and of its financial performance and its cash position for the year then ended.

Australian National Audit Office

A handwritten signature in black ink that reads "B. M. Jarrett". The signature is written in a cursive style with a large, sweeping flourish at the end.

Brandon Jarrett
Executive Director

Delegate of the Auditor-General

Canberra
4 September 2007

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY
INCOME STATEMENT
for the year ended 30 June 2007

Income Statement	Notes	2006-07 \$	2005-06 \$
INCOME			
Revenues from ordinary activities			
Revenues from Government	2A	<u>1 485 000</u>	1 124 000
Total Revenues from ordinary activities		<u>1 485 000</u>	<u>1 124 000</u>
Gains			
Resources received free of charge	2B	<u>93 000</u>	72 925
Total Gains		<u>93 000</u>	<u>72,925</u>
TOTAL INCOME		<u>1 578 000</u>	<u>1 196 925</u>
EXPENSES			
Employees	3A		
Remuneration		738 462	702 662
Superannuation		<u>166 650</u>	140 949
Total employees		<u>905 112</u>	843 611
Suppliers			
Resources received free of charge		93 000	72 925
Comcare premium	3B	2 750	2 519
Other goods and services	3B	<u>337 123</u>	219 223
Total suppliers		<u>432 873</u>	294 667
Net losses from sale of assets	3D	-	2 099
Assets written off	3E	9 676	-
Equipment depreciation	3C	<u>28 743</u>	35 902
TOTAL EXPENSES		<u>1 376 404</u>	<u>1 176 279</u>
OPERATING RESULT		<u>201 596</u>	<u>20 646</u>

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

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY
BALANCE SHEET
as at 30 June 2007

Balance Sheet	Notes	2006-07 \$	2005-06 \$
ASSETS			
Financial Assets			
Cash and cash equivalents	4A	293 105	372 850
Receivables - current	4B		
Appropriations receivable		797 800	417 000
GST receivable		2 452	2 444
Other debtors		77 339	22 140
Total receivables		<u>877 591</u>	<u>441 584</u>
Total financial assets		<u>1 170 697</u>	<u>814 434</u>
Non-financial assets			
Infrastructure, plant and equipment	5A	33 741	72 336
Other non financial assets			
Prepayments	5B	-	494
Total non-financial assets		<u>33 741</u>	<u>72 830</u>
TOTAL ASSETS		<u>1 204 438</u>	<u>887 264</u>
LIABILITIES			
Provisions			
Employee provisions	7A	596 148	493 769
Total provisions		<u>596 148</u>	<u>493 769</u>
Payables			
Suppliers	6A	46 036	25 913
Total payables		<u>46 036</u>	<u>25 913</u>
TOTAL LIABILITIES		<u>642 184</u>	<u>519 682</u>
Net Assets		<u>562 254</u>	<u>367 582</u>
EQUITY			
Asset revaluation reserve		2 511	9 435
Contributed equity		402 000	402 000
Retained Earnings		157 743	(43 853)
TOTAL EQUITY		<u>562 254</u>	<u>367 582</u>
Current Assets		1 170 697	814 928
Non-Current Assets		33 741	72 336
Current Liabilities		614 025	508 745
Non-Current Liabilities		28 159	10 937

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

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY
STATEMENT OF CASH FLOWS
for the year ended 30 June 2007

Cash Flows	Notes	2006-07 \$	2005-06 \$
OPERATING ACTIVITIES			
Cash received			
Appropriations		1 104 200	1 015 000
Net GST refunds		15 742	23 318
Other cash received		34 120	-
Total cash received		<u>1 154 062</u>	<u>1 038 318</u>
Cash used			
Employees		(892 840)	(755 390)
Suppliers		(259 283)	(254 960)
Other Cash Used		(74 934)	-
Total cash used		<u>(1 227 057)</u>	<u>(1 010 350)</u>
Net cash used from operating activities	8	<u>(72 995)</u>	<u>27 968</u>
INVESTING ACTIVITIES			
Cash received			
Proceeds from sales of equipment		-	674
Total cash received		<u>-</u>	<u>674</u>
Cash used			
Purchase of equipment		(6 750)	(2 252)
Total cash used		<u>(6 750)</u>	<u>(2 252)</u>
Net cash used from investing activities		<u>(6 750)</u>	<u>(1 578)</u>
FINANCING ACTIVITIES			
Cash received			
Equity injection		-	-
Total cash received		<u>-</u>	<u>-</u>
Cash used			
Return of equity		-	(66 000)
Total cash used		<u>-</u>	<u>(66 000)</u>
Net cash used from financing activities		<u>-</u>	<u>(66 000)</u>
Net increase/(decrease) in cash held		<u>(79 745)</u>	<u>(39 610)</u>
Cash at beginning of reporting period		<u>372 850</u>	<u>412 460</u>
Cash at the end of the reporting period	8	<u><u>293 105</u></u>	<u><u>372 850</u></u>

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

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY
STATEMENT OF CHANGES IN EQUITY
For the year ended 30 June 2007

Item	Retained Earnings		Asset Revaluation Reserve		Contributed Equity/Capital		Total Equity	
	2007	2006	2007	2006	2007	2006	2007	2006
	\$	\$	\$	\$	\$	\$	\$	\$
Opening Balance	(43 853)	(64 499)	9 435	9 435	402 000	468 000	367 582	412 936
Net Operating Result	201 596	20 646	-	-	-	-	201 596	20 646
Total income and expenses	201 596	20 646					201 596	20 646
Asset Revaluation Movements			(6,924)				(6,924)	
Transactions with Owners	-	-	-	-	-	-	-	-
Distributions to owners	-	-	-	-	-	-	-	-
Returns of Capital	-	-	-	-	-	(66 000)	-	(66 000)
Contributions by Owners	-	-	-	-	-	-	-	-
Appropriation (equity injection)	-	-	-	-	-	-	-	-
	-	-	-	-	-	-	-	-
Sub-total Transaction with Owners	-	-	-	-	-	(66 000)	-	(66 000)
Transfers between equity components	-	-	-	-	-	-	-	-
Closing balance at 30 June	157 743	(43 853)	2 511	9 435	402 000	402 000	562 254	367 582

STATEMENT OF COMMITMENTS AND CONTINGENCIES*as at 30 June 2007*

The Office had no contingencies to report in either 2005-06 or in 2006-07.

	2007	2006
	\$	\$
BY TYPE		
Commitments Receivable		
GST recoverable on commitments	8	1
Total Commitments Receivable	<u>8</u>	<u>1</u>
Capital Commitments		
Infrastructure, plant and equipment	58	-
Total Capital Commitments	<u>58</u>	<u>-</u>
Other Commitments		
Operating Leases	119	76
Total Other Commitments	<u>119</u>	<u>76</u>
Net Commitments by Type	<u>169</u>	<u>75</u>
BY MATURITY		
Commitments Receivable		
Operating Lease income		
One year or less	2	1
From one to five years	1	-
Over five years	-	-
Total operating lease income	<u>3</u>	<u>1</u>
Other Commitments Receivable		
One year or less	5	-
From one to five years	-	-
Over five years	-	-
Total other commitments receivable income	<u>5</u>	<u>-</u>
Commitments Payable		
Capital Commitments		
One year or less	58	-
From one to five years	-	-
Over five years	-	-
Total Capital Commitments	<u>58</u>	<u>-</u>
Operating Lease Commitments		
One year or less	64	76
From one to five years	55	-
Over five years	-	-
Total Operating Lease Commitments	<u>119</u>	<u>76</u>
Net Commitments by Maturity	<u>169</u>	<u>75</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 office is to meet the following outcome:

Assurance that Australia's intelligence agencies act legally, ethically and with propriety.

The office has one output:

Inspect, inquire into, and report on, the activities of the intelligence and security agencies.

In previous reporting periods, the office had two outputs (Output 1:- Inspect and report on the activities of the intelligence and security agencies, Output 2: - Conduct inquiries and provide a complaint resolution service) which were combined into one output as part of the 2005-06 Budget process.

The decision to change the output structure was made for three main reasons:

- to recognise that reporting responsibilities apply to inquiry activities, not just to inspection activities
- to recognise that complaints are handled as inquiries and are not a separate activity from inquiries, and
- to recognise that inspection activities can potentially lead to inquiries, and are in turn influenced by inquiries.

Under the revised output structure, the office will continue to carry out all the activities performed under the two former outputs, including complaints resolution.

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 statements have been prepared in accordance with:

- Finance Minister's Orders (being the *Financial Management and Accountability Orders (Financial Statements for reporting periods ending on or after 1 July 2006)*)
- Australian Accounting Standards issued by the Australian Accounting Standards Board that apply for the reporting period, and
- Interpretations issued by the AASB and Urgent Issues Group that apply for the reporting period.

The Income Statement and Balance Sheet have been prepared on an accrual basis and are in accordance with the historical cost convention, except for certain assets which have been noted at fair value. 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.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2007

Note 1 - Summary of Significant Accounting Policies (continued)

1.3 Statement of Compliance

Australian Accounting Standards require a statement of compliance with International Financial Reporting Standards (IFRSs) to be made where the financial report complies with these standards. Some Australian equivalents to IFRSs and other Australian Accounting Standards contain requirements specific to not-for-profit entities that are inconsistent with IFRS requirements. This Agency is a not-for-profit entity and has applied these requirements, so while this financial report complies with Australian Accounting Standards including Australian Equivalents to International Financial Reporting Standards (AEIFRSs) it cannot make this statement.

Adoption of new Australian Accounting Standard Requirements

No accounting standard has been adopted earlier than the effective date in the current period.

Other effective requirement changes

The following amendments, revised standards or interpretations have become effective but have had no financial impact or do not apply to the operations of the Agency:

Amendments:	2005-1 Amendments to AASBs 1, 101, 124
	2005-6 Amendments to AASB 3
	2006-1 Amendments to AASB 121
	2006-3 Amendments to AASB 1045
Interpretations:	UIG 4 Determining whether an Arrangement contains a Lease
	UIG 5 Rights to Interests arising from Decommissioning, Restoration and Environmental Rehabilitation Funds
	UIG 7 Applying the Restatement Approach under AASB 129 Financial Reporting in Hyperinflationary Economies
	UIG 8 Scope of AASB 2
	UIG 9 Reassessment of Embedded Derivatives

Future Australian Accounting Standard Requirements

The following standards and interpretations have been issued but are not applicable to the operations of the Agency:

- AASB 7 Financial Instruments
- AASB 1049 Financial Reporting of General Government Sectors by Governments
- UIG 10 Interim Financial Reporting and Impairment

1.4 Revenue

Revenues from Government

The full amount of the departmental appropriation for office 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.

Note 1 - Summary of Significant Accounting Policies (continued)

1.5 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 2006-07 are office space (from the Department of the Prime Minister and Cabinet) and the installation and maintenance of the OIGIS owned internal secure computer networks (from Defence Signals Directorate). Other resources received free of charge include auditor remuneration as disclosed in Note 11.

1.6 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 office 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 office'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 2007. The estimate of the present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

Superannuation

Liabilities for services rendered by employees are recognised at the reporting date to the extent that they have not been settled.

Liabilities for wages and salaries (including non-monetary benefits), annual leave, sick leave are measured at their nominal amounts. Other employee benefits expected to be settled within 12 months of the reporting date are also measured at their nominal amounts.

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

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2007

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.

1.7 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.

All receivables are with Commonwealth entities. Credit terms are net 30 days (2005–06: 30 days).

1.8 Trade Creditors & Accrued Expenses

Trade creditors and accruals are recognized at their nominal amounts, being the amounts at which the liabilities will be settled. Liabilities are recognized to the extent that the goods or services have been received (and irrespective of having been invoiced).

With the exception of one creditor, the remaining creditors are entities that are not part of the Commonwealth legal entity. Settlement is usually made net 30 days.

1.9 Cash

Cash means notes and coins held and any deposits held at call with a bank or financial institution. Cash is recognized at its nominal amount.

1.10 Acquisition of Assets

Assets are recorded at cost on acquisition.

1.11 Infrastructure, Plant and Equipment

The office's fixed assets are comprised of office equipment and software only.

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).

Revaluations

Plant and equipment are carried at valuation. Fair values for the one class of asset have been determined by market selling price. With the exception of software which is carried at cost.

Frequency and Conduct

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 2007 by an independent valuer.

Note 1 - Summary of Significant Accounting Policies (continued)

Revaluation adjustments are made on a class basis (the office has only one asset class). 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 plant and equipment assets are written-off to their estimated residual values over their estimated useful lives to the office 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.

1.12 Impairment of Non-Current Assets

All assets were assessed for impairment at 30 June 2007 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.

1.13 Taxation

The office 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.

1.14 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.

1.15 Comparative Figures

Comparative figures have been adjusted to conform to changes in presentation in these financial statements where required.

1.16 Rounding

Amounts have been rounded to the nearest dollar.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2007

Note 2 – Income

Revenue

Note 2A – Revenues from Government

	2007	2006
	\$	\$
<u>Revenue from Government</u>		
Appropriations for outputs	1 485 000	1 124 000
Total revenue from government	1 485 000	1 124 000

Gains

Note 2B – Other Gains

	2007	2006
	\$	\$
Other Gains		
Resources Received free of charge	93 000	72 925
Total Other Gains	93 000	72 925

Note 3 – Expenses

Note 3A – Employee Benefits

	2007	2006
	\$	\$
Wages and salaries	726 444	617 476
Superannuation	166 650	140 949
Leave and other entitlements	12 018	85 186
Separation and redundancies	-	-
Total employee benefits	905 112	843 611

Note 3B - Suppliers

	2007	2006
	\$	\$
Provision of goods – related entities		
Provision of goods – external entities	236 845	148 691
Rendering of services – related entities	138 000	118 925
Rendering of services – external entities	55 278	24 532
Workers compensation premiums	2 750	2 519
Total supplier expenses	432 873	294 667

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2007

	2007 \$	2006 \$
Note 3C – Depreciation and amortisation		
Depreciation – Infrastructure, plant and equipment	28 743	35 902
Total Depreciation	28 743	35 902
	2007 \$	2006 \$
Note 3D – Net Losses from Sale of Assets		
Infrastructure, plant and equipment:		
Proceeds from sale	-	832
Carrying value of assets sold	-	2 690
Selling expense	-	241
Total losses from asset sales	-	2 099
Note 3E – Assets Written Off		
Infrastructure, plant and equipment	9 676	-
Total Assets Written Off	9 676	-
Note 4 – Financial Assets		
	2007 \$	2006 \$
Note 4A – Cash and cash equivalents		
Cash on hand or on deposit	293 105	372 850
Total cash and cash equivalents	293 105	372 850
	2007 \$	2006 \$
Note 4B – Trade and other receivables		
Appropriations Receivable:		
For existing outputs	797 800	417 000
Total appropriations receivable	797 800	417 000
GST receivable from the Australian Taxation Office	2 452	2 444
Other receivables:		
Department of Defence	77 339	22 140
Total other receivables	79 791	24 584
Total trade and other receivables (gross)	877 591	441 584
Less Allowance for Doubtful Debts	-	-
Total trade and other receivables (net)	877 591	441 584
Receivables are aged as follows:		
Not overdue	877 591	441 584

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2007

Note 5 – Non-Financial Assets

Note 5A – Infrastructure, plant and equipment

	2007	2006
	\$	\$
Infrastructure, plant and equipment		
Infrastructure, plant and equipment:		
- gross carrying value (at fair value)	31 200	2 385
- accumulated depreciation	-	(1 765)
Infrastructure, plant and equipment		
- gross carrying value (at cost)	5 769	142 706
- accumulated depreciation	(3 228)	(70 990)
Total Infrastructure, Plant and Equipment (non-current)	33 741	72 336

Note 5B – Other Non-Financial Assets

	2007	2006
	\$	\$
Other Non-Financial Assets		
Prepayments	-	494
Total Other Non-Financial Assets	-	494

Note 5C – Analysis of Infrastructure, plant and equipment

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	145 092
Accumulated depreciation	(72 756)
Opening Net book value as at 1 July 2006	72 336
Additions	
by purchase	6 750
Depreciation expense	(28 743)
Disposals	
Net cost of disposals	(9 677)
Revaluations and impairments through equity	(6,924)
Net Book Value 30 June 2007	33 742
As at 30 June 2006	
Gross book value	36 970
Accumulated depreciation	(3 228)
Net book value as at 30 June 2006	33 742

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2007

Table A – Reconciliation of the Opening and Closing Balances of Infrastructure, Plant and Equipment (2005-06)

Item	Infrastructure Plant and Equipment
As at 1 July 2005	
Gross book value	147 895
Accumulated depreciation	(39 014)
Opening Net book value as at 1 July 2005	108 881
Additions	
by purchase	2 047
Depreciation expense	(35 902)
Disposals	
Book value of disposals	(4 850)
Accumulated depreciation on disposals	2 160
As at 30 June 2006	
Gross book value	145 092
Accumulated depreciation	(72 756)
Net book value as at 30 June 2006	72 336

All revaluations are independent and are conducted in accordance with the revaluation policy stated at Note 1. In 2006-07, the revaluations were conducted by an independent valuer A.F. Graham (Certified Practicing Valuer).

Note 6 – Payables

	2007 \$	2006 \$
<u>Note 6A – Suppliers</u>		
Trade creditors	46 036	25 913
Total Suppliers	46 036	25 913
Supplier payables are represented by:		
Current	46 036	25 913
Non-current	-	-
Total supplier payables	46 036	25 913

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2007

Note 7 – Provisions

	2007	2006
	\$	\$
<u>Note 7A – Employee provisions</u>		
Salaries and wages	7 016	5 030
Leave	545 353	457 410
Superannuation	41 795	31 012
Other – Fringe Benefits Tax	1 984	317
Total Employee Provisions	596 148	493 769
Employee provisions are represented by:		
Current	567 989	482 832
Non-current	28 159	10 937
Total employee provisions	596 148	493 769

Note 8 – Cash Flow Reconciliation

	2006-07	2005-06
	\$	\$
Reconciliation of Cash and cash equivalents as per Balance Sheet to Cash flow statement		
Report cash and cash equivalents as per:		
Cash Flow Statement	293 105	372 850
Balance Sheet	293 105	372 850
Difference	-	-
Reconciliation of net surplus to net cash from operating activities:		
Operating result	201 596	20 646
Depreciation	28 743	35 902
Gain/Loss on disposal of assets	9 676	2 221
Write-off of assets	-	-
Increase/(Decrease) in provision for employee liabilities	102 376	90 740
Increase/(Decrease) in supplier trade creditors	20 126	8 459
(Increase)/Decrease in appropriations receivables	(380 800)	(109 000)
(Increase)/Decrease in other assets	(55 198)	(22 146)
(Increase)/Decrease in other prepayments	494	-
(Increase)/Decrease in GST receivable	(8)	1 146
(Increase)/Decrease in transfers to the Official Public Account	-	-
Net cash flow from operating activities	(72,995)	27 968

Note 9 – Contingent Liabilities and Assets

The Agency had no contingent liabilities or contingent assets at the reporting date.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2007

Note 10 – Executive Remuneration

Executive Remuneration	2006-07	2005-06
Number of executives in the range \$340 000 to \$399 999:	1	1
For privacy reasons the aggregate amount of executive remuneration is not shown		
The aggregate amount of separation and redundancy/termination benefit payments during the year to executives shown above:	Nil	Nil

Note 11 – Remuneration of Auditor

Financial statement audit services are provided free of charge to the office. No other services were provided by the Auditor-General.

Remuneration of Auditor	2006-07	2005-06
The fair value of audit services provided was:	\$14 100	\$16 500

Note 12 – Staffing Level

The average staffing level for the office in 2006-07 was 7 (2005-06: 6).

Note 13 – Financial Instruments

Note 13A – Interest Rate Risk

Financial Instruments (Recognised)	Floating interest rate		Non-Interest Bearing		Total		Weighted Average Effective Interest Rate	
	06-07	05-06	06-07	05-06	06-07	05-06	06-07	05-06
	\$	\$	\$	\$	\$	\$	\$	\$
Financial Assets								
Cash on hand	-	-	55	36	55	36	n/a	n/a
Cash at Bank	-	-	293 050	372 814	293 050	372 814	n/a	n/a
Receivables for goods or services (gross)	-	-	877 591	441 584	877 591	441 584	n/a	n/a
Total			1 170 696	814 434	1 170 696	814 434		
Total Assets					1 204 438	887 264		
Financial Liabilities								
Trade Creditors	-	-	46 036	25 913	46 036	25 913	n/a	n/a
Other Payables	-	-	-	-	-	-	n/a	n/a
Total	-	-	46 036	25 913	46 036	25 913		
Total Liabilities					642 184	519 683		

No funds were invested at a fixed interest rate.

Note 13B – Net Fair Value of Financial Assets and Liabilities

The office'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 2007

Note 13C – Credit Risk Exposure

The office's maximum exposure to credit risk at reporting date in relation to each class of recognised financial assets is the carrying amount of those assets as indicated in the Balance Sheet. The office has no significant exposure to any concentrations of credit risk.

Note 14 – Special Accounts

The office 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 15 – Appropriations

Note 15A – Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund for Ordinary Annual Services Appropriations (Acts 1 and 3)

Particulars	Total
Year Ended 30 June 2007	\$
Balance carried from previous year	459 119
Appropriation Act (No.1) 2006-2007	1 485 000
Appropriation Act (No.3) 2006-2007	-
Section 31 receipts (FMA Act)	
GST credits (FMA s30A)	15 128
Total Appropriations available for payments	1 959 247
Payments made (GST inclusive)	1 192 929
Balance carried to next year	766 318
Represented by:	
Cash	274 066
Add: Receivables – Net GST Receivable from the ATO	2 452
Receivables – departmental appropriations	489 800
Total	766 318
Year Ended 30 June 2006	
Balance carried from previous year	322 827
Appropriation Act (No.1) 2005-2006	1 058 000
Appropriation Act (No.3) 2005-2006	66 000
GST credits (FMA s30A)	23 113
Section 31 receipts (FMA Act)	674
Total Appropriations available for payments	1 470 614
Payments made (GST inclusive)	1 011 495
Balance carried to next year	459 119
Represented by:	
Cash	347 675
Add: Receivables – Net GST Receivable from the ATO	2 444
Receivables – departmental appropriations	109 000
Total	459 119

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2007

Note 15 – Appropriations (continued)

Note 15B – Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund for Other than Ordinary Annual Services Appropriations (Acts 2 and 4)

Particulars	Total \$
Year Ended 30 June 2007	
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
Balance carried to next year	327 039
Represented by:	
Cash	19 039
Add: Receivables – Receivable from the Official Public Account	308 000
Total	327 039
Year Ended 30 June 2006	
Balance carried from previous year	401 222
Appropriation Act (No.2) 2005-2006	-
Appropriation Act (No.4) 2005-2006	-
Reallocation of prior year appropriation ¹	(66 000)
GST credits (FMA Act s30A)	205
Total Appropriations available for payments	335 427
Payments made (GST inclusive)	2 252
Balance carried to next year	333 175
Represented by:	
Cash	25 175
Add: Receivables – Receivable from the Official Public Account	308 000
Total	333 175

1. An equity injection of \$66 000 was received in the financial year ended 30 June 2001. The office did not spend any of this appropriation during prior years. The \$66 000 was reallocated to departmental operating expenses in 2005-06 by appropriating \$66 000 through Appropriation Act No.3, 2005-06 and applying to the Minister for Finance for an equivalent reduction in equity in 2005-06.

The office received \$402 000 as an equity injection in the financial year ended 30 June 2005. The office holds \$308 000 of this amount in the Official Public Account to partially fund the non-current portion of accrued leave liabilities. The office spent \$6 750 in 2006-07 and \$2 252 in 2005-06 (GST inclusive) from these appropriations.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the year ended 30 June 2007

Note 16 - Reporting of Outcomes

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

Note 16A – Net Cost of Outcome Delivery

The net cost of this outcome in 2006-07 was \$1 297 907 (Appropriation: \$1 485 000).

Note 16B – Agency Revenue and Expenses by Output Group

Revenue and Expenses	Output Group 1		OUTCOME TOTAL	
	2006-07	2005-06	2006-07	2005-06
	\$	\$	\$	\$
Operating revenues				
Revenues from government	1 485 000	1 124 000	1 485 000	1 124 000
Other income	93 000	72 925	93 000	72 925
Total operating revenues	1 578 000	1 196 925	1 578 000	1 196 925
Operating expenses				
Employees	905 112	843 611	905 112	843 611
Suppliers	432 873	294 667	432 873	294 667
Net losses from sale of assets	-	2 099	-	2 099
Assets written off	9 676	-	9 676	-
Equipment depreciation	28 743	35 902	28 743	35 902
Total operating expenses	1 376 404	1 176 279	1 376 404	1 176 279

Note 17 – Compensation and Debt Relief

No 'Act of Grace' payments were made during the reporting period, (2005-06: nil).

No waivers of amounts owing to the Commonwealth were made during the reporting period, (2005-06: nil).

No payments were made under the 'Defective Administration Scheme' during the reporting period, (2005-06: nil).

No payments were made under section 73 of the *Public Service Act 1999*, (2005-06: nil).

Annex 1 – Complaint and inquiry statistics

Annex 1, Table 1
IGIS Act inquiries actioned between 1 July 2006 – 30 June 2007

Agency	Source	Date of Receipt	Type of Inquiry ¹	Conclusion Notified	Current Status
ASIS	Public	23/05/06	Preliminary	01/09/06	Closed
ASIO	Public	09/06/06	Preliminary	20/09/06	Closed
ASIS	Employee	16/06/06	Preliminary	19/01/07	Closed
ASIO	Public	19/06/06	Preliminary	08/08/06	Closed
ASIO	Own motion	27/07/06	Full	18/01/07	Closed
ASIO	Public	27/07/06	Preliminary	24/08/06	Closed
ASIS	Public	22/08/06	Preliminary	08/11/06	Closed
ASIO	Public	25/09/06	Preliminary	18/01/07	Closed
ASIO	Public	31/10/06	Preliminary	11/12/06	Closed
ASIS	Public	03/11/06	Preliminary	15/12/06	Closed
ASIO	Ex-employee	07/11/06	Preliminary	13/04/07	Closed
DSD	Public	14/11/06	Preliminary	01/02/07	Closed
ASIO	Public	27/11/06	Full	02/04/07	Closed
ASIO	Public	08/12/06	Preliminary	21/12/06	Closed
ONA	Own motion	14/02/07	Full		Open
ASIO	Public	29/03/07	Preliminary		Open
DIG ²	Own motion	05/06/07	Full		Open

¹ 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.

² Defence Intelligence Group (comprising DSD, DIGO and DIO)

Annex 1 Table 2

Summary of concerns about agencies that were handled administratively 1 July 2006 to 20 June 2007

Agency	Number of Complaints	Source of Complaint			Type of Complainant	
		Public	Employee/ Ex-employee	Former Complainant	New Complaint	
ASIO	45	44	1	25	20	
ASIS	5	4	1	1	4	
DSD	1	1	0	1	0	
DIGO	1	1	0	0	1	
DIO	3	1	2	0	3	
ONA	1	1	0	0	1	
AIC	9	8	1	1	8	
Total	65	60	5	28	37	

Annex 1, Table 3

Immigration related concerns that were handled administratively 1 July 2006 to 30 June 2007

Visa Category	Migration Agent	Complainant	Complaint's spouse	Commonwealth Ombudsman	Total Complaints	Number closed as at 30/06/2007
Protection	14	4	1	3	22	19
Spouse	4	0	19	7	30	28
Skilled Migrant	2	2	0	2	6	5
Remaining Relative	1	1	0	0	2	1
Other	7	3	3	1	14	12
Total Complaints	28	10	23	13	74	65

Annex 2 – Consultancy services let during 2006–07

Consultant Name	Description	Contract Price	Selection Process	Justification
W J Blick	Specialist operational audits	\$16 132	Direct Sourcing	Need for specialised skills
W J Blick	Specialist operational audits and special project work	\$26 160	Direct Sourcing	Need for specialised skills

The selection method was direct sourcing. The consultant was selected on the basis of experience, independence and specialist expertise in conducting similar audits.

Annex 3 – IGIS inquiry into ASIO’s assessment of Mr Rhuhel Ahmed

Background

1. I received a written complaint on 27 November 2006 from a member of the public who was concerned about the denial of a visa to Mr Rhuhel Ahmed, the effect of which was to deny Mr Ahmed entry into Australia.
2. The decision to deny Mr Ahmed a visa was made by a delegate of the Secretary of the (then titled) Department of Immigration and Multicultural Affairs (DIMA), on the basis of an adverse security assessment made of Mr Ahmed by the Australian Security Intelligence Organisation (ASIO).
3. Media reporting around the time I received this complaint indicated that Mr Ahmed, who is a United Kingdom national, planned to visit Australia to promote the cinema release of a new film *“The Road to Guantanamo”*.
4. The film Mr Ahmed intended to promote recounts the story of Mr Ahmed and two fellow UK nationals who were captured in Afghanistan in 2001 and subsequently detained in the United States of America complex located at Guantanamo Bay, Cuba, until their eventual release in March 2004. The film, which was released in Australia, uses a mixture of traditional documentary form (i.e. interviews with the three key subjects) with dramatic recreations of particular events (performed by actors) to convey Mr Ahmed and his colleagues version of events.
5. The complainant who wrote to my office expressed concern that the ASIO assessment may have been politically driven to avoid embarrassment to the Australian and American

governments over issues such as the continuing detention of Mr David Hicks at Guantanamo Bay.

6. I decided to conduct an inquiry under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) into the matter and advised the Attorney-General and the Director-General of Security accordingly, on 29 November 2006.
7. Shortly thereafter my office received another 36 similarly expressed complaints on the matter, but the author of the first letter my office received has been taken as the principal complainant for the purposes of the IGIS Act.

Scope of inquiry

8. My jurisdiction in respect of ASIO security assessments of non-citizens was succinctly described by Madgwick J in *Leghaei v Director-General of Security* [2005] FCA 1576 as follows:

“Non-citizens etc. therefore have limited rights under the IGIS Act, in that while they may make complaints to the Inspector-General under s 11 of the IGIS Act, any consequent inquiry by the Inspector General must be within the latter’s functions (s 11(1)(b)). In the result, effectively, the only recourse a non-citizen etc. has under the IGIS Act is in relation to the matters contained in s 8(1)(a). Those matters may be summarised as legality, propriety and procedural efficacy. They do not include the merits of a security assessment.”

ASIO legislation

9. The functions of ASIO are prescribed at section 17 of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act).
10. One of the significant functions which ASIO is required to perform is set out at section 17(1)(c) of the ASIO Act, namely:

“to advise Ministers and authorities of the Commonwealth in respect of matters relating to security, in so far as these matters are relevant to their functions and responsibilities.”

11. “Security” is defined under section 4 of the ASIO Act as meaning:

“(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 sub paragraphs of paragraph (a).”

12. In addition to defining ASIO’s mandate, there is also a separate component of the ASIO Act which deals exclusively with the subject of security assessments (Part IV). This provides, among other things, that ASIO may make security assessments and assessments in the performance of its functions.

13. The terms “security assessments” and “assessments” are defined under section 35 of the ASIO Act in the following way:

“security assessment or assessment means a statement in writing furnished by the Organisation to a Commonwealth agency expressing any recommendation, opinion or advice on, or otherwise referring to, the question whether it

would be consistent with the requirements of security for prescribed administrative action to be taken in respect of a person or the question whether the requirements of security make it necessary or desirable for prescribed administrative action to be taken in respect of a person, and includes any qualification or comment expressed in connection with any such recommendation, opinion or advice, being a qualification or comment that relates or that could relate to that question.”

14. The term **prescribed administrative action** is also defined under section 35 of the ASIO Act and is taken to include:

“the exercise of any power, or the performance of any function, in relation to a person under the Migration Act 1958 or the regulations under that Act.”

ASIO Assessment

15. Mr Ahmed lodged an application for a Business (Short Stay) Visa in the United Kingdom on 16 October 2006, indicating that he wished to travel to Australia on 26 October 2006.

16. One of the requirements Mr Ahmed needed to satisfy for a visa to be issued is public interest criterion 4002 in Part 1 of Schedule 4 of the Migration Regulations. This provides as follows:

“4002 The applicant is not assessed by the Australian Security Intelligence Organisation to be directly or indirectly a risk to security, within the meaning of section 4 of the Australian Security Intelligence Organisation Act 1979.”

17. DIMA sought an assessment from ASIO, and this request was referred to the relevant work area within ASIO for consideration on 18 October 2006.

18. Security considerations preclude me from detailing the checks which the ASIO action officer undertook, but they were of the kind I would have expected to be done, and not otherwise.

19. The officer drafted an assessment and submitted it to a more senior ASIO officer on

25 October 2006. The senior officer approved the assessment the same day and advised DIMA that ASIO had assessed Mr Ahmed to be directly or indirectly a risk to Australian national security.

20. The consequential effect of ASIO's assessment, given the requirement cited in paragraph 16 above, was that Mr Ahmed was refused a visa.

Comments

21. One of the questions raised by the complainant was whether there was any political or external influence on the assessment.
22. There is no indication whatsoever in the records that there was such influence or attempt at such influence, nor have I found any such evidence in my investigation into this matter. The process followed was entirely normal and the staff concerned have assured me that the assessment was ASIO's judgement alone.
23. I also asked these staff for statutory declarations and each stated unequivocally in these statements that there had not been any attempt to improperly influence the assessment.
24. The material on which the assessment drew was relevant and apparently reliable. I am also satisfied that there was no inflation of the significance of the material in its use in the assessment.
25. As noted earlier, the central test applied was whether Mr Ahmed was directly or indirectly a threat to security, and this was legally correct. Although I am not empowered to make a merits-based assessment of Mr Ahmed's case, I can say that I am of the view that the material available to ASIO was sufficient for it to conclude that this test was met.
26. I would have preferred the assessment to have included more exposition of one element of the underlying reasoning. However, the conclusion reached was sufficiently justified.
27. I should note that independently of this particular inquiry ASIO has introduced enhancements to the way in which it approaches the structuring of the content of assessments and I am supportive of such action.

Conclusion

28. Taking into account all of the above circumstances, I conclude that ASIO acted legally and properly in making its assessment in respect of Mr Ahmed in October 2006.

Ian Carnell
Inspector-General of
Intelligence and Security

12 March 2007

Annex 4 – Statement of procedures – warrants issued under Division 3 of Part III, ASIO Act



Statement of Procedures — warrants issued under Division 3 of Part III

Australian Security Intelligence Organisation Act 1979

I, PHILIP MAXWELL RUDDOCK, Attorney-General, approve this Statement of Procedures under subsection 34C (4) of the *Australian Security Intelligence Organisation Act 1979*.

Dated 16 October 2006

PHILIP RUDDOCK
Attorney-General

1 Name of Statement of Procedures

This Statement of Procedures is the *Statement of Procedures — warrants issued under Division 3 of Part III*.

2 Commencement

This Statement of Procedures commences on the day after it is registered.

3 Revocation of Protocol

The Protocol:

(a) provided for in paragraph 34C(3)(ba) and subsection 34C(3A) of the *Australian Security Intelligence Organisation Act 1979* (as in force immediately before 19 June 2006); and

(b) that was tabled in the House of Representatives by the Minister on 12 August 2003 is revoked.

4 Definitions

In this Statement of Procedures:

ASIO Act means the *Australian Security Intelligence Organisation Act 1979*.

police officer and *prescribed authority* have the meanings given in section 34A of the ASIO Act.

subject means a person who is authorised to be questioned before a prescribed authority in accordance with a warrant issued under Division 3 of Part III of the ASIO Act.

5 General

The Director-General must, in relation to a warrant issued under Division 3 of Part III of the ASIO Act, maintain a written record of:

- (a) the identity of the subject;
- (b) the authority for the questioning or detention of the subject;
- (c) the place, date and time of questioning under the warrant and the details of any procedural time (calculated by reference to subsection 34R(13)); and
- (d) the place, date and time of detention (if any) and release of the subject;

The Director-General must annex this record to the report required to be made under section 34ZH.

6 Transport

The subject may be transported if:

- (a) the subject is authorised to be detained under a warrant issued under section 34G of the ASIO Act; or
- (b) the prescribed authority directs that the subject be detained.

A police officer must arrange any transportation required. The transportation must be safe and dignified.

A police officer must remain present during the transportation of any subject who is being detained.

The subject must not be transported in a vehicle with inadequate ventilation or light, or in a way which would expose the subject to unnecessary physical hardship.

7 Questioning

7.1 Manner

All persons present during questioning or any period of detention under a warrant must interact with the subject in a manner that is both humane and courteous, and must not speak to the subject in a demeaning manner.

The subject must not be questioned in a manner that is unfair or oppressive in the circumstances.

A police officer must remain present at all times during the questioning of the subject.

7.2 Language

Information must be given to the subject in a language the subject can understand.

An interpreter must be provided for a subject if the prescribed authority believes on reasonable grounds that the subject is unable, because of inadequate knowledge of the English language or a physical disability, to communicate with reasonable fluency in English in accordance with section 34M or 34N.

7.3 Explanation of the effect of a warrant

The prescribed authority must explain to a subject the effect of the warrant in accordance with section 34J, and must satisfy him or herself that the subject has understood the explanations given.

In particular, the prescribed authority must explain to the subject the use which may be made of any information or materials provided by the subject, including any derivative use for the purpose of criminal investigations.

The prescribed authority must also explain to the subject the effect of the non-disclosure obligations set out in section 34ZS, in particular how those obligations relate to the subject in the questioning and detention context.

The prescribed authority must explain to a subject the function or role of all persons present during questioning. The prescribed authority must also state his or her role in supervising the questioning of the person and in giving appropriate directions under section 34K in relation to the person.

7.4 Conditions

The subject must have access to fresh drinking water and clean toilet and sanitary facilities at all times during questioning.

The subject must not be questioned continuously for more than 4 hours without being offered a break.

Such break must, at a minimum, be of 30 minutes duration.

A subject may elect to continue questioning without taking a break, or after taking a break shorter than 30 minutes, provided the prescribed authority is satisfied that this is entirely voluntary.

8 Detention

8.1 When detention occurs

A subject is detained if:

- (a) the subject is brought before a prescribed authority in accordance with a warrant issued under section 34G; or
- (b) the prescribed authority directs that the subject be detained under section 34K.

For the purposes of section 34S of the ASIO Act, the detention of the subject of a warrant is continuous from the time the person is first detained until the person is released from detention in accordance with a direction of the prescribed authority.

8.2 Arrangements for detention

A police officer must make arrangements to take a subject into custody and for subsequent detention. These arrangements must be consistent with applicable police practices and procedures in relation to custody of persons, except if such practices are inconsistent with the terms of the warrant or this Statement of Procedures.

8.3 Police supervision

A police officer must supervise any detention that occurs under a warrant.

The prescribed authority is responsible for issuing directions on any matter relating to the detention of the subject during questioning.

8.4 Personal effects

The subject must not have access to, or be able to manufacture, any implement that could be used as a weapon.

The subject must not be permitted to retain any listening or recording devices or any communications equipment during any periods of detention or questioning.

The subject must be permitted, upon request, to retain any clothing or personal effects during questioning unless the prescribed authority has reason to believe that the subject may use such items to:

- (a) injure him or herself, or other persons;
- (b) damage property; or
- (c) attempt to escape.

During periods of detention in which the subject is not being questioned, decisions on the retention of items by the subject are the responsibility of a police officer supervising detention. Any effects belonging to a subject which he or she is not allowed to retain in detention must be itemised and placed in safe custody. An inventory of the property retained is to be signed by the subject if the subject is able and willing to do so.

On release from detention all such articles must be returned to the subject who must be asked to sign a receipt for them.

A subject who is not permitted to wear his or her own clothing must be provided with clothing suitable for the climate and adequate to maintain good health and dignity. Such clothing must not be degrading or humiliating in any manner.

8.5 Searches

An ordinary or frisk search of a subject must, if practicable, be conducted by a police officer of the same sex as the subject.

Any strip search of a subject conducted pursuant to section 34ZB of the ASIO Act must comply with the requirements of section 34ZC, including the requirement that the search be conducted by a police officer of the same sex as the subject.

Any search of a subject must be conducted with appropriate sensitivity.

8.6 Use of force and restraint

A police officer may only use the minimum force reasonably necessary in the circumstances, and may only use instruments of restraint as is reasonably necessary in the circumstances.

In particular, the use of force or instruments of restraint must not be applied as a punishment.

Restraint may only be applied by a police officer, and must not be applied or a longer time than is necessary.

Health and welfare

9.1 Facilities and accommodation

Facilities employed for questioning or detention must:

- (a) have adequate fresh air and ventilation, floor space, and heating and cooling appropriate to the climatic conditions;
- (b) have sufficient natural or artificial light to permit reading; and
- (c) need not be the same throughout the period of the warrant.

9.2 Food during detention

This clause applies if a person is detained.

The subject must have access to fresh drinking water at all times.

The subject must be provided with three meals a day at the usual hours or at the times necessary to meet religious requirements.

Food must be of sufficient nutritional value, adequate for health and wellbeing, be culturally appropriate, and well-prepared and served.

A subject must be provided with special dietary food where such food is necessary for medical reasons, on account of a subject's religious beliefs, because the subject is a vegetarian, or if the subject has other special needs.

9.3 Sleep during detention

This clause applies if a person is detained.

The subject is to be provided with a separate bed and, where facilities permit, must be accorded a separate room or cell in which to sleep.

The subject must be provided with sufficient clean bedding which must be kept in good order and changed often enough to ensure its cleanliness.

Unless directed by the prescribed authority, a subject must be accorded the opportunity for a minimum continuous, undisturbed period of 8 hours sleep during any 24 hour period of detention.

9.4 Personal hygiene during detention

This clause applies if a person is detained.

The subject must be provided with access to clean toilet and sanitary facilities for the subject to use as required in a clean and decent manner.

The subject must be provided with such toilet articles as are necessary for health and cleanliness and the maintenance of self-respect.

The subject must be permitted to bathe or shower daily in facilities that are clean, adequate, and at a temperature suitable for the climate.

The subject must be permitted to bathe, use a toilet and dress in private, subject to the requirements of safety and security.

9.5 Health care

The subject must be provided with necessary medical or other health care.

Arrangements must be made for any recommendation made or treatment prescribed by a medical or health professional to be given effect.

9.6 Religion

The subject must be permitted to engage in religious practices as required by his or her religion.

The prescribed authority and persons exercising authority under the warrant may limit such practices in accordance with the requirements of safety and security.

9.7 Subjects under the age of 18 years

If the subject is under the age of 18 years:

- (a) the operation of this Statement of Procedures is limited as provided in section 34ZE of the ASIO Act; and
- (b) any period of questioning or detention may only take place under conditions that take full account of the subject's particular needs and any special requirements having regard to the subject's age.

10 Video recording of procedures

10.1 Facilities for recording

ASIO is responsible for ensuring that there are facilities available for the making of video recordings in accordance with section 34ZA of the ASIO Act.

The facilities must be appropriate to enable a clear visual recording to be made of the subject's appearance before the prescribed authority for the duration of questioning. The facilities must also enable a clear audio recording of all questions, answers and statements made during questioning, including any statements made by the prescribed authority in accordance with section 34J.

If there is a failure in the recording equipment, or if the recording has to be suspended, during the subject's appearance before the prescribed authority for questioning, the prescribed authority must direct that questioning of the subject be deferred until recording resumes.

10.2 Notification to the subject

Upon the commencement or resumption of any recording for the purpose of questioning in accordance with subsection 34ZA(1), the prescribed authority must inform the subject that the questioning is being recorded, and must state the time and date of the questioning.

10.3 Security of recordings

ASIO must ensure that a master version is retained of any video recording of the subject's appearance before a prescribed authority. The master version must be sealed in the presence of the prescribed authority and the label must be signed by the prescribed authority. The sealed master version must be made available to the Inspector-General of Intelligence and Security on request.

ASIO is responsible for ensuring that any copies of video recordings made in accordance with section 34ZA are securely maintained and that a register is kept of any persons or agencies that have access to such copies.

As required under section 34ZL, the Director-General must cause the destruction of a video recording, or copy of a video recording, which is in ASIO's possession or custody or under ASIO's control, if the Director-General is satisfied that the video recording or copy is not required for the purposes of the performance of functions or the exercise of powers under the ASIO Act.

11 Contact

11.1 Contact if subject is not authorised to be detained

If the subject is questioned but is not authorised to be detained, the subject may contact any person unless the prescribed authority limits such contact.

The subject must be provided with access to such facilities as are, in the view of the prescribed authority, appropriate for such contact in all the circumstances.

The prescribed authority may limit contact between the subject and:

- (a) any person by directing questioning to continue despite the subject's request to contact a person; or
- (b) a lawyer, or parent, guardian or other representative, if the prescribed authority directs a person exercising authority under the warrant to remove the lawyer, or parent, guardian or other representative, for disrupting the questioning.

The subject may only contact a person in accordance with section 34ZS of the ASIO Act.

11.2 Contact if subject is detained

A subject who is detained must be permitted to contact:

- (a) a person specified in the warrant as a person with whom the subject may have contact;
- (b) a person falling within a class of persons so specified in the warrant; and
- (c) a person identified in a direction by the prescribed authority in accordance with paragraph 34K(1)(d).

The subject must be provided with access to such facilities as are, in the view of the prescribed authority, appropriate for such contact in all the circumstances.

Contact must be made in a way that can be monitored by persons present for the purposes of executing or supervising the execution of the warrant.

The prescribed authority may limit contact, including by:

- (a) directing questioning to continue despite a subject's request to contact a person; or
- (b) directing a person exercising authority under the warrant to remove the subject's lawyer, or parent, guardian or other representative, for disrupting the questioning.

The subject may only make contact in accordance section 34ZS of the ASIO Act.

12 Complaints

In accordance with subsection 34K(11), a subject must be permitted to contact:

- (a) the Inspector-General of Intelligence and Security concerning ASIO;
- (b) the Commonwealth Ombudsman, the Australian Federal Police (AFP) Commissioner or an AFP appointee concerning the AFP; or

- (c) an appropriate complaints agency during the period of the warrant or following, including when the subject is being questioned or is in detention.

The subject must be provided with such facilities as are, in the view of the prescribed authority, appropriate to make such a complaint.

The subject must be permitted to make such complaint outside of the hearing of persons present for the purposes of executing or supervising the execution of the warrant.

13 Arrangements for liaison

As soon as possible after a warrant is issued under Division 3 of Part III of the ASIO Act, the Director-General must inform the Inspector-General of Intelligence and Security, the prescribed authority, and the Commissioner of the relevant police service(s) of the details of the warrant, and as to the proposed arrangements for its execution.

Annex 5 – IGIS submission to ALRC on legal professional privilege

2007/238
File Ref: 2007/24

Professor David Weisbrot AM
President
Australian Law Reform Commission
GPO Box 3708
SYDNEY NSW 2001

Dear Professor Weisbrot

ALRC Inquiry into Legal Professional Privilege

Thank you for your letter of 24 April 2007 concerning the current inquiry by the Australian Law Reform Commission (ALRC) into the application of legal professional privilege (or client legal privilege) to the coercive information gathering powers of Commonwealth bodies.

You asked for information on how this office approaches the key issues and I am happy to provide a response. By way of context I should note at the outset that:

- (a) The role of this office (which commenced on 1 February 1987) is to review the activities of the six Australian government agencies which are collectively called the Australian Intelligence Community. Importantly, the focus is very much on the activities of the agencies and their staff.
- (b) One element of this review is the conduct of formal inquiries, and certain coercive powers (together with a use immunity) are available in the course of such inquiries.

- (c) The Inspector-General has considerable flexibility about how each formal inquiry is conducted, although they must be conducted in private.
- (d) The purpose of these formal inquiries is to ascertain the truth and make recommendations.
- (e) The Inspector-General does not have any capacity to give directions or make determinations at the conclusion of an inquiry.

Frequency of coercive powers use

Since I was first appointed as Inspector-General on 23 March 2004, I have used the coercive powers in section 18 of the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) in the course of three inquiries.

Section 18 powers have not been used in all inquiries because, in my view, it has not been necessary or appropriate to use them. In most instances inquiries have proceeded by way of examination of records (access to which has been freely provided by the relevant agencies), interviews with relevant staff which have not involved compulsion and the administration of an oath or affirmation, and obtaining statutory declarations from staff addressing questions pertinent to the inquiry.

I understand that the practice of my predecessors was essentially similar.

In the three inquiries where I have issued notices under section 18, this was done either because I formed a belief based on reasonable grounds that certain persons may not have been forthcoming or truthful, or because I took the view that as it was a matter of significant public interest, key witnesses should give their evidence on oath or affirmation.

Some 20 notices under section 18 were involved in these three inquiries. Nineteen of those were notices to appear before me and to answer questions relevant to the matter under inquiry. In one instance the notice required the person to provide me certain information in writing. All of these requests were complied with by the recipients.

It should be noted that in all instances the recipient of the notice was a current or former staff member of one of the six agencies within my jurisdiction.

Client professional privilege

As noted by the ALRC in Issues Paper 33 of April 2007, section 18(6) of the IGIS Act provides that it is not a reasonable excuse for not providing information or documents or answers if it would disclose legal advice given to a minister or an agency or authority of the Commonwealth.

The Issues Paper suggests that this abrogates privilege for those bodies in relation to advice but not in respect of existing or anticipated legal proceedings i.e. the "litigation limb". And clearly the privilege is not abrogated for people or bodies other than those specified in section 18.

The office records and recollections of long serving staff do not reveal any instances of an agency, authority or person attempting to rely on client legal privilege as a reason for not responding to a section 18 notice.

Practice and procedures

I am only aware of one instance where privilege in the context of the section 18 powers in the IGIS Act has potentially been an issue. This related to the notice mentioned above where a person was required to provide information in writing.

Prior to issuing the notice I discussed the matter with the individual concerned. He indicated that the easiest way for him to respond would be to provide me with a copy of a statement he had provided to the legal area of an organisation which was not a Commonwealth organisation.

I advised him that the particular document appeared to attract client legal privilege and I would be happy for him to provide the information in another way. Alternatively he should speak with the relevant legal area as to how he might proceed. In

the event the document was subsequently provided to me.

As client legal privilege issues arise only very rarely in relation to section 18 of the IGIS Act, this office has not set down any policies or procedures in a manual or otherwise.

For completeness I should also comment that if necessary, the privilege could be maintained against third parties because the Inspector-General and the staff of the office cannot be compelled to disclose information (see in particular section 34 of the IGIS Act). This has not arisen as a practical issue in the experience of this office.

Use and derivative use immunity

Section 18(6) of the IGIS Act provides for use immunity and I can say confidently that this has not been an inhibition to effective investigation in my experience.

Arguably, use immunity provides additional incentive for a person to cooperate insofar as they do not have to engage in an exercise of weighing the potential penalty for non-compliance with the potential penalties that might attach to prosecution of them for conduct which is under consideration.

In any case, in my view it is intuitively fair that use immunity be available if the normal right concerning self-incrimination is not available.

Derivative use immunity is not provided for in the IGIS Act and I see no reason to contemplate its introduction into the Act.

General Comments

There are cogent reasons for generally maintaining client legal privilege. While some of the rationales for privilege given in the first chapter of Issues Paper 33 are debatable, it is difficult to put aside the rationales of full and frank disclosure, encouraging compliance and protecting the fairness of the adversarial system.

Nonetheless, I would suggest some important exceptions or qualifications need to be made.

One concerns Royal Commissions of the inquisitorial/investigatory type. Such Royal Commissions will have been established because there is a matter of substantial public

interest/concern. A great deal of public monies is usually expended. Ascertaining the truth is the fundamental purpose of having the Royal Commission. Such Royal Commissions are relatively unusual and abrogation of privilege would not impact to any significant degree on the instrumental rationales for client legal privilege – it would be most surprising if the possibility of a Royal Commission was on people’s “mental horizon” when conducting their affairs and obtaining legal advice. In any case, the public interest in Royal Commissions ascertaining the truth should be paramount.

I should mention that on occasion there have been policy advisory Royal Commissions (as compared to inquisitorial/investigatory Royal Commissions). This distinction is drawn in Scott Prasser’s *Royal Commissions and public inquiries in Australia* (LexisNexis, Chatswood NSW 2006). It must be acknowledged that policy advisory Royal Commissions should not, in practice, need to access material of the sort which might raise issues of client legal privilege.

A second area where the appropriateness of client legal privilege needs to be considered is where review of the activities of government bodies is being carried out.

Adequate accountability of government entities is vital for several reasons. These are neatly encapsulated in a quotation from the publication *Accountability in the Commonwealth Public Sector* by the Management Advisory Board and its Management Improvement Advisory Committee, No 11, June 1993:

“Accountability is fundamental to good governance in modern, open societies. Australian officials rightly see a high level of accountability of public officials as one of the essential guarantees and underpinnings, not just of the kinds of civic freedoms they enjoy, but of efficient, impartial and ethical public administration. Indeed, public acceptance of government and the roles of officials depends upon trust and confidence founded upon the administration being held accountable for its actions.”

Given the importance of ensuring the proper accountability of public bodies, a strong argument can be made out to limit or remove the possibility of entities claiming client legal privilege when being

lawfully reviewed by other parts of the executive arm of government.

Even if this general argument is thought to go too far, I would argue that there is an additional consideration in respect of the intelligence and security agencies. Such agencies operate largely in secrecy. Other processes which might restrain the conduct of public entities, such as the capacity of citizens to be fully aware of what is being done in respect of them, or for representatives of the entity to be questioned about operational details in public sessions of parliamentary committees, are not applicable to the intelligence and security agencies.

In these circumstances the special review mechanism of the Inspector-General of Intelligence and Security has been developed. Consistent with the need for the Inspector-General to be something of a substitute for other accountability mechanisms and hence very incisive, there should be no restrictions on what the Inspector-General can view within the agencies.

Moreover, formal inquiries under the IGIS Act are, in significant respects, similar to a Royal Commission. Coercive powers (with a use immunity) are available, the objective is to ascertain the truth, and the IGIS does not have any determinative or decision making powers at the conclusion of an inquiry.

For these reasons I believe the abrogation of legal professional privilege in the IGIS Act in respect of the intelligence and security agencies is entirely appropriate.

However, given that the IGIS is an ongoing body and its focus is very much intended to be upon those six agencies, the abrogation rightly does not go beyond the agencies and relevant ministers.

At the same time I must say that limiting the abrogation in respect of the agencies to legal advice is, in my view, a potential deficiency. Privilege in respect of the litigation arm should also be clearly abrogated.

There could well be occasions when the Inspector-General should, to properly achieve the stated objectives of the IGIS Act, examine the compliance of agencies with the *Legal Services Directions* issued by the Attorney-General pursuant to section 55ZF of the *Judiciary Act 1903*. There has been significant growth in the number of litigation actions to which ASIO is a party or otherwise involved (see page

four of the unclassified ASIO report to Parliament 2005–2006).

Of course, abrogation in respect of litigation should not extend to any situation where both an agency and the Inspector-General are parties to a particular action (not that this seems remotely likely).

I hope this information and comment is useful. Please don't hesitate to contact me if further information or clarification would be helpful.

Yours sincerely

Ian Carnell
Inspector-General of
Intelligence and Security

1 June 2007

Annex 6 – Report on the statutory independence of the Office of National Assessments – Executive Summary

- In the 2004 *Report of the Inquiry into Australian Intelligence Agencies*, Mr Philip Flood AO recommended that the IGIS should have a general own motion capacity in respect of ONA and should conduct periodic reviews of ONA's statutory independence. Subsequent legislative amendments to the *Inspector-General of Intelligence and Security Act 1986*, effective from 2 December 2005, tasked the IGIS in accordance with these recommendations.
- To establish a basis for a review in 2006, a set of principles were developed by my office setting out what independence and propriety in respect of ONA's assessments are – and are not (see Annex A).
- This review essentially covered ONA's assessments in the period December 2005 until October 2006. It involved examination of ONA's formal assessment products, interviews with key ONA clients, a survey of ONA analysts and confidential interviews with selected analysts.
- The general view of ONA analysts was that ONA judgements are not shaped to suit the political concerns of government ministers and no suggestions were put to the review of improper pressure and/or attempted direction from ministers and their offices.
- Analysts surveyed or interviewed were fully conscious that their assessments must be policy relevant but not policy driven. Analysts believed ONA assessments are not biased towards desired policy outcomes.
- Policy departments and ministers' offices did not consider that ONA produced assessments that are driven by the policy objectives of the government or assessments that are tailored to suit ministers' agenda. Examples were given which do indeed support this.
- Analysts felt ONA judgements are not shaped to align with the judgements of Australian intelligence agencies or of the allied intelligence community, and no suggestions were made to the review of improper pressure or attempted direction from such agencies.
- A number of analysts (but not a majority) believe or were ambivalent about whether there may be some subjects with policy/political sensitivity on which ONA might self-censor (ie. touch on in a limited manner only). Examination of ONA products in the small number of areas nominated did not support this in some instances, but was inconclusive in others.
- Several processes that are important in ensuring independence and propriety in the assessment work undertaken at ONA – including general circulation of drafts among analysts for comment, feedback exchanges, openness to debate – were rated well by ONA analysts.
- Analysts identified processes such as deliberately identifying and challenging underlying assumptions, and reviewing past judgements, as not having always been pursued systematically in the past, but believed these were improving. The Director-General recently instituted a formal review process in relation to reviewing past judgements.

- I noted during the review that new procedures for documenting source information have also been implemented. This is commendable and something which I will examine in future reviews, along with how any limitations of the available information and intelligence used to form the basis of an assessment is addressed.
- Dissent on assessments within ONA is not discouraged, although it was not clear how in particular instances the divergent viewpoints were evaluated and a final position reached. This will be an additional focus in future review activity.
- Although the ONA Act specifically provides for dissent to be recorded by members on the National Assessments Board, there were no instances of this in the review period. While not necessarily indicative of a problem – indeed no one whom I interviewed suggested this to be the case – this needs to be monitored.

15 December 2006

Index

A

- Access and equity, 78
- Administrative Appeals Tribunal (AAT)
 - appeals against ASIO assessments, 8
 - persons who may appeal to, 12
 - refugee applicants, 12
 - Security Appeals Division, 49
- Administrative Review Council, 10, 31
- Advertising, 79
- Agency seminars, presentations at, 6, 22
- Ahmed, Mr Ruhel, 7, 24–5, 49, 106
- AML/CTF Amendment Act 2007*, 28, 46–7
- Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, 28
- Arar, Mr Maher, 23
- Archives, 47
- Archives Act 1983*, 47
- Asia-Pacific Economic Cooperation (APEC)
 - Leaders Forum, 13
- Assumed identities, use of
 - ASIO, 47, 72
 - ASIS, 57
- Assurance, level of, 36–7
- Attorney-General, 13, 31
- Audit Committee, 75
- AusTender, 77
- Australian Commission for Law Enforcement Integrity (ACLEI), 21
- Australian Defence Force (ADF), 13, 59
- Australian Government Solicitor (AGS), 78
- Australian Intelligence Community (AIC) agencies,
 - 6, 8
 - complaints about, 19
 - growth of, 9, 13
 - leadership changes, 17
 - powers and capabilities, 10
 - responsiveness to issues raised, 36
 - review of activities of, 8
- Australian National Audit Office (ANAO), 8, 12, 21, 79
- Australian Public Service Commissioner, 31
- Australian Secret Intelligence Service (ASIS), 52–8
 - AIC, part of, 8
 - carriage of weapons for self-defence, 6, 10, 55
 - establishment, 52
 - ethical issues, 53
 - functions, 52
 - grievance process issues, 58
 - growth and expansion, 52–3
 - inspection activities, 54–7
 - ministerial authorisations, review of, 54
 - ministerial submissions, 55
 - operational file review activities, 55–6
 - periodic roundtable meetings, 57
 - privacy rules, 56–7
 - recruitment related complaints, 57–8
 - significant issues, 52–4
 - special briefings, 53
 - staff, visits and contact with, 53
 - training, 54
 - year in prospect, 73

Australian Security Intelligence Organisation (ASIO), 38–51

- AIC, part of, 8
- approvals to investigate, 45, 72
- Attorney-General’s Guidelines, 39, 45–6
- career information, 50
- compensation, 50
- complaints and inquiries, 48–51
- exchange of information with foreign liaisons, 41
- growth and expansion, 13, 38
- inspection activities, 40–7
- law enforcement agencies and, 46
- monthly meetings, 41–2
- new headquarters, 39
- new powers, 71–2
- operational activities, review of, 41
- questioning and detention warrants, 6, 10, 30–1, 39, 109–18
- role, 38
- significant issues, 38
- special briefings, 39–40
- training, 40
- warrant inspections, 42–3
- warrant operations, 42
- warrant reviews, 44–5, 72
- year in prospect, 71–3

Australian Security Intelligence Organisation Act 1979, 10, 38

Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003, 30, 39

Australian Transaction Reports and Analysis Centre (AUSTRAC), 28

- ASIO, information obtained by, 46

- ASIS, access by, 54

Awards, 18

B

‘Balibo Five’, 25

Blick, Mr Bill, 15

Bryan, Mr Neville, 18

Business continuity plan, 76

C

Canada, conference in, 23

Canadian Security Intelligence Review Committee, 24

Client legal privilege

- see Legal professional privilege

Cole ‘Oil-for-Food’ Commission, 26

Commissioner of Taxation, 47

Commonwealth Ombudsman, 12, 14, 16, 21, 31, 35

Community outreach, 22

Complaints

- advice on outcomes of, 31

- AIC agencies, about, 19–20

- ASIO, about, 48–51

- ASIS, about, 57–8

- DIGO, about, 66

- DIO, about, 68

- DSD, about, 62–3

- inquiries triggered by, 6

- levels of, 34–6

- ONA, about, 70

- receipt of, 19–20

- statistics, 103

- year in prospect, 74

Consultancies, 77, 105

Contract services, 77, 78

Corporate governance, 75

Cousins, Mr Ian, 18

Crimes Legislation Amendment (National Investigative Powers and Witness Protection) Bill 2006, 29

D

Defence Imagery and Geospatial Organisation (DIGO), 64–6

- AIC, part of, 8

- complaints and inquiries, 66

- establishment, 64

- functions, 64

- growth and expansion, 64

- inspection activities, 65–6

- meetings with senior staff, 66

- ministerial authorisations, 65

- new director, 17, 64
 - privacy rules, 65
 - significant issues, 64–5
 - training, 66
 - year in prospect, 73–4
 - Defence Intelligence Organisation (DIO), 67–8
 - AIC, part of, 8
 - analytical integrity, 68
 - complaints and inquiries, 68
 - functions, 67
 - privacy guidelines, 67
 - training, 68
 - year in prospect, 74
 - Defence Signals Directorate (DSD), 59–63
 - AIC, part of, 8
 - complaints and inquiries, 62–3
 - functions, 59
 - inspection activities, 60–2
 - military operations, support to, 59
 - ministerial authorisations, 60–1
 - monthly meetings, 61
 - new director, 17, 59
 - privacy rules, 62
 - significant issues, 59
 - site visits, 62
 - spot checking of databases, 61
 - support from, 75
 - training, 62
 - year in prospect, 73
 - Department of Defence
 - Deputy Secretary Intelligence and Security, 17
 - Secretary of, 17
 - Department of Immigration and Citizenship (DIAC), 48
 - Department of the Prime Minister and Cabinet (PMC), 12, 14
 - support from, 75
 - Disability Discrimination Act 1992*, 77
 - Disability strategy, 77
 - Disaster recovery plan, 76
- E**
- East Timor, 25, 60
 - Employees
 - complaints by, 12
 - Energy saving measures, 78
 - External scrutiny, 79
- F**
- Financial performance, 80
 - Flood review, 2004, 6, 10, 12, 13, 24
 - Foreign visits, 23
 - Fraud control, 76
 - Freedom of information, 79
- G**
- Governor-General, 16
- H**
- Holdich, Mr Roger, 15
 - Honours, 18
 - Human resources, 77
 - Human rights, 11
 - Human Rights Commissioner, 12
 - Human Services (Enhanced Service Delivery) Bill 2007, 29
- I**
- IGIS model, 11
 - Immigration
 - complaints, 35, 48
 - security assessment complaints, 6, 49
 - Inquiry activities, 8, 18
 - advice on outcomes of, 31
 - ASIO, about, 48–51
 - ASIS, about, 57–8
 - DIGO, about, 66
 - DIO, about, 68
 - DSD, about, 62–3
 - levels of, 34–6
 - ONA, about, 70
 - statistics, 103
 - year in prospect, 74

Inspection activities, 18

ASIO, 40–7

ASIS, 54–7

DSD, 60–2

program, 9, 20–1

role, 8

year in prospect, 71–4

Inspector-General of Intelligence and Security

acting, 16

activities, 18–21

continuation of final term, 71

corporate activities, 18

functions, 8

growth of, 14

independence, 11, 14

independent statutory office, 8

inquiries activities, 8, 18

inspection role, 8, 18, 20–1

jurisdiction, scope of, 11

liaison, 12, 21–2

new premises, 14, 75

previous office-holders, 14–15

re-appointment as, 16

role of, 8

20th anniversary, 6, 14

Inspector-General of Intelligence and Security Act 1986

(IGIS Act), 6, 8, 28

Division 3, 19

section 6, 16

section 6A(1), 16

section 8, 8, 18

section 8(3)(c), 24, 69

section 8(8)(a), 50

section 8(8)(c), 49

section 9, 8

section 9A, 8, 18, 24

section 11, 19

section 14, 19

section 16, 21

section 22, 28

section 25A, 28

section 26, 16, 71

section 35(2), 24, 69

Integrity Commissioner, 21

Intelligence assessments, 10

International cooperation, 23

International Intelligence Review Agencies (IIRA)
conference, 23

Internet presence, 78

J

Jurisdiction, 11

K

Key intelligence and security interests, 13

L

Law Enforcement Integrity Commissioner Act 2006, 21

Legal professional privilege

ALRC review of, 32, 119–22

Legal services, 78

Legislation, 10

Legislative developments, 28–31

M

McInnis, Mr Neil, 15

McLeod, Mr Ron, 15

McMillan, Professor John, 16

acting IGIS, 16

acting Integrity Commissioner, 21

Market research, 79

Media, 79

Moss, Mr Philip, 16, 22

N

National Security Committee, 12, 59

National Security Hotline (NSH), 34, 78

Nexis Accountants, 78

O

Occupational health and safety, 77

Office Inspector-General of Intelligence and Security
see Inspector-General of Intelligence and
Security

Office of National Assessments (ONA)

AIC, part of, 8

complaints and inquiries, 70

- functions, 69
- independence and propriety of, 10
- inspection work, 6
- privacy guidelines, 70
- statutory independence, review of, 24, 69–70, 123–4
- training, 70
- year in prospect, 74

Office of National Assessments Act 1977, 69

‘Oil-for-Food’ Commission, 26

Outcomes, 34

- resources for, 80

Outputs, 34

P

Parliamentary Joint Committee on Intelligence and Security (PJCIS), 8, 10, 12, 27

- liaison with, 12

Parliamentary oversight, 27

Performance, 33

Performance indicators, 34

Performance pay, 76

Peters, Mr Brian, 25–6, 60

Powers, new, 6, 71–2

Prime Minister, 8, 11, 16, 17

Privacy

- ASIS rules, 56
- DIGO rules, 65
- DIO guidelines, 67
- DSD rules, 62
- ONA guidelines, 70

Privacy Act 1988, 29

- ALRC Review of, 31

Privacy Commissioner, 12, 31

Privacy Legislation Amendment (Emergencies and Disasters) Act 2006, 29

Propriety, 11

Public Service Medals, 18

Purchasing, 77

Q

Questioning and detention warrants, 6, 10, 30–1, 39, 109–18

R

Recommendations, acceptance of, 36

Refugees

- AAT, appealing to, 11

Resource allocation, 33–4

Royal Commission on Australia’s Security and Intelligence Agencies, 20

Rule of law, 9

Safety, Rehabilitation and Compensation Act 1988, 51

S

Security, definition, 38

Security assessments

- Commonwealth employment, for, 48–9
- complaints about, 6, 19, 48–9
- migration related, 49
- Mr Rhuhel Ahmed, 7, 24–5, 49, 106

Security Legislation Review Committee (SLRC), 10, 31

Senate Finance and Public Administration Committee, 27

Sheller Committee, 10

Shergold, Dr Peter, 18

Social justice, 78

South Africa, conference, 23

Staff, 71, 76

- increase in, 9
- recruitment, 71

Strang, Mr Hadyn, 17

T

Taloni, Dr Paul, 18

Taxation

- access to information, 47

Taxation Administration Act 1953, 47

Taylor, Mr Allan, AM, 13

- valediction, 17

Telecommunications interception

- B-Party warrants, 6, 30, 43
- interception management systems, 44
- unauthorised, 43–4

Telecommunications (Interception and Access) Act 1979, 30, 43

Telecommunications (Interception and Access)

Amendment Bill 2007, 29

Terrorism, 13

counter-terrorism, 11, 60

offence provisions, 10

"The Road to Guantanamo", 7

Timeliness, 36

"Tipton Three", 7

Training, 22

ASIO, for, 40

ASIS, for, 54

DIGO, for, 66

DIO, for, 68

DSD, for, 62

ONA, for, 70

U

Uhrig templates, 11

United Nations 'Oil-for-Food' Program, 26

V

Valedictions, 17

W

Workplace agreements, 76

Workplace diversity, 76

Workplace Relations Act 1996, 76

Y

Year in prospect, 71–4

Year in review, 13

