







© Commonwealth of Australia 2005

ISBN 0-9756755-1-6

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without permission from AusInfo. Requests and inquiries concerning reproduction and rights should be addressed to the Manager, Legislative Services, AusInfo, GPO Box 1920, Canberra ACT 2601.

Design and typesetting by ZOO, ACT.  
Printed by New Millennium, ACT.



## INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

2005/375

File Ref: 2005/41

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 2004 and 30 June 2005.

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 2005.

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

A handwritten signature in black ink that reads "Ian Carnell".

Ian Carnell  
Inspector-General of  
Intelligence and Security

17 October 2005



# Table of contents

<b>LETTER OF TRANSMITTAL</b>	<b>iii</b>	<b>Level of Assurance</b>	<b>11</b>
<b>KEY POINTS</b>	<b>iv</b>	Number of complaints	11
		Summary	11
<b>GLOSSARY OF ACRONYMS USED IN THIS REPORT</b>	<b>viii</b>	<b>AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION</b>	<b>12</b>
<b>ROLE OF THE INSPECTOR-GENERAL</b>	<b>1</b>	<b>What ASIO Does</b>	<b>12</b>
<b>THE YEAR IN REVIEW</b>	<b>2</b>	<b>Senior Appointments</b>	<b>12</b>
<b>Overview</b>	<b>2</b>	<b>Significant Issues</b>	<b>13</b>
<b>AIC Related Reviews</b>	<b>2</b>	Questioning and detention warrants	13
Flood Inquiry	2	Search warrants	14
PJCAAD—Review of ASIO questioning and detention warrants	4	Immigration related issues	15
PJCAAD—Review of the Intelligence Services Legislation Amendment Bill 2005	5	Training	15
Blunn Review of the Telecommunications (Interception) Act 1979	5	<b>Inspection Activities</b>	<b>16</b>
<b>Legislation</b>	<b>5</b>	Scope and reporting arrangements	16
Intelligence Services Act 2001	5	Warrant operations—procedures	16
Inspector-General of Intelligence and Security Act 1986	6	Outcome of warrant inspections	17
<b>Training</b>	<b>6</b>	Unauthorised telephone interception	18
<b>Inspections, Complaints and Inquiries</b>	<b>6</b>	Interception management systems	18
Inspections	6	Warrant related processing issues	18
Complaints	6	Timeliness of reporting on warrant outcomes	19
Immigration related complaints	7	Authorities to investigate—procedures	20
Search warrants	7	Authorities to investigate— inspection results	20
Recruitment/employment concerns	8	ASIO and law enforcement agencies	20
Defence Force complainant	8	AUSTRAC and the Australian Taxation Office	21
<b>PERFORMANCE</b>	<b>9</b>	Use of assumed identities	21
<b>Resource allocation</b>	<b>9</b>	Archives	21
<b>Performance Indicators</b>	<b>9</b>	Contact with staff	22
<b>Timeliness</b>	<b>9</b>	<b>Complaints and Inquiries</b>	<b>22</b>
<b>Acceptance of Recommendations</b>	<b>10</b>	Possible forewarning of Bali bombing	22
<b>Responsiveness to Issues Raised</b>	<b>10</b>	Possible AIC complicity in the arrest and detention of an Australian citizen	23
		Inappropriate interference in personal affairs	23
		Generalist Intelligence Officer training	23

<b>AUSTRALIAN SECRET INTELLIGENCE SERVICE</b>	<b>24</b>	<b>DEFENCE INTELLIGENCE ORGANISATION</b>	<b>37</b>
<b>What ASIS Does</b>	<b>24</b>	<b>What DIO Does</b>	<b>37</b>
<b>Significant Issues</b>	<b>24</b>	<b>Senior Appointment</b>	<b>37</b>
Founding Director-General	24	<b>Flood Review</b>	<b>37</b>
Queen's birthday honours	24	<b>Accountability Arrangements</b>	<b>38</b>
Weapons and/or self-defence	24	<b>Complaints and Inquiries</b>	<b>38</b>
ISA immunity provisions	25		
ISLA Bill 2005	25	<b>OFFICE OF NATIONAL ASSESSMENTS</b>	<b>41</b>
<b>Inspection Activities</b>	<b>25</b>	<b>What ONA Does</b>	<b>41</b>
Privacy rules	26	<b>Significant Issues</b>	<b>41</b>
Ministerial authorisations	26	Flood Review	41
Review of operations	27	Flood implementation	42
Use of assumed identities	27	ISLA Bill 2005	42
Contact with staff	27	<b>Review Activities</b>	<b>42</b>
Training	27	<b>Training</b>	<b>43</b>
<b>Complaints and Inquiries</b>	<b>27</b>	<b>Complaints and Inquiries</b>	<b>43</b>
Own motion inquiry	28		
Recruitment related complaint	28	<b>THE YEAR 2005–06 IN PROSPECT</b>	<b>44</b>
		<b>Inspection Activity</b>	<b>44</b>
<b>DEFENCE SIGNALS DIRECTORATE</b>	<b>29</b>	ASIO	44
<b>What DSD Does</b>	<b>29</b>	ASIS	44
<b>Significant Issues</b>	<b>29</b>	DSD	45
Flood review	29	DIGO	45
ISLA Bill 2005	29	ONA	45
<b>Inspection Activities</b>	<b>30</b>	DIO	45
Ministerial authorisations	30	<b>Inquiries and Complaints</b>	<b>45</b>
Privacy rules	30	<b>Legislative Review</b>	<b>45</b>
Monthly meetings	31		
Comsec monitoring	31	<b>CORPORATE AND COMMUNICATION</b>	<b>46</b>
New collection activities	31	<b>Support from DPMC and DSD</b>	<b>46</b>
Site visits	31	<b>Outcome and Outputs</b>	<b>46</b>
<b>Training</b>	<b>32</b>	<b>Corporate Governance</b>	<b>46</b>
<b>Complaints and Inquiries</b>	<b>32</b>	<b>Disaster Recovery Plan/Business</b>	
Interference with personal		<b>Continuity Plan</b>	<b>46</b>
communications	32	<b>Fraud Control</b>	<b>47</b>
Security checking	32	<b>Staffing and Resources</b>	<b>47</b>
		<b>Composition of the Office</b>	<b>47</b>
<b>DEFENCE IMAGERY AND GEOSPATIAL</b>		<b>Performance Pay</b>	<b>47</b>
<b>ORGANISATION</b>	<b>34</b>	<b>Workplace Agreements</b>	<b>47</b>
<b>What DIGO Does</b>	<b>34</b>	<b>Workplace Diversity</b>	<b>47</b>
<b>Brief History</b>	<b>34</b>	<b>Disability Strategy</b>	<b>47</b>
<b>Accountability Arrangements</b>	<b>34</b>	<b>Occupational Health and Safety</b>	<b>47</b>
<b>Flood Review</b>	<b>34</b>	<b>Management of Human Resources</b>	<b>48</b>
<b>ISLA Bill 2005</b>	<b>35</b>	<b>Purchasing</b>	<b>48</b>
<b>Inspection Activities</b>	<b>35</b>	<b>Consultancy Services</b>	<b>48</b>
<b>Training</b>	<b>36</b>		
<b>Complaints and Inquiries</b>	<b>36</b>		

<b>Contract Services</b>	<b>48</b>	<b>ANNEX 1—COMPLAINT AND INQUIRY STATISTICS</b>	<b>72</b>
<b>Competitive Tendering and Contracting</b>	<b>48</b>		
<b>Energy Saving Measures</b>	<b>48</b>	<b>ANNEX 2—SUBMISSION TO THE PJCAAD REVIEW OF ASIO QUESTIONING AND DETENTION WARRANTS</b>	<b>76</b>
<b>Social Justice: Access and Equity</b>	<b>48</b>		
<b>Internet Presence</b>	<b>49</b>		
<b>Media</b>	<b>49</b>		
<b>International Liaison</b>	<b>49</b>	<b>ANNEX 3—IGIS LETTER TO MINISTER FOR DEFENCE—LT COL LANCE COLLINS</b>	<b>83</b>
<b>Advertising and Market Research</b>	<b>49</b>		
<b>Freedom of Information</b>	<b>49</b>	<b>ANNEX 4—ABRIDGED IGIS REPORT—LT COL LANCE COLLINS</b>	<b>86</b>
<b>External Scrutiny</b>	<b>49</b>		
<b>Summary of the Office’s Financial Performance</b>	<b>49</b>		
<b>FINANCIAL STATEMENTS</b>	<b>50</b>		
<b>IGIS CONTACT INFORMATION</b>	<b>71</b>		
Location	71		
Written inquiries	71		
Parliamentary and media liaison	71		
General inquiries	71		
Internet address	71		

# Glossary of acronyms used in this report

AIC	Australian Intelligence Community
AIO	Australian Imagery Organisation
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
ATI	Authority to Investigate
AUSTRAC	Australian Transaction Reports and Analysis Centre
DIGO	Defence Imagery and Geospatial Organisation
DIO	Defence Intelligence Organisation
DPMC	Department of the Prime Minister and Cabinet
DSD	Defence Signals Directorate
GIO	Generalist Intelligence Officer
IDC	Inter-Departmental Committee
IGIS	Inspector-General of Intelligence and Security
ISA	<i>Intelligence Services Act 2001</i>
ISLA	<i>Intelligence Services Legislation Amendment Bill 2005</i>
MOU	Memorandum of Understanding
IGIS	Office of the Inspector-General of Intelligence and Security
ONA	Office of National Assessments
PJCAAD	Parliamentary Joint Committee on ASIO, ASIS and DSD
TI Act	<i>Telecommunications (Interception) Act 1979</i>

# Role of the Inspector-General

The Inspector-General of Intelligence and Security (IGIS) is an independent statutory office which helps the Prime Minister, the Attorney-General, the Minister for Foreign Affairs and the Minister for Defence, oversight and review the activities of the following six intelligence and security agencies:

- ▶ 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).

These six agencies collectively form what is known as the Australian Intelligence Community (AIC).

Other government agencies, such as the Australian Federal Police and the Australian Customs Service also play very important roles in safeguarding Australia's national interests, but as they are not members of the AIC, their activities fall outside of the legislative jurisdiction of the IGIS.

The purpose of the oversight and review activities undertaken by the IGIS is to ensure that each AIC agency acts legally and with propriety, complies with ministerial guidelines and directives and respects human rights.

The office was established by the *Inspector-General of Intelligence and Security Act 1986* and commenced from 1 February 1987.

The Inspector-General can undertake an inquiry into the activities of an agency in response to a complaint or a request from a minister. The Inspector-General can also act independently to initiate inquiries and conducts regular inspections and monitoring of agency activities.

In conducting an inquiry, the Inspector-General has significant powers which include requiring the attendance of witnesses, taking sworn evidence, copying and retention of documents and entry into an agency's premises. The Inspector-General can also conduct preliminary inquiries into matters in order to decide whether to initiate a full inquiry.

Further information about the role and functions of the Inspector-General can be found elsewhere in this report and at <http://www.igis.gov.au>.



of the *Inquiry into Australian Intelligence Agencies* is accessible on the Internet at [http://www.dpmc.gov.au/publications/intelligence\\_inquiry](http://www.dpmc.gov.au/publications/intelligence_inquiry).

Mr Flood made 23 recommendations, all of which were accepted by the government with the exception of a proposal for ONA to be renamed as the Australian Foreign Intelligence Assessments Agency.

Among the more significant of the recommendations made by Mr Flood were:

- ▶ The remit of the PJCAAD should be extended to cover all of Australia's intelligence agencies (ie. it should also cover ONA, DIO and DIGO on the same basis as it presently covers ASIO, ASIS and DSD).
- ▶ The functions and ministerial accountabilities of DIGO should be formalised in legislation by amendments to the *Intelligence Services Act 2001* (ISA).
- ▶ The budget of ONA should be effectively doubled from \$13.1 million to \$25 million by 30 June 2007, to enable a significant expansion in its analytical capacity.
- ▶ A Foreign Intelligence Coordination Committee should be established under the chairmanship of the Director-General ONA, to assist in coordinating, monitoring and reporting on the performance of Australia's foreign intelligence community, and to provide guidance to more senior level committees on cross-AIC issues.
- ▶ The Department of the Prime Minister and Cabinet (DPMC) should play an enhanced coordination and monitoring role in respect of ASIO and Australia's foreign intelligence community.

As one of Mr Flood's key terms of reference was to inquire into and report on "*the effectiveness of the intelligence community's current oversight and accountability mechanisms*", I naturally met with Mr Flood several times to offer my perspectives. My staff and I liaised frequently with the secretariat which supported Mr Flood during his review.

Mr Flood offered the following thoughts in his final report on extant accountability arrangements in the AIC and on the role of my office:

*"Our liberal, democratic society demands that all elements of government are accountable. Australians are entitled to be confident that government institutions are operating according to law, under the authority of ministers, and that they offer value for money, efficiency and effectiveness.*

*Intelligence agencies are no exception. Indeed, these obligations are, if anything, higher in relation to intelligence agencies than other branches of government. With the capacity to infringe on citizen's privacy and to undertake acts that without specific legislation might be unlawful, Australians are entitled to expect that intelligence collection agencies are properly scrutinised and held to account."*<sup>1</sup>

*"Overall, the accountability arrangements in the Australian intelligence community are working effectively. The National Security Committee of Cabinet is vigorous and engaged. The Intelligence Services Act has worked well in practice. The Parliamentary Joint Committee (by reviewing administration and expenditure) and the Inspector-General of Intelligence and Security (by reviewing operations and activities) provides complementary forms of scrutiny."*<sup>2</sup>

*"The Inquiry found that the Inspector-General of Intelligence and Security performs an important function in the system of accountability of the agencies. Most valuable among the roles of the Inspector-General is the power to investigate deeply into the conduct of the agencies. The penetrating character of those powers is a strong feature of Australia's accountability systems."*<sup>3</sup>

Notwithstanding this positive assessment about the suite of accountability mechanisms which oversight and guide the activities of the AIC, Mr Flood also identified several apparent gaps or deficiencies. Some of these gaps related to the mandate of this office. In order to plug those perceived accountability gaps, Mr Flood made

1 P Flood, *Report of the Inquiry into Australian Intelligence Agencies*, Canberra, July 2004 p. 51 (cited hereafter as 'Flood').

2 Flood, p. 57.

3 Flood, p. 59.

several recommendations in respect of the role and functions of the IGIS, as follows:

*“Recommendation 2—... the Inspector-General of Intelligence and Security Act 1986 should be amended to include scrutiny of DIGO on a basis comparable with that which applies to DSD and ASIS.*

*Recommendation 3—The mandate of the Inspector-General of Intelligence and Security should be extended to allow IGIS to initiate inquiries at his or her own discretion into matters relating to ONA and DIO without ministerial referral, consistent with the IGIS jurisdiction in respect of ASIO, ASIS and DSD. The Inspector-General should also conduct a periodic review of ONA’s statutory independence.”<sup>4</sup>*

The various government endorsed recommendations made by Mr Flood required significant planning and coordination to put into effect. To this end DPMC created an Inter-Departmental Committee (IDC) and several subsidiary working groups to facilitate the implementation of the agreed recommendations.

This office was an active and engaged member of the IDC and the IDC’s Accountability Working Group while these bodies were active (ie. throughout the first half of the reporting period). Details of proposed legislative changes flowing from Mr Flood’s recommendations are detailed in the section of this chapter which deals with ‘Legislation’.

### **PJCAAD—Review of ASIO questioning and detention warrants**

The Commonwealth Parliament passed the *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003* on 26 June 2003, and it received assent on 22 July 2003.

The effect of this Act was to insert a new Division into Part III of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act), permitting the Director-General of Security, with the Attorney-General’s consent, to seek a warrant authorising the questioning or detention of a person where doing so would substantially assist the collection of intelligence in relation to a terrorism offence.

Recognising that the extension of these extraordinary new powers to ASIO was likely to remain a subject of public concern and ongoing debate, parliament inserted a three year sunset clause on the operation of these new provisions (via s.34Y of the ASIO Act), meaning these provisions will cease to have effect on 23 July 2006 unless renewed.

The execution of the first questioning warrants granted under section 34D of the ASIO Act occurred in the later part of 2003. Practical experience derived from seeking and then executing these warrants, led the government to propose a number of modifications to the new provisions.

The modifications proposed by the government were contained in the *ASIO Legislation Amendment Act 2003*, which was assented to on 17 December 2003. This Act also effected several consequential amendments to the ISA, including amending the functions of the PJCAAD to require it to review, by 22 January 2006, the operation, effectiveness and implications of the new Division 3 of Part III of the ASIO Act, and to report the Committee’s comments and recommendations to each House of the Parliament and to the responsible Minister.<sup>5</sup>

I lodged a written submission with the PJCAAD on 30 March 2005. The submission provided an overview of the role of the IGIS in respect of these new powers, various observations on how Division 3 of Part III of the ASIO Act has operated in practice, and a series of proposals for further possible legislative refinements. A copy of the submission can be found at Annex 2 to this annual report.

The Committee conducted a series of public hearings in Canberra, Sydney and Melbourne, in May–June 2005. I appeared before the Committee in Canberra, on 20 May 2005. In my submission and in my oral evidence to the Committee, I supported the continuation of these powers in the short and perhaps medium term, but also the maintenance of a sunset clause.

The PJCAAD’s review of ASIO’s questioning and detention powers was still in train at the conclusion of the reporting period.

<sup>4</sup> Flood, p. 180.

<sup>5</sup> Section 29(1)(bb)(i)(ii) and (c) of the *Intelligence Services Act 2001* refers.

### **PJCAAD—Review of ISLA Bill 2005**

The *Intelligence Services Legislation Amendment Bill 2005* (ISLA Bill) was introduced into parliament on 16 June 2005. The Senate resolved the same day to refer the Bill to the PJCAAD for comment and to provide a report to the Minister for Defence (the sponsor of the Bill).

I and other affected AIC agency heads met with the PJCAAD, also on 16 June 2005, to provide a brief overview of the ISLA Bill and explain its likely impact on each of our agencies. A fuller explanation of the background to the ISLA Bill is provided under the 'Legislation' section of this chapter.

The PJCAAD review of the ISLA Bill 2005 was on-going at the conclusion of the reporting period.

### **Blunn Review of the TI Act 1979**

On 18 March 2005, the Attorney-General, the Hon. Philip Ruddock MP, announced that he had asked a former Secretary of the Attorney-General's Department, Mr AS Blunn AO, to conduct a review of the regulation of access to communications under the *Telecommunications (Interception) Act 1979* (the TI Act).

The Blunn Review is intended to have particular regard to:

- ▶ 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.

As recognised in the terms of reference for this review, any proposals to amend the TI Act are likely to have a significant impact upon the activities of many of the agencies for which the Inspector-General has oversight responsibilities. I met with Mr Blunn on 1 April 2005, and provided the perspective of this office on the matters he is reviewing.

The Blunn Review remained on-going at the completion of the reporting period.

## **Legislation**

### ***Intelligence Services Act***

The ISA was passed by parliament in late September 2001, assented to on 1 October 2001, and came into effect on 29 October 2001.

Despite the apparent coincidence in timing, the ISA was not formulated in response to the 11 September 2001 terrorist attacks on the United States, but had been introduced into parliament several months previously, following recommendations contained in a Commission of Inquiry into ASIS<sup>6</sup> and significant policy development and consultation.

The immediate practical effect of the ISA was to:

- ▶ convert ASIS into a statutory body
- ▶ set out the functions of ASIS and DSD and the limits on those functions
- ▶ authorise the minister responsible for each agency to issue directions to that agency
- ▶ require ministerial authorisation for collection activities intentionally directed at Australian persons
- ▶ limit the circumstances in which responsible ministers can authorise collection of intelligence on Australian persons
- ▶ require the responsible ministers to make rules regulating the communication and retention by the agencies of intelligence information concerning Australian persons, and
- ▶ provide for the establishment of a parliamentary oversight committee, namely the PJCAAD.

While generally satisfied that the ISA was achieving the objectives set for it, my predecessor as Inspector-General, Mr Bill Blick PSM, identified several issues, of a predominantly technical nature, which he believed should be addressed whenever the ISA was next to be amended.

Mr Blick formally pursued this matter with Dr Peter Shergold (the Secretary of DPMC) before his retirement in March 2004. Dr Shergold, wrote to

6 GJ Samuels and MH Codd, Commission of Inquiry into the Australian Secret Intelligence Service, 1994–1995.

me shortly after I took up my appointment agreeing that such a review would be valuable.

This review, which was administrative in character, was conducted by officers of DPMC between October 2004 and March 2005. My office contributed significantly to this review, liaising frequently with the DPMC reviewers on the one hand, and acting as a sounding board for the AIC agencies on the other.

The ultimate result of this review activity was to complement changes flowing from the Flood review, and both sets of changes are included in the ISLA Bill.

### **IGIS Act**

There were no amendments to the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) during the reporting period. However, as indicated elsewhere in this chapter, Mr Flood made several recommendations in his report which will require changes to the IGIS Act.

I took the opportunity presented by the ISA review to propose a number of essentially minor, technical amendments to the IGIS Act. The vehicle for these amendments is also the ISLA Bill.

The amendments which I have proposed to the IGIS Act, separate from Mr Flood's recommendations, include the insertion of provisions which would provide me with a guaranteed right of access to any place where the subject of a detention warrant issued under section 34D of the ASIO Act, is being detained. This change is necessary because the extant legislation only provides the IGIS with a right of access to premises occupied by an AIC agency. If the detention provisions of the ASIO Act were to be invoked, it is likely that the detention would occur at premises other than those occupied by an AIC agency (eg. a gaol or watch-house, or similar such facility).

A minor amendment to section 16 of the IGIS Act has been proposed to provide a clear basis for me to consult with the Commonwealth Ombudsman prior to commencing an inquiry in relation to an AIC agency. This is with a view to avoiding duplication in inquiries and clarifying jurisdiction where necessary.

I have proposed amendments to sections 15 and 21 of the IGIS Act to establish alternative mechanisms for providing advice of an inquiry, and for providing

copies of draft reports relating to inquiries, where the inquiry relates directly to the head of an agency in a personal capacity. The desirability for an amendment of this kind was highlighted by a recent inquiry conducted by this office, in which an agency head was a key figure, rather than being a participant simply by virtue of his office.

The proposed amendments would allow the Secretary of the Department of Defence to serve as the principal point of contact for IGIS inquiries should any future cases arise where the head of any of the Defence members of the AIC (ie. DSD, DIGO and DIO) is personally involved, and the responsible Minister in the case of any of the other members of the AIC.

### **Training**

I have actively sought to make presentations at suitable agency training courses and seminars as often as possible. In 2004–2005 I or a senior member of staff presented to approximately 700 staff in the six agencies.

The presentations are tailored to the particular agency or audience, but all cover the history and activities of this office, the importance of the rule of law and agencies acting in accordance with the law, and the need for accountability and community confidence in their use of special powers and capabilities.

### **Inspections, Complaints and Inquiries**

#### **Inspections**

As in previous years, inspection of the activities of the intelligence collection agencies (namely ASIO, ASIS, DSD and DIGO) has occupied a significant proportion of the resources of the office.

My office visits each of these agencies regularly to inspect operational records, to check that their activities are conducted with propriety and comply with the law. Details of the specific inspection activities are set out in the chapters of this report that deal with each respective agency.

#### **Complaints**

During 2004–05 this office received 33 new complaints leading to preliminary or full inquiries (23 in 2003–04) and 45 new complaints which

specifically nominated an AIC agency that were handled administratively (35 in 2003–04).

Although these raw figures might suggest an increase in public dissatisfaction with the agencies, the increase is attributable to an upsurge in immigration related complaints directed against ASIO.

During the reporting period I pursued 14 preliminary inquiries into complaints about alleged delays on the part of ASIO in conducting immigration related security assessments, and 17 similar complaints were handled administratively. The treatment of these complaints is explained below, and in the chapter of this report dealing with ASIO.

The underlying level of complaint about AIC agencies prior to the terrorist attacks of 11 September 2001 was quite low. There was an upsurge shortly thereafter and in the wake of the Bali bombings in October 2002, driven by an increase in overt operational activity on the part of ASIO (eg the execution of a number of entry and search warrants). In more recent times the level of complaints has essentially stabilised (or, if the immigration related complaints are removed, slightly declined) but can be anticipated to fluctuate depending on the level of operational activity.

### ***Immigration related complaints***

In previous years, this office has received occasional complaints about the timeliness or manner in which ASIO conducts security assessments of individuals seeking protection visas, or permanent residency in Australia. In 2003–04 two such complaints were received which led to preliminary inquiries.

As noted in the preceding section, in 2004–05 there was a marked increase in the level of immigration related complaints to this office concerning timeliness. I initiated a number of preliminary inquiries into such cases.

Upon investigation my office learnt that the workload had increased significantly and that systems employed by ASIO for processing these applications were under significant strain as important resources were reallocated to high priority tasks. Delays were also caused due to issues about the transfer of data between agencies.

Significant resources were allocated in the most recent Federal budget to address various processing

and information technology issues associated with this subject. The government also made an important announcement in June 2005 that included a commitment to timelier processing by the Department of Immigration, Multiculturalism and Indigenous Affairs and by ASIO.

I am hopeful that this injection of funding and the commitment of the responsible agency heads, will address those concerns which gave rise to an upsurge of complaints to my office.

As at the end of the reporting period, there was still a steady stream of immigration related complaints. The practice now is to handle these complaints administratively (eg my office ascertains when the request for a security assessment was levied, where in the queue the application sits, and if there are any unusual features or complexities which would justify a deeper level of inquiry). I will now only proceed to a preliminary or full inquiry in unusual circumstances.

### ***Search warrants***

As has been widely reported in the media, and subsequently confirmed by the Attorney-General, ASIO executed a number of entry and search warrants against persons of interest, in June 2005.

It has also been publicly reported that my office has received complaints relating to the execution of these warrants. These complaints are concerned with whether there was a proper basis for granting the warrants, and allegations that sensitive information was released to the media without proper authorisation, with a view to prejudicing the interests of the subjects of the warrants. My inquiries into these complaints were ongoing as at the end of the reporting period.

Although not strictly falling within the reporting period, I can advise that my office was also contacted in July 2005 by several individuals who had goods seized during the execution of these warrants. In each instance the individuals concerned wished to have the return of those goods expedited.

The terms of the relevant warrants require the return of seized goods within a reasonable time frame. My office has been closely monitoring progress on the return of these goods, to ensure that the terms of the warrants are complied with. These contacts have been handled administratively rather than as inquiries.

### ***Recruitment/employment concerns***

The number of staff employed by the AIC has risen substantially in the last few years. As a consequence, the AIC agencies have been undertaking large-scale recruitment campaigns.

While grievances of staff members within agencies are generally outside my jurisdiction, we received several complaints about recruitment practices and background security checking during 2004–05 which did fall within the jurisdiction of this office. These complaints were, in a relative sense, few in number and were spread evenly across the agencies.

### ***Defence Force complainant***

As was reported in our last annual report, a serving member of the ADF, Lieutenant Colonel Lance Collins, wrote to the Prime Minister in March 2004, with a series of grievances which were subsequently made public.

In his letter to the Prime Minister, Lt Col Collins was critical of an inquiry conducted by my predecessor as IGIS, Mr Bill Blick PSM, which was finalised in May 2003.

I was appointed Inspector-General in late March 2004. Shortly after my appointment, the then Chief of the Defence Force, General Peter Cosgrove AC MC, referred various papers for my independent consideration. I reviewed these papers as well as Mr Blick's report administratively, rather than in the guise of a formal IGIS Act inquiry.

On 3 May 2004, I wrote a letter to Senator the Hon Robert Hill, Minister for Defence (copied to General Cosgrove) offering my views on the papers I had reviewed. I concurred with the majority of findings made by Mr Blick in his May 2003 report but suggested that one line of investigation whilst comprehensive, was not exhaustive. That being so, I suggested that this issue could be pursued by me, as a formal IGIS inquiry.

Senator Hill formally requested me to inquire into this matter, in accordance with section 8(3)(a)(ii) of the IGIS Act, on 6 May 2004.

I provided the report of this inquiry to Senator Hill on 30 November 2004. In my report I suggested that Senator Hill seek further advice from the Secretary of the Department of Defence in respect of certain issues.

Senator Hill issued a press release on 9 December 2004 in which he indicated that he had sought advice from the Secretary to the Department of Defence, on matters raised in my report, and that the Secretary was pursuing legal and administrative issues arising from the report. Senator Hill attached a copy of my letter to him of 3 May 2004 to the press release. This letter is reproduced as Annex 3 to this report.

Senator Hill released an abridged version of my inquiry report publicly on 25 August 2005. This is reproduced as Annex 4.

# Performance

## Resource Allocation

The work of my office is divided between conducting inspections and pursuing inquiries or investigations.

The aim is to devote approximately 60–70 per cent of the resources of the office in any given year to monitoring the day to day activities of the intelligence collection agencies, with a view to identifying concerns while they are in a nascent state, or where possible, anticipating problems before they arise. This is consistent with that envisaged for the office when its establishment was first proposed by the late Justice Robert Hope in the General Report of his *Royal Commission on Australia's Security and Intelligence Agencies*, which was published in December 1984.<sup>7</sup>

Justice Hope's belief that this office should devote the majority of its time and resources to monitoring the activities of the AIC rather than inquiry related work is reflected in his recommendation for the creation of an Inspector-General (to be principally concerned with inspection work), rather than a Security Commissioner or Ombudsman (who would focus largely on complaints).

A thorough and rigorous inspection program can proactively identify issues of potential concern and has a substantial normative effect.

## Performance Indicators

The effectiveness of the office can be assessed against several key performance indicators. The following indicators, which are both quantitative and qualitative in nature, take into account the

unique role and functions of the OIGIS, and the small size of the office:

- ▶ 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 with regard to human rights.

## Timeliness

At the commencement of 2004–05 four full inquiries and five preliminary inquiries remained open. These comprised one own motion inquiry involving ASIS, a ministerial referral in respect of DIO, two preliminary inquiries involving DSD, with the remainder being a mix of preliminary and full inquiries involving ASIO. Each of the above matters was finalised during 2004–05.

In addition to the nine preliminary and full inquiries which were carried over, there were 91 approaches from people with new or continuing complaints against a nominated agency. This compares with a figure of 68 such contacts during the 2003–04 reporting period.

These 91 approaches comprised:

- ▶ 33 new complaints leading to preliminary or full inquiries, five of which remained open as at 30 June 2005 (see Annex 1, Table 1). There were 23 such complaints in 2003–04

7 Justice RM Hope, RCASIA General Report, AGPS, Canberra, December 1984.

- ▶ 13 approaches seeking a previous complaint be reviewed or a new inquiry be conducted (compared to 10 in 2003–04)
- ▶ 28 new complaints where an agency was specifically identified, which were dealt with administratively (see Annex 1, Table 2). There were 35 such complaints in 2003–04, and
- ▶ 17 complaints about alleged delays by ASIO in conducting immigration related security assessments that were handled administratively rather than as preliminary or full inquiries (see Annex 1, Table 3—this is a new table which has not appeared in previous annual reports).

We try to process complaints about AIC agencies which do not proceed to preliminary or full inquiry within a few days at most. Only two such cases remained open as at 30 June 2005, and these were both concluded early in the next reporting period.

In addition to the 100 cases referred to above (ie. nine carried over plus 91 new or resumed complaints), 56 other persons contacted the office with concerns which did not directly refer to or involve an AIC agency (compared to 60 in 2003–04).

Each of these contacts was handled administratively.

Many of the 56 contacts referred to above were from individuals who were clearly suffering from delusional or imaginary concerns, or raised matters which fell outside of our jurisdiction, or sought to provide tip-off information (all such information was passed to the National Security Hotline).

Although nearly 20 years of experience provides a good guide to how long an inquiry is likely to take from inception to resolution, it is not possible or desirable to apply rigid target times for completing preliminary or full inquiries, not least because significant factors which influence when an inquiry is completed do not lie within the direct control of this office. Also important are the complexity and range of issues raised and the accessibility of necessary information.

Notwithstanding this qualification, it has been my wish to reduce the time taken to complete inquiries to the maximum extent that this is within my control and still consistent with a thorough and incisive approach.

In the five years between 1 July 2000 and 30 June 2005, the average time taken for inquiries was 121 days.

The average time taken to finalise preliminary and full inquiries in 2003–04 was 170 days (ie. 24 cases completed in a total of 4,083 days between receipt and finalisation).

In 2004–05, the figure was 75 days (ie. 37 cases completed in 2,762 days).

This should not be read as an absolute guide to the efforts of the office, or suggest particular trends. The office's capacity to minimise the time it takes to conduct its investigations will continue, as always, to depend on the complexity of the cases that come to our attention and the responsiveness of others, as well as our own efficiency.

### Acceptance of Recommendations

It is very rare 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 a formal recommendation in 2004–05, 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 streamlined or improved. These suggestions were generally accepted and acted upon.

I am pleased to advise that the intelligence and security agencies continued to seek the views of my office on draft policies and procedures where issues of propriety and/or legality arose, or were likely to arise.

Where I have an interest or a concern about a particular activity, I do not hesitate to seek a briefing. On all occasions when I have sought such briefings or additional information my requests have been agreed to without question or qualification.

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

## **Level of Assurance**

### ***Number of complaints***

A review of past IGIS annual reports reveals that in the four completed reporting years prior to the terrorist attacks on the United States on 11 September 2001, the average number of new complaints leading to full and preliminary inquiries averaged around 14.25 per annum. In the four years since, this average has risen to 27.75 per year.

While this approximate doubling in the number of inquiries conducted by this office could suggest that the agencies are going awry, these figures must be considered against the differing times in which we live. The terrorist attacks which have been directed against western targets and western interests, as have occurred in the United States, Bali, Jakarta, Madrid, and most recently in London, have prompted an effective doubling in the size of the AIC, the passage of a range of anti-terrorism related security laws and the extension of greater powers to the intelligence community.

It follows logically that this significant increase in powers and resources, combined with a less stable global security environment will necessarily lead to increased investigative effort by the intelligence community within Australia, with consequential impacts on the wider community.

I have made tentative linkages with some community leaders to explain the role and functions of this office, to discuss concerns and to take on-board and seek remedies to valid criticisms. I intend to devote more time to this in 2005–06. 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 during the reporting period a small number of instances were found where the agencies acted beyond their authority. These cases are described in the chapters of this report that deal with each agency individually.

While any instance where an intelligence agency has acted without authority is a matter for concern, the instances detected were few in number and largely technical or procedural in nature. 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 my experience in inspecting and inquiring into those agencies which fall within the remit of the Inspector-General, 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.

The intelligence and security agencies continue to be focussed on achieving the objectives set for them by the parliament and the government, responsive to ministerial direction, aware of the limits of their authority, and concerned to conduct their business in a professional manner.

# Australian Security Intelligence Organisation

## What ASIO Does

ASIO is Australia's 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 main role is to gather information and produce intelligence that will enable it to warn the government about activities or situations that might endanger Australia's security. It is not a law enforcement agency.

The focus of ASIO's work is on terrorism, people who may act violently for political reasons, and people who may clandestinely obtain sensitive government information or otherwise harm Australia's interests in order to further their own causes or the interests of foreign governments.

Under its legislation, ASIO must not limit the right of persons to engage in lawful advocacy, protest or dissent and the exercise of that right shall not, by itself, be regarded as prejudicial to security.

ASIO does not have the statutory authority or the resources 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, such as questioning persons who are believed to possess information which would substantially assist the collection of intelligence in relation to a terrorism offence, telecommunications interception, use of listening devices etc.

Other ASIO functions include collecting foreign intelligence in Australia, and providing security assessments and protective security advice.

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>.

## Senior Appointments

On 17 May 2005, the Minister for Foreign Affairs announced the nomination of the Director-General of Security, Mr Dennis Richardson AO, to be Australia's next Ambassador to the United States of America. Mr Richardson departed ASIO shortly afterwards.

Mr Richardson served as the Director-General of Security (ie. the Head of ASIO) for approximately eight and a half years, following a distinguished and varied public-service career in which he held senior positions in the Departments of Foreign Affairs, Prime Minister and Cabinet, and Immigration and Multicultural Affairs. Mr Richardson also served as the Principal Adviser to Prime Minister Hawke in the early 1990s.

During his lengthy tenure as Director-General of Security, Mr Richardson had dealings with three different Inspectors-General. In the course of these dealings, Mr Richardson revealed himself to be a strong leader with a clearly evident commitment to transparency and accountability.

By choosing to heighten the public profile of his office and the Organisation (through his regular personal appearances before various parliamentary committees, attendance at security related conferences, and direct engagement with various community groups), Mr Richardson did much to demystify the work of ASIO in the eyes of the public.

Mr Richardson and his senior management team also did much to prepare ASIO to cope with a rapidly changing security environment and to make it responsive to challenges which had

not been anticipated when he commenced as Director-General.

In the year or so during which our respective appointments overlapped, I valued Mr Richardson's open and constructive approach to dealings with this office and his day-to-day commitment to accountability in his management of ASIO.

On 10 July 2005, the Prime Minister, the Hon. John Howard MP, announced the selection of Mr Paul O'Sullivan as the new Director-General of Security. At the time of this announcement, Mr O'Sullivan was serving as the Senior Adviser (International) in the Prime Minister's office, having previously been a Deputy Secretary in the Department of Foreign Affairs and Trade, and having completed several senior ambassadorial level appointments.

My initial dealings with Mr O'Sullivan have all been positive, and he has evinced to me, and to his staff, a strong commitment to the principles of fairness and accountability.

## Significant Issues

### Questioning and detention warrants

As discussed in the 'The Year in Review' chapter of this report, the PJCAAD commenced an inquiry during the reporting period into the questioning and detention powers provided to ASIO by Division 3 of Part III of the ASIO Act.

I provided a written submission to the PJCAAD review of these questioning and detention powers on 30 March 2005. A copy of the submission is at Annex 2 to this report. The submission was based on the experiences of my predecessor, myself and my staff, in attending questioning conducted under warrants issued under section 34D of the ASIO Act.

In making my submission to the PJCAAD review, I drew upon information which the Director-General of Security had put into the public domain, namely that ASIO had executed questioning warrants against three persons in 2003–04.<sup>8</sup>

This office was personally represented on all days when the subjects of these warrants were questioned, for the full duration of the questioning with the exception of a relatively brief period on one day (in which questioning occurred for only a short period).

The Director-General of Security provided more up to date information on the number of questioning warrants which had been issued to date, in ASIO's submission to the PJCAAD review, as follows:

*"ASIO reports annually on the number of questioning and detention warrants sought and issued. We do not, however, normally publicly report those totals outside the annual Australian Security Intelligence Organisation Report to Parliament. An exception has been made here for the purpose of the Committee's Review. Eight questioning warrants have been sought and issued since the legislation commenced on 23 July 2003. No detention warrants have been sought or issued since the legislation was enacted."<sup>9</sup>*

Mr Richardson also appeared at a public hearing before the PJCAAD in Canberra on 19 May 2005, and in his introductory remarks provided some additional details on the use ASIO had made to that date of its new powers:

*"The questioning power has been utilised on eight separate occasions since the legislation was enacted in July 2003. The detention power has not been utilised. No individual between the ages of 16 and 18 years has yet been questioned and there has been no strip searching undertaken. The fact that there have been no detentions, no questioning thus far of 16 to 18 year olds and no strip searching is entirely consistent with expectations expressed to this committee at the time and is consistent with what was stated by the then Attorney-General in his second reading speech. It is a good thing that those powers have not had to be utilised ... in the event that they are needed they will be important for the safety of the community."<sup>10</sup>*

8 ASIO Annual Report 2003–2004, unclassified version, pp. 39–40.

9 ASIO submission to the PJCAAD Review of Division 3, Part III of the ASIO Act 1979, submission number 95, paragraph 11.

10 D Richardson AO, evidence to the PJCAAD Review of Division 3, Part III of the ASIO Act 1979, Committee Hansard, 19 May 2005, pp. 4–5.

When I appeared before the PJCAAD the following day, I used my opening remarks, to expand on the role played by my office:

*“For the first three warrants, the office attended on 20 of the 21 days involved. For the reasons given in paragraph 21 of my submission, the practice is now to attend on the first day and then decide if further attendance is required. In the five further warrants, the result has been that I or my staff have attended on the first day and not on subsequent days. I would emphasize that, where there is not attendance on a particular day, my staff and I make a point of reading all of the transcripts carefully and, if necessary, viewing relevant parts of the video.”<sup>11</sup>*

I can confirm, consistent with the limitations imposed by section 34VAA of the ASIO Act, that a number of questioning warrants in addition to the eight referred to by Mr Richardson, were executed towards the end of the reporting period.

Either myself or one of my staff attended at least the first day of questioning under each of these warrants, and we also attended some additional days of questioning.

The overarching conclusions I reached from the questioning sessions attended by my office during the full reporting period were, as follows:

- ▶ In each instance, the basis for requesting the warrant was founded on a strong intelligence case (details of which are provided to me in advance of each warrant being sought).
- ▶ A variety of issuing and prescribed authorities were used, rather than one or two qualified individuals being used.
- ▶ Care was taken to ensure that the serving of the warrant papers was done discretely, with a view to causing minimal overt disruption to the activities of the subject of the warrant.
- ▶ The facilities used for each questioning session were appropriate, with adequate provision made for the needs and requirements of the subjects of the warrant and their legal representatives.

- ▶ The subjects of questioning have been accorded dignity and respect by prescribed authorities and ASIO questioners, despite conduct on the part of some subjects which might be cause for contempt actions were these court proceedings rather than questioning sessions.
- ▶ Information obtained in the course of various questioning sessions appears to have materially assisted ASIO's counter-terrorism related activities.

### **Search warrants**

During 2002–03 this office received a significant number of complaints about ASIO's use of entry and search warrants. The catalyst for several of these complaints was a series of entry and search warrants executed in the weeks following the Bali bombings of October 2002.

The then Inspector-General, Mr Blick, conducted inquiries into each of these complaints, all of which were concluded during 2003–04 and reported in that year's annual report. Mr Blick found that generally the complaints could not be substantiated but he did identify some procedural issues in relation to the conduct of the searches and recommended that ASIO and concerned law enforcement agencies should work towards a common understanding of each party's roles and responsibilities.

During 2004–05, I met with the Director-General of Security, the Commonwealth Ombudsman, and senior officers from the Australian Federal Police (AFP), to discuss the development of a memorandum of understanding (MOU) or agreements between ASIO and the AFP, to clarify the respective responsibilities of each party when both agencies are involved in the execution of such warrants.

Work on this is continuing, but in the meantime the Ombudsman and I will continue to work together to monitor and oversight joint operational activities of this kind. I would expect that when this work is completed, a similar approach might be applied to state jurisdictions, where there is operational cooperation between ASIO and local police services.

<sup>11</sup> I Carnell, evidence to the PJCAAD Review of Division 3, Part III of the ASIO Act 1979, Committee Hansard, 20 May 2005, p. 2.

As mentioned earlier in this report, ASIO executed a number of overt entry and search warrants in the later part of the reporting period which received significant amounts of media coverage at the time.

My office received complaints arising from the execution of these entry and search warrants. These complaints were made by individuals with a direct involvement in these matters, their legal representatives, and community groups/concerned individuals with no direct involvement but a genuine concern that ASIO be held accountable for its actions. These complaints raised a range of issues, including:

- ▶ whether the legislative requirements had been met for the issue of the warrants
- ▶ whether ASIO had been responsible for the alleged unauthorised disclosure of information to the media, tipping the media off that a series of “raids” were to be conducted
- ▶ whether the alleged unauthorised disclosure of information about the subjects of the warrants had been orchestrated to deliberately prejudice the interests of these individuals, and
- ▶ in those instances where goods or property were seized, ensuring that this material was returned in a timely manner.

Each of these complaints, which were received in the last weeks of the reporting period, were the subject of ongoing inquiries, or administrative action, at the end of the reporting period.

It is worthy of note that none of the complaints received in this office about ASIO’s operational activities in June 2005, were along the lines of the complaints received in 2002–03. This indicates that what lessons there were to be drawn from the execution by ASIO of various entry and search warrants in 2002–03, have apparently been learnt, and that this experience has informed the planning for these later overt searches.

### ***Immigration related issues***

As discussed in ‘The Year in Review’ chapter of this report, there has been a noticeable increase in the number of complaints about the timeliness with which ASIO processes security assessments for immigration applications.

I initiated preliminary inquiries into a significant number of these complaints, and the remaining complaints were handled administratively.

In June 2005, the government announced that it was committed to more timely processing of immigration applications by those agencies which are involved in such matters. This commitment combined with additional resources should contribute to a reduction in the time it takes for immigration applications which require individual security assessments to be processed.

As at the end of the reporting period, we continued to receive immigration related complaints but the numbers appear to be reducing.

### ***Training***

I believe it is important for the role and functions of my office to be visible to as wide a cross-section of AIC staff as possible, and that we should wherever possible promote and reinforce messages about acting legally and with propriety. To this end, my staff and I accept as many invitations as possible to present at AIC-wide and agency specific training courses.

During 2004–05 either I or a member of my staff presented at seven in-house training courses run by ASIO on the subject of ethics and accountability.

I was especially pleased that one of these courses was run specifically for ASIO’s generalist intelligence officer (GIO) trainees as a part of their induction into the Organisation, as this served to emphasise at the outset of their careers the importance of ethical conduct and accountability.

I also attended a residential component of the GIO training course, so that I could witness some of their training first hand, and address any questions the trainees might have in a less formal/intimidating setting than might have been presented in their initial period with the Organisation.

In addition to the above, my staff and I regularly present at the AIC-wide common induction program which has been developed in response to a recommendation in the Flood report. A number of dedicated spaces are reserved for ASIO personnel to attend these courses.

So as to have a better understanding of the work of ASIO, the former Director-General of Security, Mr Richardson, extended a general invitation

for myself and my staff to attend other training courses run by the Organisation. The office took advantage of this invitation during the reporting period to attend some courses where there was a clear overlap between the course content and the interests of this office.

## Inspection Activities

### *Scope and reporting arrangements*

Due to its role and functions, ASIO is the AIC agency most likely to come into contact with members of the Australian public. It follows logically that ASIO's intelligence collection activities should be subjected to more intensive and more frequent review by the Inspector-General than any of the other members of the intelligence community.

The largest concentration of ASIO staff is in Canberra where the Organisation has its headquarters. ASIO also has offices in other mainland capital cities, and a network of liaison officers who are based overseas.

Since becoming Inspector-General, I have increased the frequency of visits to ASIO's central office and to its various state collection offices to match the increasing operational tempo of the Organisation. During the reporting period, my staff and I conducted 36 inspection visits to ASIO's various offices. In most (but not all) instances, two staff conduct these inspections.

It is my objective to visit each of ASIO's Australian collection offices at least once each year, and my office visits the busier offices three to four times a year (or more frequently if other work takes us to those localities). During 2004–05 this objective was achieved.

It has been the practice of successive Inspectors-General to write to the Director-General of Security upon taking office, and set out the range of inspection activities they plan to undertake. I did so myself, shortly after my appointment as Inspector-General.

In my letter to the then Director-General of Security, I indicated that if any concerns or matters worthy of comment were to arise during an inspection activity, a member of my staff or I would discuss them with an appropriate senior manager or liaison officer in the first instance. I also indicated that following each inspection visit I would write to the Director-General with a summary of findings.

I reiterated that commitment to the Director-General in December 2004, when I wrote to him setting out the proposed visits schedule for the 2005 calendar year.

During the reporting period, and consistent with my advice to the Director-General, this office inspected records associated with the following ASIO activities:

- ▶ warrant operations
- ▶ authorities to investigate
- ▶ access to, and use of, information obtained from the Australian Transaction Reports and Analysis Centre and the Australian Taxation Office
- ▶ provision of information to, and liaison with, law enforcement agencies
- ▶ the official use of alternative documentation to support assumed identities, and
- ▶ compliance with the Archives Act.

### *Warrant operations—procedures*

ASIO has access to a range of special powers to assist it to perform the functions mandated for it by parliament. These special powers can only be used in limited circumstances following the issue of a properly authorised warrant.

The use of special powers is provided for under Divisions 2 and 3 of Part III of the ASIO Act, and various sections of the TI Act.

The Attorney-General is the issuing authority for all special powers warrants, with the exception of questioning and detention warrants issued under section 34D of the ASIO Act. The issuing authority for s34D warrants will ordinarily be a Federal Magistrate or a Judge. A s34D warrant cannot be sought from an issuing authority unless the Attorney-General has consented to this action.

In addition to questioning and detention warrants there are the following powers warrant categories:

- ▶ telecommunications interception (including named person warrants)
- ▶ entry and search
- ▶ computer access
- ▶ listening device
- ▶ tracking device relating to persons or objects, and
- ▶ inspection of postal and delivery service articles.

Shortly after becoming Inspector-General I increased the frequency of our warrant inspection visits to ASIO's central office from bi-monthly visits to monthly. This frequency was maintained during 2004–05 and the duration of those visits was increased.

My decision to increase the frequency of our warrant inspection activities reflects my belief that the use by ASIO of special powers (which by their nature significantly intrude upon the privacy of individuals), requires special scrutiny by this office.

The increase in the duration of these inspections is a by-product of the growth in the size of the Organisation and the range and number of investigations undertaken by the Organisation in recent years.

In scrutinising ASIO's warrant related activities, we particularly check that:

- ▶ the intelligence or security case that ASIO has made in support of the application is soundly based
- ▶ the individuals named in these warrants are actually identical with, or closely linked to, persons of serious security interest
- ▶ appropriate internal approvals for the request have been obtained
- ▶ the Director-General has identified in writing those individuals whom may execute the warrant, or communicate information obtained from the warrant
- ▶ that appropriate certifications or approvals external to ASIO have been obtained (eg the Attorney-General, and in the case of s34D questioning and detention warrants, the issuing authority)
- ▶ reports to the Attorney-General of the outcome of executed warrants are factual and have been provided in a timely manner, and
- ▶ the activity concerned did not begin before, or continue after, the period approved.

During the office's rolling visits programme, the aim is to inspect supporting documentation for all warrants which are issued and to review each report which is provided to the Attorney-General on the use to the Organisation of information obtained through the use of each special powers warrant.

This frequently involves reviewing the same warrant documentation file more than once during any given reporting period.

During the reporting period, the inspection results were that in each case where a warrant had been issued, ASIO had:

- ▶ reasonable grounds for seeking the warrant
- ▶ provided sufficient information for the Attorney-General (or the issuing authority in the case of s34D warrants) 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 manner, and
- ▶ maintained the key accountability documents on the relevant files for examination by the OIGIS.

As the resources of the office permit, my staff and I also periodically review a sample of operational management files alongside the warrant documentation files. In the past the inspection of operational management files relating to warranted collection activity has usually occurred only in the context of a preliminary or full inquiry being conducted into a complaint. I am hopeful of reviewing more such files, as a regular inspection activity, in the year ahead.

### ***Outcome of warrant inspections***

While it is my intention for this report to be as comprehensive as possible, ASIO's warrant operations tend to be highly classified (for quite valid source protection and operational security reasons). As a consequence, while we have tried to fairly reflect the outcomes of our inspection activities, some details necessarily cannot be included.

### ***Unauthorised telephone interception***

There was one instance of an error which potentially could have resulted in unlawful telephone interception during 2004–05. This compares to three instances of inadvertent unlawful interception in 2003–04.

In the case in question, ASIO sought and obtained a named person's warrant under section 9A of the TI Act in respect of an individual of security interest. However, ASIO inadvertently provided the telecommunications carrier with an incorrect telephone number. The telecommunications carrier duly complied with this request, unaware that a wrong number had been provided to it.

Fortunately, the number which was incorrectly nominated for interception was not actually an active (ie. connected) service at that time. Although the potential existed for unauthorised collection to have occurred, as the intercepted service was not connected, this did not happen. All action for interception was ceased immediately the error was identified, and the correct service was then placed on cover.

I am satisfied that ASIO has appropriate checking procedures in place to ensure mistakes of this kind do not ordinarily slip through, however, on this occasion those processes failed to identify the transcription error described above. I accepted that this was a product of genuine human error, rather than evidence of a widespread systems failure or of anything more sinister.

### ***Interception management systems***

Prior to the above mistake being identified, I had already instituted independent checking of the technical systems ASIO has in place which facilitates some of its warranted intelligence collection activities. The desirability of undertaking these checks was reinforced by the above case.

In the course of regular warrant inspections, my staff and I will sometimes identify details of telecommunications services which are being, or have been, the subject of interception activities. We also note the expiry dates of the warrants which authorise such collection.

On a periodic basis, we interrogate ASIO's interception management systems, to check that collection is only occurring against numbers which are listed on properly authorised warrants, and within the specified collection period.

The office also interrogated these systems using telephone numbers of persons of past interest to ASIO (taken from expired warrants), and of persons of possible interest (where this information

is available to us), as an additional check on the integrity of the system.

When conducting checks of this kind, services which the management system shows to be on cover are also randomly selected, and checks are then made that a valid and current warrant exists, authorising collection.

I am pleased to advise that none of these independent checks revealed any instances of unauthorised or inappropriate collection.

### ***Warrant related processing issues***

The number and variety of warrants used by ASIO has risen significantly in the four years since the terrorist attacks which occurred in the United States of America on 11 September 2001. The increase in the number of warrants being sought has put pressure on all sections of ASIO, not least the Warrant Documentation Section, which has to process an increased number of requests.

Notwithstanding the vigilance of the staff in this section, some processing errors will inevitably occur. In this reporting period, the office identified some processing errors ranging from inconsequential to potentially quite serious.

One was an anomaly relating to certain authorisation lists. These are lists in writing, endorsed by the Director-General (or a senior officer of the Organisation appointed by the Director-General) of officers and employees of ASIO, and other people, authorised to exercise on behalf of the Organisation, the authority conferred by the relevant warrant, and/or to communicate information which has been obtained under the warrant.

The preparation and maintenance of such lists is required by various provisions of the ASIO Act and the TI Act.

In one instance ASIO brought to our attention that signed authorisation lists could not be located in respect of a particular operation. This being so, either of two scenarios were likely to pertain:

- ▶ if the authorisation lists had been put to the Director-General and signed, there would be no legal consequences flowing from the subsequent absence of the lists (but it would be prudent to issue new/substitute lists as soon as possible), or

- ▶ if the lists were not put to the Director-General, or put forward and not endorsed, it was possible that action purportedly taken under the warrant may have been unlawful, despite the fact that the warrant itself is valid.

I accept that it is extremely unlikely that authorisation lists were not prepared for this operation, or if they weren't, that their absence would not be noticed in the various internal and external checking processes that each warrant request is subjected to before submission to the Attorney-General.

Based on the experience of this office in reviewing warrant documentation over many years, the fact that ASIO brought this problem to our attention, and that the warrant package was subjected to several layers of review before it was endorsed, I believe that in all likelihood the lists were put forward and signed by the Director-General but then either misfiled or accidentally destroyed.

The period between the date of effect of the warrants and the date when the absence of the authorisation lists was noted was quite short. Replacement authorisation lists were issued on the same day that this anomaly was identified.

I advised the then Director-General of Security that I did not consider this matter indicative of a systems failure, but did take the opportunity to highlight the importance of ensuring that authorisation lists are correct in every detail and available for checking, lest the conduct of an operation be threatened.

Two instances were noted where ASIO had mistakenly advised a telecommunications carrier that warrants had been endorsed by the Attorney-General, 24 hours before the endorsement had actually been obtained. Neither of these requests was actioned before this mistake was identified, and in consequence the only collection which occurred was legally authorised. However, the importance of avoiding such mistakes in the future was emphasised to ASIO.

During an inspection my staff identified a potentially significant processing defect relating to a particular warrant. The records we reviewed indicated that the Attorney-General had read the warrant request and approved the operation, but there was no indication that he had signed the warrant itself.

This was drawn to the attention of the responsible officer, who was able to confirm that the warrant had not yet been executed for technical reasons. Further action under the warrant was immediately ceased whilst a replacement warrant was put to the Attorney-General, and subsequently endorsed.

### ***Timeliness of reporting on warrant outcomes***

As in the last reporting period, the timeliness of warrant outcome reporting provided by ASIO to the Attorney-General was queried.

While there is a statutory requirement for ASIO to report to the Attorney-General on the outcome of every warrant issued to it, the only mandatory timeframe for the provision of these reports is imposed by section 17 of the TI Act, which requires the Director-General of Security to furnish reports of TI related warrants within three months of expiry or revocation.

By contrast, section 34 of the ASIO Act simply requires the Director-General to furnish a report to the Attorney-General in respect of each (non-TI) warrant, ie. it does not specify a period within which reports must be provided.

There were at least four instances where reports were provided to the Attorney-General in the range of 6–12 months after the expiry of the relevant warrants, and two reports in respect of questioning warrants which were provided more than a year after their execution (although I understand early oral briefings were given to the Attorney-General).

In respect of the former instances I wrote to the then Director-General of Security suggesting that unless there are exceptional circumstances it should be possible to provide reports on non-TI warrants within 90 days. The latter instances, relating to reporting on the utility of questioning warrants, prompted me to recommend in my submission to the PJCAAD review of Part III of Division 3 of the ASIO Act, that section 34P of the ASIO Act should be amended to require ASIO to provide such reports to the Attorney-General within 90 days.

Notwithstanding the above comments, the majority of ASIO reporting on the outcome of warrants and the utility of the information obtained occurs in a timely fashion.

### ***Authorities to investigate—procedures***

Prior to the investigation of an individual or organisation by ASIO, the Attorney-General's Guidelines and ASIO's internal policies and procedures require the preparation and approval of an authority to investigate (ATI).

The initial ATI process involves the formal identification of the person or organisation to be investigated and proposes the level of the investigation (as set out in the Attorney-General's Guidelines), and the objectives and duration of the investigation.

The seniority level at which an ATI can be approved is dictated by the nature and sensitivity of the investigation being proposed. The more sensitive or intrusive the proposed investigation, the more senior the authorising officer in ASIO has to be.

My staff and I aim to review all ATIs which are issued. To achieve this ASIO's central office is visited at least every two months (sometimes more frequently), and ASIO's other domestic offices at least annually. During 2004–05 we conducted 19 ATI inspections.

My office revamped its internal ATI checklist to ensure rigour in the review process. Issues regularly looked at include:

- ▶ whether there were reasonable grounds for the request
- ▶ whether the level of the ATI is appropriate for the proposed investigative activities
- ▶ if the proposed duration of the approval is appropriate or excessive
- ▶ what limits, if any, have been placed on the investigative activity, and whether these are 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 is placed on file.

### ***Authorities to investigate—inspection results***

As with warrant operations, detailed public discussion of specific cases is not possible but comment follows in general terms upon several issues which arose in the course of ATI inspections.

We made a range of suggestions for possible improvements to the ATI template. In all instances the suggestions were acknowledged and where technically feasible, implemented.

Several instances were noted where, due to an administrative oversight, different ATIs were issued on the same individual within a few days of each other. We suggested that, if possible, applications for an ATI on an individual on whom an ATI already exists should be automatically rejected.

Some quality control issues were raised, relating to the inclusion of irrelevant (ie. accidentally transposed) information in an ATI which had no relationship to the person of interest.

We also identified several instances where the review dates proposed by the originating officer and authorising officer were inconsistent and could give rise to confusion about the duration of the authorisation.

The office identified several instances where ASIO's internal policy requirement that warrant operations be supported by a current ATI had not been fully met (due to the lapsing of one ATI and a gap of several weeks before renewal).

I was satisfied that the ATI processes are taken seriously, and certainly that requests are made only when there is a valid basis for doing so. Since becoming Inspector-General, I have noticed an improvement in the standard of ATIs, and those issues identified as being of concern in this reporting period are all fairly minor.

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

The continuing focus on counter terrorism activities during the reporting period necessarily involved close cooperation between ASIO and law enforcement agencies.

During regular visits to ASIO's state offices the office examines the Organisation's files which deal with liaison with local law enforcement agencies and any exchanges of information about individuals of security interest.

In conducting the reviews of these files we paid particular attention to the passage of, storage, and access to, information on persons of intelligence interest to law enforcement agencies. ASIO's control measures were found to be satisfactory.

### **AUSTRAC and the Australian Taxation Office**

The *Financial Transactions Reports Act 1988* (FTR Act) and the *Taxation Administration Act 1953* provide for ASIO to obtain information from the Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Australian Taxation Office, in strictly prescribed circumstances. The procedures involved in ASIO accessing financial transaction reports and taxation information are set out in MOUs between the respective parties.

The IGIS and the Director of AUSTRAC have also entered into a MOU covering oversight issues and the Inspector-General provides an annual report to the Attorney-General on ASIO's compliance with its obligations.

I provided a report to the Attorney-General on 1 September 2005, covering the 2004–05 reporting period, certifying ASIO's compliance with the requirements of the FTR Act and the terms of its MOU with AUSTRAC.

During this reporting period, my staff conducted eight AUSTRAC related inspections.

In the course of the inspections, one instance was noted where checks were undertaken four months after the relevant ATI had expired. While the requirement for an ATI is an internal rather than statutory requirement, the need for these requirements to be met was reinforced.

My staff and I, in consultation with AUSTRAC, have been involved in the scoping of an electronic template, which should assist in eradicating errors of this kind. This template will be developed by AUSTRAC.

ASIO has consulted my office on the development of revised internal guidelines dealing with access to, and the communication of, financial transaction records which are relevant to security investigations.

Overall, an improvement was noted in the quality of requests for AUSTRAC checking during the reporting period. This improvement appears to have been built on a greater familiarity/understanding of what such checking can and cannot deliver, and good internal guidance.

As indicated earlier, ASIO also has access to taxation records in strictly prescribed circumstances, although it does so relatively infrequently. My office reviews all instances where ASIO seeks and/or obtains access to taxation records. On the basis

of these review activities, I am satisfied that ASIO is complying with the requirements of the MOU between itself and the Australian Taxation Office.

### **Use of assumed identities**

The insertion of Part IAC into the *Crimes Act 1914* (Crimes Act) came into effect on 12 October 2001. This requires Commonwealth agencies that issue or use alternate identity documentation, to maintain appropriate records.

Section 15XUA(1) of the Crimes Act requires ASIO, as soon as practicable after 30 June each year, to provide the IGIS with a report for the year just ended. The Director-General of Security furnished me with such a report for 2004–05 on 5 August 2005.

The report showed that ASIO issued an increased but still moderate number of authorisations for the use of assumed identities by its officers for appropriate purposes.

The Director-General of Security also provided me with six-monthly internal audit reports which indicated no concerns had been identified in the issuing, variation, use, and cancellation of relevant supporting documentation.

During 2004–05, my staff independently inspected ASIO's assumed identity registers on four separate occasions. We reached the same conclusions as ASIO's internal auditor and the Director-General of Security.

### **Archives**

The Director-General of Security provides my office with comprehensive quarterly progress reports on ASIO's performance in meeting its obligations under the *Archives Act 1983*. These reports provide good insight into ASIO's workload in respect of applications for access to 'open-period' records (ie. documents which are more than 30 years old) and the extent to which statutory timeframes for consideration/release of such material are being met.

The Director-General's quarterly reports on archive related activities also provide an indication of any trends which might be developing, in relation to requested material, or possible difficulties in meeting high volume requests.

I also meet periodically with relevant ASIO staff to discuss their handling of significant archive issues.

Complaints are sometimes received about the handling of archives access requests but we received no such new requests during 2004–05.

Although I will consider pursuing archive related complaints about ASIO (when they raise issues of contemporary significance), my inclination is to remind individuals who are dissatisfied with decisions on archives applications that they have the right to have such decisions reviewed by the Administrative Appeals Tribunal.

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

### **Contact with staff**

My staff and I regularly address training sessions for ASIO officers on accountability issues and the work of this office. I believe this is an important responsibility and as a consequence readily accept invitations to speak to ASIO staff.

ASIO officers brief me from time to time on matters that touch upon the work of the office, or to seek an independent opinion. The former Director-General of Security, Mr Dennis Richardson, placed no barriers to contact between ASIO staff and this office, and his successor, Mr Paul O'Sullivan, is similarly minded.

Due to a combination of history, the terms of their employment contracts, and fears of possible disruption to their essential activities, ASIO staff have as a matter of practice not belonged to trade unions but have had their interests represented to management by a Staff Association.

I have continued the practice of my predecessors of meeting with the President of the ASIO Staff Association, on at least an annual basis. Due to a changeover in this leadership position, I had two such meetings during 2004–05.

### **Complaints and inquiries**

Five full or preliminary inquiries into complaints about ASIO were carried over from 2003–04. Each of these inquiries was finalised in 2004–05.

The office conducted preliminary inquiries into 23 new complaints about ASIO (compared to 10 in 2003–04), and initiated full inquiries into four new complaints (two in 2003–04).

The office received 50 other complaints about ASIO, from individuals seeking to reopen former complaints, or new complaints allegedly involving ASIO (compared to 35 in 2003–04). These complaints/requests were handled administratively rather than as preliminary or full inquiries.

The increase in the number of preliminary inquiries and complaints about ASIO handled administratively, is attributable to complaints about the timeliness with which ASIO handled requests for security assessments on immigration applicants. A fuller explanation of this is contained in 'The Year in Review' chapter of this report.

Some of the complaints or referrals leading to inquiries by this office are summarised below.

### **Possible forewarning of the Bali bombing**

Following the terrorist bombings in Bali in October 2002, the Prime Minister asked my predecessor to conduct an inquiry to establish whether Australia's intelligence community or the AFP, had advance warning of the bombings.

Mr Blick conducted a thorough investigation before reaching the conclusion that there was no such advance warning available to any of the agencies whose records he had examined. An unclassified version of Mr Blick's report is contained in the 2002–03 IGIS Annual Report (which is accessible via the IGIS website at <http://www.igis.gov.au/annual.cfm>).

The Flood review also considered material relating to the Bali bombing, in preparing an appreciation of how Australia's foreign intelligence agencies understood/responded to Jemaah Islamiya (JI) and its emergence as a significant terrorist network in our region.

In the report of his inquiry, which was published in July 2004, Mr Flood made the following pertinent observation:

*"The Inquiry has seen nothing to indicate that any Australian agency, including ASIO, had any specific intelligence warning of the attack in Bali. This is consistent with the findings of the Inspector-General of Intelligence and Security's report on the Bali terrorist attack."<sup>12</sup>*

<sup>12</sup> Flood, p. 42.

Shortly after the publication of Mr Flood's report, a member of the public raised some concerns with a member of parliament, suggesting that notwithstanding these investigations, ASIO might well have had forewarning of the Bali bombings.

The basis for these concerns was that the complainant was a personal acquaintance of an ASIO officer and his wife, and was staying with the couple for the days either side of the bombing incident.

The complainant indicated that the ASIO officer with whom she was staying had received a call on the evening prior to the bombing requiring him to return to his office to receive a communication. The complainant construed from this, and other indications, that ASIO could well have had advance notice of the impending atrocity.

With the agreement of the person concerned, this matter was referred to me by the member of parliament for consideration. I deemed it appropriate to conduct a full inquiry.

In my investigation, which involved interviewing the ASIO officer in question, examining communication records, and accessing relevant files, I was able to satisfy myself that a single faxed document was indeed sent to the ASIO officer on the night of 11 October 2002, but that document could not be construed as in any way constituting forewarning of the bombings.

In light of the above, I concluded that while the complainant was sincere, there was nothing in the information they provided which indicated specific knowledge on the part of ASIO of the impending attack. It does not cast into doubt the relevant conclusions of my predecessor's inquiry or the Flood review.

#### ***Possible AIC complicity in the arrest and detention of an Australian citizen***

I became aware in the second half of the reporting period, via media reporting, of allegations that an Australian person with dual citizenship had been arrested and detained in his former homeland. Claims were made that members of the AIC may have had some involvement in his arrest and purported torture.

Given the serious nature of these claims I initiated preliminary inquiries with ASIS and ASIO, as I considered these agencies would be the most likely to have had dealings with, or knowledge of, the individual concerned.

I saw no indication that either agency had acted in the manner suggested, and insofar as these agencies might have had any interest in the individual, this was entirely appropriate.

#### ***Inappropriate interference in personal affairs***

In the first half of the reporting period, I received a complaint that an ASIO officer had exerted undue pressure on the marriage of two persons, with a view to taking operational advantage of any resulting domestic disharmony.

The sensitive subject matter associated with this complaint precludes me from providing fuller details, but upon investigation I concluded that ASIO had not acted unprofessionally or improperly.

#### ***Generalist intelligence officer training***

In October 2004, I received a complaint about the quality of the training offered to trainee generalist intelligence officers and a range of cognate human resource development issues. After discussions and consideration of the person's options, I decided at that time to exercise my discretion under section 11(2) of the IGIS Act not to conduct an inquiry.

The complainant in this matter provided additional information later alleging bullying, partiality in the treatment of trainees, and issues surrounding performance feedback. I then decided to initiate a full inquiry into these matters, and this inquiry was still in train at the conclusion of the reporting period.

# Australian Secret Intelligence Service

## What ASIS Does

ASIS was established by executive order on 13 May 1952 and operated under government directive until the *Intelligence Services Act 2001* (ISA) came into effect on 29 October 2001.

ASIS collects foreign intelligence, generally relying on human sources to obtain information. It produces and disseminates intelligence reports to key government decision-makers. It also undertakes counter-intelligence activities, liaises with overseas agencies, and undertakes other activities formally directed by the Minister.

The intelligence collection, reporting and other activities of ASIS are regulated by ministerial directions, ministerial authorisations and privacy rules, which have been made pursuant to the ISA.

Intelligence 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

### Founding Director-General

Alfred Deakin Brookes, the founding Director-General of ASIS, died on 19 June 2005, at the age of 85.

In mid-1950, Mr Brookes persuaded the government of the day of the utility of establishing an organisation, modelled on the United Kingdom's Secret Intelligence Service (also known as MI6). The government agreed and the resulting organisation, ASIS, was established in May 1952.

Mr Brookes served as the head of ASIS from its inception until the completion of his five year appointment in 1957, following which he left public employment for the private sector.

### Queen's birthday honours

The Director-General of ASIS, Mr David Irvine, was made an Officer of the Order of Australia, in the Queen's birthday honours list which was announced on 13 June 2005.

Mr Irvine, who enjoyed a long diplomatic career with the Department of Foreign Affairs and Trade before being appointed Director-General of ASIS in February 2003, received his award "for service to furthering Australian international interests and the development of trade link, particularly in negotiating a bilateral agreement with China for the supply of energy."

### Weapons and/or self-defence

In last year's annual report I wrote of the passage through parliament of amendments to the ISA that aimed to afford greater protection to ASIS persons overseas, through the provision of, training in, and use of, weapons and/or self-defence techniques, for protection purposes only<sup>13</sup>.

ASIS actively consulted Commonwealth agencies which have practical experience in the handling, storage and use of weapons and self defence techniques, in the development of the guidelines required by Schedule 2 of the ISA. I was also consulted in this process, which continued into this reporting period. I made suggestions for improvements to the draft guidelines before they were finalised and my suggestions were all accepted.

13 IGIS Annual Report 2003–2004, pp. 6–7, 30–31.

In the period since the guidelines have been finalised, I have taken a close interest in their implementation.

ASIS is required by clause 1(5) of Schedule 2 of the ISA to provide the IGIS with copies of all approvals issued by the Minister of Foreign Affairs in respect of training in the use of a weapon or in self-defence techniques or the provision of a weapon.

I had visibility of all such approvals granted both through the regular examination of each submission made by the Director-General of ASIS to the Minister for Foreign Affairs, and the copying to me of each approval which specifically dealt with weapons and/or self-defence.

It is not possible in a public report to provide details of these approvals, however, I can report that the number of persons who were approved to receive weapons and/or self-defence training during the reporting period was very small, and that an even smaller number than this were authorised to carry/use weapons and/or self-defence techniques when they were deployed in certain situations.

The training afforded to the above cohort appeared to be comprehensive and appropriate, and the cases put to the Minister for approval were soundly based given the circumstances in which the officers in question were to be deployed.

I will continue to monitor approvals given under Schedule 2 of the ISA closely in the coming reporting period.

### ***ISA immunity provisions***

In recent IGIS annual reports, both my predecessor and I have made specific reference to the immunity provisions (section 14) of the ISA.

Section 14 provides that a staff member of ASIS or DSD is not subject to civil or criminal liability for certain acts that might otherwise attract liability, provided that the act is done in the proper performance of a function of that agency. A further provision of section 14 empowers the Inspector-General to certify in writing facts relevant to whether an act was done in the proper performance of the agency's functions.

Following the enactment of the ISA, protocols were drafted so that in the event of any claim for immunity under the legislation, consultation with the Inspector-General and consideration

by law enforcement agencies could be more easily facilitated.

Protocols have been signed with all police services except two. Despite the best efforts of ASIS and the Attorney-General's Department this situation did not change during the reporting period.

While it is true that the immunity provisions can operate regardless of whether protocols are in place, and also that the provisions have not been invoked since the Act came into being, one would hope it is not beyond our federal system to achieve a common approach.

### ***ISLA Bill 2005***

As discussed in 'The Year in Review' chapter, a Bill is presently before parliament which, if passed, will further amend the ISA.

The majority of the proposed amendments contained in the ISLA Bill spring from recommendations contained in the Flood Review, or suggestions made to the review of the ISA which was conducted by DPMC.

Given that ASIS has operated successfully within the framework established for it by the ISA, the proposed changes in respect of the Service are not extensive.

### **Inspection Activities**

The inspection activities carried out by this office in respect of ASIS are:

- ▶ monitoring compliance with the ASIS privacy rules
- ▶ reviewing all submissions, including requests for ministerial authorisations, made by ASIS to the Minister, and
- ▶ inspecting current operational files.

The agreed arrangement is that following each inspection activity I write to the Director-General reporting the results of our reviews and outlining any issues raised during these inspections.

It has also been agreed that where appropriate I will bring to the attention of the Minister for Foreign Affairs or the Prime Minister any matter arising from an inspection that warrants such attention. I am pleased to advise that no such matters arose during the reporting period.

### **Privacy rules**

The ASIS privacy rules required by section 15(1) of the ISA, were published at Annex 4 of the IGIS Annual Report for 2001–02, and can also be accessed on the ASIS website ([http://www.asis.gov.au/rules\\_to\\_privacy.html](http://www.asis.gov.au/rules_to_privacy.html)).

One of the major ASIS inspection activities of my office is review of ASIS's reporting and other communications for references to Australian persons, and judging whether these references comply with the requirements of the ISA (in terms of collection) and the privacy rules (in respect of reporting and dissemination).

There is no prohibition on ASIS referring to Australian persons in their reporting, but there is a requirement that any such reporting be justified against strict criteria which are spelt out in the privacy rules.

As indicated in last year's annual report, my office temporarily stopped reviewing ASIS's internal processing of these reports (but not the reports themselves) due to differing perspectives on the utility of the records being kept. My intention was to resume these wider examinations following the development of clearer internal guidelines informing ASIS's reporting staff how the privacy rules should be applied, as well as providing guidance on how the related 'IGIS audit' coversheets should be prepared for consideration by this office.

My office worked closely with ASIS in the development of these revised internal guidelines and I endorsed a final draft in September 2004, prior to their issue and circulation to relevant ASIS staff in October 2004.

Following the distribution of these internal guidelines, review of the internal processing has recommenced. In practice this means that my office receives hard copies of each of these reports and their accompanying audit cover sheets bundled together every two weeks or so. The contents are reviewed and comments/observations provided to relevant senior managers within ASIS.

Approximately every two months members of my staff and I meet with senior reporting staff/intelligence coordinators and discuss issues arising out of the rolling reviews. These round-table meetings are a very useful mechanism for me to raise any issues of concern, and in turn, to have

issues of interest or concern to relevant ASIS staff brought directly to my attention.

Although a number of quality control issues were identified in the initial material reviewed following the full resumption of this review activity, these generally flowed from a conservative approach to applying the privacy rules by some ASIS staff, rather than the obverse.

The proportion of ASIS reporting (and other, less formal communications) which contains any reference to Australian persons is very small, when measured against the full range of reports which ASIS issues and/or distributes.

### **Ministerial authorisations**

Another significant change wrought by the ISA was the creation of a formal process whereby the Minister for Foreign Affairs, rather than the Director-General of ASIS, was empowered to authorise certain of ASIS's activities (eg. entering into formal relationships with foreign liaisons, opening or closing ASIS stations, approving any activities carried out for the purpose of collecting intelligence on Australian persons etc.)

Given that ASIS is a foreign intelligence collector there are very few instances where ASIS seeks ministerial authorisation to deliberately collect intelligence information on Australian persons.

My office reviews all ministerial authorisations, and I am satisfied on the basis of these inspections that ASIS only seeks approval to collect intelligence information on Australian persons where there is a sound basis for doing so, and that the submissions referred to the Minister contain sufficient detail for well informed decisions to be made.

In addition to reviewing all requests which are put by ASIS to the Minister for Foreign Affairs to authorise particular activities, I also have access to, and review, all other submissions which the Director-General puts to the Minister.

My purpose in reviewing this material is so that I might place the Service's ministerial authorisation requests within the context of the full range of ASIS's operational activities.

As a consequence of reviewing ASIS's ministerial submissions, I have sought oral and written briefings from the Director-General on a range of subjects.

These briefings included but were not limited to subjects such as ASIS's internal and operational audit functions, foreign liaison arrangements, joint operational activities, and internal administrative arrangements.

### **Review of operations**

A member of my staff and I devote approximately four person days per month to visiting ASIS headquarters and reviewing current operational files. The purpose of this review activity is to monitor whether ASIS's operations are being conducted with legality and with propriety.

This review activity naturally has a retrospective focus as I subscribe to the view that it is not the proper place of the IGIS to second-guess operational decisions as they occur, or attempt to manage operational matters at one remove.

During the reporting period, a thematic approach to the files selected for examination was taken, rather than reviewing a random selection of files across several subject areas.

For the most part, the operational cases reviewed in 2004–05 were well planned and run, and delivered outcomes that were consistent with ASIS's charter. Notwithstanding this generally positive assessment, the review of these files did prompt me to raise a number of issues with the Director-General.

As ASIS's on-the-ground operational activities are among some of its most sensitive work it is not possible to provide details.

The Director-General has provided written replies in all instances where we have required a response, or offered briefings by key staff, and I was satisfied with these responses and briefings.

### **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.

My office had visibility of matters associated with the use of alternate forms of identity documentation through the various inspection and review activities, and the specific briefings sought and received.

The advice provided to this office by ASIS for the reporting period confirmed that no evidence of fraud or any other unlawful activity had been detected.

### **Contact with staff**

I met with a significant number of ASIS officers prior to 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 their behaviour.

I also met 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.

These meetings are 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.

### **Training**

In addition to these pre-departure meetings, members of my staff and I regularly attend training sessions for ASIS officers and inductees, addressing them on accountability issues and the work of the office.

I increased my exposure to ASIS staff compared to last year by attending several residentially based training sessions, meeting with each intake of trainee intelligence officers, and by presenting regularly at the newly commenced AIC common induction course, which has a number of positions reserved for ASIS staff.

### **Complaints and Inquiries**

One incomplete 'own-motion' inquiry into ASIS was carried over this reporting period. This inquiry was concluded in November 2004.

I received one complaint about ASIS which led to a preliminary inquiry, and I initiated a preliminary inquiry into one matter potentially involving ASIS.

In addition to these matters three persons contacted OIGIS with queries or concerns about ASIS which were handled administratively (ie without need for formal inquiry action).

The own-motion inquiry and one of the preliminary inquiries are described below. The other preliminary inquiry has been covered in the ASIO chapter.

### ***Own motion inquiry***

In November 2003 my predecessor, Mr Blick, initiated an own motion inquiry into ASIS's handling of a human resource management matter involving allegations of harassment and intimidation, alleged misconduct and the alleged provision of misleading statements to achieve a particular outcome.

Mr Blick was unable to conclude his consideration of this matter prior to his retirement in March 2004. I took carriage of this matter upon my appointment, and ultimately concluded the investigation in November 2004.

Despite repeatedly seeking further information from an individual in respect of the allegations of misconduct and the provision of misleading statements, the information I required was not forthcoming. I therefore did not formally inquire into those particular allegations.

After considering all of the available material relating to the other matters I concluded that:

- ▶ there was no evidence of systematic intimidation or harassment as alleged
- ▶ the instances nominated as evidencing intimidation or harassment did not constitute such behaviour, and
- ▶ ASIS management had dealt with the matter in a proper manner.

### ***Recruitment related complaint***

ASIS, as with the other members of the intelligence community, has received a significant boost to its budget in recent years. Much of this additional funding has been used to recruit new staff. Given the rate at which the AIC has been expanding the number of recruitment related complaints received by this office has been, and remains, very small.

This office received one recruitment related complaint about ASIS during the reporting period, compared to three in the previous reporting period.

In the case in question, an unsuccessful applicant for a position with the Service alleged that there were flaws in the interview process.

Upon investigating this matter, I was satisfied that the selection panel was appropriately composed. I found no evidence that the complainant was treated discourteously or differently from other candidates, and in consequence did not support the complainant's request to be re-interviewed.



DSD was well placed to make a significant contribution to the DPMC review and the development of the ISLA Bill. In recognition of this, and given that many of the proposed amendments will have the greatest impact on the Defence Intelligence Group of agencies (ie. DSD, DIGO and DIO), the Minister for Defence is sponsoring the Bill and steering its passage through parliament.

### Inspection Activities

Shortly after I was appointed as Inspector-General, I wrote to the Director DSD setting out the range of inspection activities I planned to undertake. I wrote to the Director DSD again in December 2004, setting down the inspection activities involving DSD which I planned to undertake during the remainder of 2004–05. These activities include:

- ▶ reviewing ministerial authorisations and other relevant submissions made by DSD to the Minister for Defence on a rolling basis
- ▶ monitoring DSD reporting on a continuous basis 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 each of DSD's collection sites outside of Canberra, as opportunity permits.

The Director and I have also agreed procedures to operate should I form the view that any matter arising from an inspection needed to be brought to the attention of the Minister for Defence or the Prime Minister. No such matters arose during the reporting year.

### Ministerial authorisations

The ISA provides a framework within which DSD can deliberately collect the foreign communications of Australians in certain restricted circumstances. The Minister for Defence must authorise any activity undertaken for the specific purpose, or for purposes which include the specific purpose, of producing intelligence on an Australian person.

In those cases where DSD seeks a ministerial authorisation on an Australian person, and where it is believed that the subject is, or is likely to be involved in an activity or activities that are, or are

likely to be, a threat to security, the agreement of the Attorney-General must also be obtained.<sup>15</sup>

If DSD wishes to obtain a ministerial authorisation to intercept the foreign communications of any Australian person, the Director needs to satisfy the minister that the criteria set out in the ISA for such intelligence collection will be met. To facilitate this end, DSD provides a comprehensive written submission to the minister in respect of each individual it wishes to produce intelligence on.

I have ready access to the details of every authorisation which is approved, and review the more detailed hardcopy documentation on at least a monthly basis.

Although I am not in a position to state how many authorisations are issued in any given year, readers should be assured that the numbers constitute only a very minor proportion of DSD's overall collection activities.

I am satisfied on the basis of the material I have reviewed, and the regular discussions I have with senior DSD staff, that the decision to seek a ministerial authorisation on an Australian person is not taken lightly. I am equally satisfied that in those cases where such a decision is made the submissions which are put to the minister contain sufficient information for the minister to make a well-informed decision.

### Privacy rules

The DSD privacy rules, like the almost identical ASIS privacy rules, regulate the communication of intelligence information about Australian persons collected by DSD. The DSD privacy rules were published at Annex 4 to the 2001–02 IGIS Annual Report, and can also be accessed from the DSD website at [http://www.dsd.gov.au/about\\_dsd/privacy\\_safeguards.html](http://www.dsd.gov.au/about_dsd/privacy_safeguards.html).

The DSD privacy rules require that DSD shall not communicate intelligence information on Australian persons unless certain strict criteria are satisfied.

DSD takes its responsibility to comply with the privacy rules seriously and has established a section within the Directorate which is dedicated to monitoring compliance and reporting standards, providing training, and liaising with customers on privacy and related issues.

<sup>15</sup> Section 9(1A)b, *Intelligence Services Act 2001*.

In addition to DSD's Office of Compliance and Reporting Standards, my own office has access to all DSD end product reports and all other forms of communication which may contain intelligence information relating to Australian persons. This access allows us to independently check DSD's compliance with the privacy rules.

As intimated earlier, the proportion of such reports and messages compared to the total output of reports disseminated by DSD has traditionally been very small, and this was so again during 2004–05.

In addition to the above checking regime DSD maintains a register of every report containing intelligence information about Australian persons, to which I and my staff have ready access. The register, amongst other things, indicates whether each reference was the result of deliberate or incidental collection. My staff and I separately cross-check the veracity of this register by independently interrogating the DSD reports database, on a sampling basis.

My staff and I liaise directly with DSD's compliance staff on any issues that arise in the course of these review activities. For their part, DSD's compliance staff readily contact my office to discuss issues in which they think I might have an interest, or upon which they are seeking an alternative viewpoint. I view this willingness of DSD staff to engage my office on these issues very positively.

### **Monthly meetings**

I have continued the practice of my predecessor of meeting with key DSD personnel on a monthly basis. These meetings ordinarily involve several DSD senior managers, as well as staff from the compliance section, the intelligence policy section, and the legal adviser.

The purpose of these meetings is to enable participants to freely discuss topical issues in which my office has a direct or potential interest. These meetings typically involve broad-ranging discussion on privacy rules casework, collection priorities, ministerial authorisations, legislative and parliamentary reviews, and current legal issues. Any specific briefings I might seek are usually scheduled to coincide with these meetings.

Depending on his availability, I also met with the Director DSD, either prior to, or following each of

these meetings. I have found these meetings to be very useful in gaining a fuller appreciation of DSD's work.

### **Comsec monitoring**

As mentioned in last year's annual report, one section within DSD is specifically devoted to Communications Security (Comsec) monitoring. Comsec monitoring involves intercepting the communications of personnel taking part in selected Defence operations to assess how secure their communications are and, if deficiencies are identified, to instigate remedial action. Comsec monitoring is not directed against members of the public.

Comsec monitoring requires ministerial authorisation. Those whose communications are targeted must be warned in advance. Given the potential of such monitoring to intrude upon the privacy of individuals, I received bi-monthly updates on Comsec activities during the reporting period.

The Comsec monitoring section has been particularly active in the past 12 months providing coverage/support to Australian Defence Force personnel overseas, and in various training exercises.

Based on the briefings I have received, I am satisfied that the responsible staff are properly aware of their responsibilities under the ISA and discharge their duties with appropriate care.

### **New collection activities**

DSD frequently develops new projects involving different approaches to collection of intelligence. DSD regularly informs this office of the nature of such projects and we discuss any issues that might arise concerning legality or propriety. I was briefed on a range of projects during the reporting period, and associated safeguards to ensure that the privacy of Australian persons is protected from unlawful or unreasonable intrusion.

### **Site visits**

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

It is important that staff in these sometimes remote facilities know that they are governed by the same laws and guidelines as apply in DSD's Canberra headquarters.

During the reporting period, I visited two of DSD's more significant sites. I intend to re-visit these and other DSD sites on a periodic basis to reinforce that my remit is not limited because of geographical factors.

## **Training**

DSD continues to devote significant resources to in-house training on the practical requirements of the ISA and the principles underpinning the application of the privacy rules.

As noted earlier in this report in relation to other agencies, I regard training and awareness as an important part of the remit of my office and as a consequence present at as many courses as possible.

## **Complaints and Inquiries**

The level of complaint about DSD is generally low because its primary business is to collect foreign signals intelligence by technical means. As a logical consequence DSD is unlikely to come into direct contact with members of the Australian public. Notwithstanding this, my office receives a small number of complaints about DSD each year.

Two preliminary inquiries into DSD's activities remained open at the conclusion of 2003–04, both of which were concluded early in 2004–05.

I received complaints from three other persons during 2004–05 which led to preliminary inquiries. These complaints related to security checking.

Three other persons also contacted the office about DSD but their concerns were handled without the need for inquiry action.

A summary of some of the complaints about DSD which this office dealt with during the reporting period is provided below.

### ***Interference with personal communications***

An individual wrote to me indicating that he was actively involved in regional political activities and was concerned that sensitive e-mails he had sent to a named individual on these matters were not being delivered. The complainant suggested this was being done deliberately.

The complainant subsequently provided me with some computer records which he believed substantiated his claims.

An analysis of these records did not indicate a specific or unusually concerted attack on the complainant's computer, but suggested that the problems he had experienced were the common ones internet users face.

On the basis of my inquiries, I concluded that there was no evidence of illegality or impropriety on the part of DSD, or other members of the AIC.

### ***Security checking***

During the reporting period I received two complaints from individuals who had sought employment with DSD but were ultimately unsuccessful despite having strong claims to the positions for which they were interviewed.

In these cases, the individuals concerned were asked to submit to extensive background security checking after a conditional offer of employment was made. DSD operates in a highly secure environment and the majority of staff require high level security clearances in order to perform their duties.

In the cases in question, the complainants had been born and lived overseas for significant periods before migrating to Australia and taking out citizenship. In each instance, the vetting body which conducted the security checking procedure recommended against the granting of a security clearance because it could not satisfactorily verify the applicant's background to the degree required.

There is provision for agencies in this situation to request the vetting agency to waive the requirement to undertake a background check on individuals with an apparently uncheckable background, but this is extremely rare, and will usually only have application to individuals with skills which are either unique or otherwise unavailable within Australia.

This circumstance did not pertain to either complainant, consequently DSD acted in accordance with the recommendation made to it by the vetting agency.

I discussed the underlying cause of these complaints with various individuals within Defence, and suggested that applicants for positions should be given clear guidance on what constitutes a checkable or uncheckable background and the vetting process in general. I also queried when in the process offers of employment (even conditional ones) should or should not be made.

Although I ultimately concluded that DSD had not acted unreasonably, it has subsequently adjusted its recruitment practices so that residency and checkable background issues are adequately addressed before any offers of employment are made.

In the case of one of the complainants, DSD also provided a formal apology for its delay in advising of its decision, which fell short of the standards of service required by the Defence Service Charter.



# Defence Imagery and Geospatial Organisation

## What DIGO Does

DIGO is the lead agency 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 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 Australian Defence Force 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.

Further information about DIGO can be found at the following address, <http://www.defence.gov.au/digo>.

## Brief History

While DIGO is a relatively new organisation, Australia's involvement in imagery intelligence is not. From 1964 until 1998, responsibility for imagery intelligence related matters fell within the purview of DIO and its predecessor bodies.

In the 1990s a strong case was made to the government for the development of an indigenous imagery intelligence capability. These arguments were based on rapid technological advancements, the lowering cost of access to this technology, and the increased contribution Australia could make to various liaison relationships.

The government ultimately accepted these arguments and in 1998 the imagery intelligence function was excised from DIO and transformed

into a new body, the Australian Imagery Organisation (AIO).

Over the next few years, as AIO progressively separated itself from DIO, the alignment between AIO's imagery related activities and the geospatial work of the Defence Topographic Agency came into sharper focus.

Early in 2000, the Department of Defence commissioned an external study which examined and made recommendations on how these important functions might best be structured. The key recommendation flowing from this study was that the AIO, the Defence Topographic Agency, and the Directorate of Strategic Military Geographic Information should be merged into a single body.

The resulting structure, the Defence Imagery and Geospatial Organisation, came into being on 8 November 2000.

## Accountability Arrangements

Prior to DIGO coming into being, it was recognised that the IGIS Act would need to be amended at some point, to fully incorporate DIGO within the remit of the IGIS.

Following discussions between this office and the foundation Director of DIGO, it was agreed that until such time as this occurred, the Inspector-General should oversee the activities of DIGO as if the IGIS Act had already been amended. The government endorsed this approach and this situation pertained throughout the reporting period.

## Flood Review

As mentioned in 'The Year in Review' chapter, Mr Philip Flood conducted a significant inquiry into Australia's intelligence agencies in the later part of

2003–04 and delivered the report of his inquiry to the government in July 2004.

Mr Flood viewed DIGO's rapid development and delivery of a unique range of products during a period of high operational activity in a very positive light, but also identified several issues which he believed required attention so that DIGO could fulfil its potential. To this end, Mr Flood made the following recommendations in respect of DIGO:

*"The functions and ministerial accountabilities of DIGO should be formalised in legislation by amendments to the Intelligence Services Act 2001. Similarly, the Inspector-General of Intelligence and Security Act 1986 should be amended to include scrutiny of DIGO on a basis comparable with that which applies to DSD and ASIS."<sup>16</sup>*

*"The mandate of the Parliamentary Joint Committee on ASIO, ASIS and DSD (PJCAAD) should be extended to all of Australia's intelligence agencies—that is, it should cover also, ONA, DIO and DIGO on the same basis it at presently covers ASIO, ASIS and DSD."<sup>17</sup>*

*"A Foreign Intelligence Coordination Committee (FICC) should be established should under the chairmanship of the Director-General of ONA comprising the heads of ASIO, ASIS, DSD, DIGO and the AFP and Deputy Secretary-level representation from the Departments of the Prime Minister and Cabinet, and Foreign Affairs and Trade."<sup>18</sup>*

*"The Defence Imagery and Geospatial Organisation should develop and implement a comprehensive customer engagement strategy."<sup>19</sup>*

The government accepted these recommendations shortly after receiving Mr Flood's report and DIGO has been working actively to implement them.

## ISLA Bill 2005

The principal vehicle for giving effect to the above recommendations is the ISLA Bill which was introduced into parliament on 16 June 2005.

The incorporation of DIGO into the ISA regime will effect a major change to DIGO's operational environment in that:

- ▶ It will require DIGO to publicly set out its functions (in the same way that the functions of ASIS and DSD are specified in the ISA).
- ▶ DIGO's collection activities will be limited in accordance with the statement of its functions.
- ▶ The Minister for Defence will be required to issue written directions to the Director DIGO in respect of those matters which require a ministerial authorisation.
- ▶ The Minister for Defence rather than the Director DIGO will be required to authorise certain collection activities.
- ▶ The Minister for Defence must make rules regulating the communication and retention by DIGO of intelligence information concerning Australian persons.

I engaged with the Director DIGO during the reporting period on these and related issues, to ensure that the implementation of these proposed changes could occur with the minimum of fuss. I believe that DIGO is positioning itself well to make the transition to the ISA regime, should the ISLA Bill pass through parliament.

## Inspection Activities

I visited DIGO headquarters every three months during the reporting period.

The purpose of these visits was twofold:

- ▶ to meet with the Director DIGO and his senior policy and legal staff, to discuss issues of common interest, and
- ▶ to review those of DIGO's intelligence collection activities that may have had some impact upon Australians or Australian entities.

These meetings with the Director DIGO and his senior staff were extremely useful in gaining a better appreciation of what DIGO does and how it

<sup>16</sup> Flood, p. 180.

<sup>17</sup> *ibid*, p. 180.

<sup>18</sup> *ibid*, p. 181.

<sup>19</sup> *ibid*, p. 184.

goes about its business. While much time has been devoted to discussing the impact upon DIGO of the implementation of Mr Flood's recommendations, the Director has also briefed me on a range of operational and management activities.

The second purpose of our periodic visits to DIGO's headquarters is to actively monitor those tasking requests it receives/actions which might impact upon Australian persons or interests.

The scope for collection of imagery which could intrude upon the privacy of Australians is very limited and occurs subject to the *Rules Governing DIGO's Activities in Respect of Australia and Australians*. These rules embody similar principles to the ASIS and DSD privacy rules but will necessarily need to be reviewed, should the ISLA Bill be passed.

During the reporting period we raised several procedural issues with the Director DIGO in respect of DIGO's existing rules. Each approach received a timely and appropriate response. I was satisfied that all necessary approvals had been obtained in respect of all tasking involving Australian locations and that DIGO's records are being kept in good order.

## **Training**

During the reporting period, OIGIS made three presentations to staff based at DIGO's Canberra headquarters on the role and functions of our office. I also made two presentations to DIGO staff based at the Geospatial Analysis Centre in Bendigo, Victoria.

## **Complaints and Inquiries**

The office received no complaints about DIGO during the reporting period.

# Defence Intelligence Organisation

## What DIO Does

DIO provides all-source intelligence assessments to customers at the national level, to inform defence and government policy and planning, and to support the planning and conduct of Defence Force operations. DIO also aims to develop and maintain a defence intelligence capability for use in time of crisis and conflict.

DIO is an assessment agency rather than an intelligence collection agency. Its assessments focus on the Asia-Pacific region and cover strategic, political, defence, military, economic, scientific and technical issues which have the potential to impact on Australia's security interests.

DIO focuses on overseas developments and does not concern itself with domestic concerns or situations within Australia.

Further information about the role and functions of DIO can be found at, <http://www.defence.gov.au/dio/>.

## Senior Appointment

On 14 December 2004 the Minister for Defence, Senator the Hon. Robert Hill, announced that Major-General Maurie McNarn had been selected as the new Director of the Defence Intelligence Organisation, with effect from 24 January 2005, and that Mr Frank Lewincamp PSM, would take up another senior level appointment within the Defence portfolio.

At the time of his appointment Major-General McNarn was serving as Commander Training Command—Army, having previously been the Australian National Commander—Middle East Area of Operations, in the period leading up to, and during, the war in Iraq.

## Flood Inquiry

The background to the Inquiry into Australian Intelligence Agencies conducted by Mr Philip Flood is described in 'The Year in Review' chapter of this report. Mr Flood delivered his report to the government in early July 2004.

Mr Flood made a significant number of recommendations directly affecting DIO, each of which was accepted by the government. These recommendations included the following:

- ▶ the position of Director DIO should preferably be filled by a suitably qualified high-quality military officer
- ▶ a position of Deputy Director DIO should be created and filled by a suitably qualified high quality civilian when the Director's position is filled by a military officer (and *vice versa* when it is not)
- ▶ the mandate for DIO be revised to focus clearly on supporting defence strategic policy and meeting the strategic assessment needs of the ADF
- ▶ DIO should cease publishing intelligence not directly serving strategic level military-related analysis, and develop products which are more strongly defence-oriented
- ▶ DIO should give greater focus to longer term and strategic assessments.

## Accountability Arrangements

Mr Flood has made two recommendations which are directly related to increasing the external oversight and accountability of DIO, as follows:

- ▶ the mandate of the PJCAAD should be extended to also include ONA, DIO and DIGO, and
- ▶ the mandate of the IGIS should be extended to permit 'own motion' inquiries in respect of ONA and DIO, without ministerial referral.

These recommended changes require amendments to the ISA and the IGIS Act. The vehicle for achieving these amendments is the ISLA Bill, which was introduced into parliament on 16 June 2005.

As discussed elsewhere in this report<sup>20</sup>, Mr Flood specifically recommended that the IGIS should formally review ONA's statutory independence on a periodic basis. Mr Flood, however, was silent as to whether the IGIS should perform a similar function in respect of DIO.

DIO is a subordinate organisation within the Department of Defence, with no separate statutory mandate or direct line of budget funding. Nonetheless, the expectation is that DIO's assessments should also be independent and any suggestion of political or other forms of external pressure to tailor assessments to reach particular conclusions, would be of equal concern.

With this in mind, there will need to be occasions when I review the independence of DIO's assessments, using the own motion powers which Mr Flood recommended should be afforded to my office in respect of DIO. Such review activity could only occur should the ISLA Bill be passed and the necessary amendments to the IGIS Act come about.

## Complaints and Inquiries

In last year's annual report I provided background information on the interaction between this office and a then serving member of the ADF, Lieutenant Colonel Lance Collins, concerning a range of grievances about the Australian intelligence community in general, and DIO in particular.<sup>21</sup>

I included as an annex to that publication, a copy of an unclassified report which had been prepared by my predecessor as Inspector-General, Mr Bill Blick, into those of Lt Col Collins' grievances which fell within the jurisdiction of this office.<sup>22</sup> These matters related to Lt Col Collins' belief that:

- ▶ DIO acted in mid-1998 to quash early warning, included in an assessment prepared by Lt Col Collins, of problems developing in East Timor which would require Australian Defence Force deployment
- ▶ throughout 1999, DIO maintained a line of assessments in relation to East Timor that were relatively soft on Indonesia, reflecting a DIO view that related more to its perception of an Australian policy line than professional assessment of the situation, and
- ▶ in December 1999 DIO, without warning, cut access to a particular intelligence database.

After a conducting a thorough investigation, Mr Blick concluded in respect of each of these points that:

- ▶ what Lt Col Collins interpreted as an attempt to quash contrary views appeared to be legitimate expressions of concern about parts of the content of his assessment and about his wide distribution of assessments and comments
- ▶ DIO assessments during the period in question did not uniformly, or even predominantly, adopt a pro-Jakarta line although there were instances where that interpretation might be available, and
- ▶ to the extent that evidence was available, it supported the view that the loss of access to the database resulted from technical problems rather than a deliberate decision.

Mr Blick completed his report in May 2003, and advised Lt Col Collins in June 2003 that he had referred a copy of his report to the Minister for Defence. In July 2003, the Minister for Defence referred an unclassified version of Mr Blick's report, to Lt Col Collins, and to an individual who was

<sup>20</sup> See chapter on ONA.

<sup>21</sup> IGIS Annual Report 2003–2004, pp. 48–49.

<sup>22</sup> IGIS Annual Report 2003–2004, Annex 3, pp. 89–97.

conducting a redress of grievance investigation for the Army, into matters raised by Lt Col Collins which fell outside of the jurisdiction of this office.

In early April 2004, media reporting revealed that Lt Col Collins had written to the Prime Minister, expressing dismay at a range of alleged intelligence failures, and had called for, "... an impartial, open and wide-ranging Royal Commission into intelligence and the influences upon it."

Very shortly after my appointment as IGIS in late March 2004, I was asked by the then Chief of the Defence Force, to independently review various papers associated with Lt Col Collins' grievances and Mr Blick's report. I did so administratively, rather than in the guise of a formal IGIS Act inquiry.

On 30 April 2004, the Prime Minister publicly released an unclassified version of Mr Blick's report, in response to media enquiries about Lt Col Collins' complaints.

On 3 May 2004, I wrote to Senator the Hon. Robert Hill, Minister for Defence, informing him that my views (on the papers) were consistent with those of my predecessor but suggested that while Mr Blick's investigations into the alleged disconnection of the intelligence database was comprehensive it was not exhaustive, and that it would be desirable to pursue this matter further.

The Minister for Defence agreed with my suggestion and asked me, pursuant to section 8(3)(a) of the IGIS Act, to conduct an inquiry into that matter.

The attention paid to Lt Col Collins' concerns by the media in April 2004, coincided with the research phase of the Inquiry into Australian Intelligence Agencies being conducted by Mr Philip Flood.

Mr Flood sought to meet with Lt Col Collins but reported that Lt Col Collins ultimately declined to be interviewed "because neither the Inquiry, nor the Army, was in a position to agree to his condition that expenses for his senior and junior counsel be met."<sup>23</sup>

The Flood Inquiry nonetheless obtained access to the intelligence estimate which had been prepared by Lt Col Collins in 1998 which he believes was subject to quashing action, and independently

analysed all estimates prepared by DIO and ONA around this time, for any evidence of a pro-Jakarta line or bias.

Mr Flood's analysis of these documents is contained in the Report of his inquiry, which was provided to the government in early July 2004. The more salient of Mr Flood's conclusions were that:

- ▶ while the July 1998 Intelligence Estimate of the situation in East Timor (of which Mr Collins was the principal author) was a significant work of analysis, it discussed matters which were well beyond and outside the scope of an intelligence estimate and this compromised its utility to DIO and the Commander Australian Theatre
- ▶ the Estimate included comments on Australian political developments, including a state election, disparaging comments on policies pursued both by Labor and Coalition Governments, and reference to Wik/native title and greenhouse gases
- ▶ the Estimate did not prove to be a fully accurate prediction of what actually transpired, and
- ▶ the Inquiry found no evidence in any of the DIO and ONA assessments it reviewed of a pro-Jakarta bias.<sup>24</sup>

Mr Flood stated in his report that he did not make a separate investigation into Mr Collins' allegations regarding the disconnection of the intelligence database, as this matter was being separately investigated by this office.

I devoted significant resources during the first half of the reporting period to this inquiry. This involved calling on the services of two officers from the Defence Security Authority with forensic IT expertise, re-interviewing a number of individuals who had previously provided statements or been interviewed by Mr Blick, and interviewing a number of persons with whom Mr Blick had not spoken.

I provided the report of my inquiry to Senator Hill on 30 November 2004. I suggested that Senator Hill seek further advice from the Secretary of the Department of Defence in respect of certain issues.

<sup>23</sup> Flood, p. 47.

<sup>24</sup> *ibid*, pp. 47–50.

Senator Hill issued a press release on 9 December 2004, in which he indicated that he had sought advice from the Secretary to the Department of Defence on matters raised in my report, and that the Secretary was pursuing legal and administrative issues arising from the report. Senator Hill attached a copy of my letter to him of 3 May 2004, to the press release he issued on 9 December 2004. This letter is reproduced at Annex 3 to this report.

At the request of Minister Hill, I prepared an abridged version of my inquiry report which would be suitable for public release (having regard to security and privacy issues). Minister Hill released the abridged version of my report to the public on 25 August 2005. Although it was released outside of the period covered by this report, I have included the report at Annex 4, given its topicality and for ease of reference.

The conclusions I reached were:

- ▶ the denial of access to the intelligence database in December 1999 was deliberate and not the result of technical faults in any part of the system
- ▶ while the evidence did not establish that the then Director DIO directed the cut in access, a person identified as 'Mr A' had instructed another person to effect this outcome, and
- ▶ Mr A may have made statements in 2001 that potentially raised issues of a legal or administrative nature.

I noted that while the denial of access to the particular database for 26 hours did not seem to have been a critical deficiency in operational terms, one can readily understand the sensitivity of those in the field to any change, without consultation, in intelligence access arrangements. It appeared that security concerns were the motivating factor within DIO for the action. The issue of what general responsibility should lie with the then Director of DIO was also canvassed.

In releasing the abridged version of my report, Minister Hill stated that he had drawn certain conclusions from this matter and initiated the following administrative actions to ensure that such a scenario is not repeated in the future:

- ▶ if it was decided to remove access to a database from those in the field, even if the consequences were not significant and the action was justified, the users should have been told and given reasons for the decision
- ▶ furthermore, the fact that Mr Blick in his investigation was left to reach conclusions, which at least one officer knew to be incorrect, was highly unsatisfactory
- ▶ the events called for disciplinary action under the Public Service Act which has now occurred, and
- ▶ in relation to attitudinal differences between the strategic intelligence and tactical intelligence communities, significant reform has since occurred in accordance with the recommendation of the Flood report. This process of reform is ongoing.<sup>25</sup>

<sup>25</sup> Minister for Defence Media Release 136/2005, 25 August 2005.

# Office of National Assessments

## What ONA Does

ONA was created by the passage of the *Office of National Assessments Act 1977* (ONA Act) through parliament in late 1977, and commenced operating in early 1978.

The creation of ONA was prompted by a series of recommendations made by Justice Robert Hope, in the third report of the Royal Commission on Intelligence and Security, which was conducted between 1974 and 1977.<sup>26</sup> Justice Hope found that there was a need for a centrally located assessment function placed in the centre of government but indicated that if the assessments were to have value it was important that the judgements contained within them should be genuinely independent.

This view was accepted by the government of the day and as a consequence, 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, who is an independent statutory office holder.

The ONA Act sets two primary functions for the Office: reporting and assessment on matters of political, strategic and economic significance to Australia; and co-ordination and review of Australia's foreign intelligence activities. ONA produces three principal outputs: printed product, which is its major output, oral briefing for Ministers and officials, and intelligence co-ordination and review, which includes policy co-ordination, requirement setting and performance evaluation.

Further information about ONA can be found at, <http://www.ona.gov.au>.

## Significant Issues

### Flood Review

ONA, like DIO, was subjected to a more thorough review and analysis by Mr Flood than any of the other AIC agencies. The reason for this close attention was that both are assessment agencies, and the Flood Review was born out of a concern that the assessments of each agency in the period prior to the commencement of hostilities by coalition forces in Iraq in March 2003, may not have been sufficiently independent or robust.

In addition to his review of the assessment work of ONA, Mr Flood also recognised and commented upon the central role that ONA plays in coordinating the activities of Australia's foreign intelligence agencies.

Although Mr Flood commented favourably on ONA in some respects and commended its record of achievement, he strongly argued that if ONA were to achieve the objectives envisaged by Justice Hope and set for it by government, it should be supported by a stronger legislative mandate and a significant increase in its budget.

Mr Flood made a large number of recommendations either directly or indirectly pertaining to ONA. Each of these recommendations was accepted by the government, with the single exception that ONA be retitled the Australian Foreign Intelligence Assessments Agency. As a consequence, ONA has been more greatly affected by the implementation of Mr Flood's recommendations than any of the other AIC agencies.

26 RM Hope, Royal Commission on Intelligence and Security, Third Report, Australian Government Publishing Service, Canberra 1977.

Perhaps the most significant of the recommendations made by Mr Flood, at least in terms of everyday practicalities, was that ONA's budget and staffing should be effectively doubled in size (from \$13.1 million per annum and 74 staff, to \$25 million per annum and 145 staff).

Other important recommendations affecting ONA which were either implemented during the reporting period, or set in train, included:

- ▶ the creation of a Foreign Intelligence Coordination Committee under the chairmanship of the Director-General of ONA
- ▶ amending the ONA Act to strengthen its intelligence community coordination role, and to more accurately reflect the focus and work of the National Assessments Board
- ▶ ONA giving greater focus to longer term and strategic assessments, and institutionalising measures to ensure that assessments are the product of rigorous testing, challenge and peer review, both within and outside the agency
- ▶ the Department of Foreign Affairs and Trade's (DFAT's) Open Source Unit being transferred to ONA, and
- ▶ funding in the order of \$11 million being provided for physical accommodation, to enable an expanding ONA and ASIO to continue to be collocated.

Three of Mr Flood's recommendations related directly to increasing the external oversight and accountability of ONA, as follows:

- ▶ the mandate of the PJCAAD should be extended to also include ONA, DIO and DIGO
- ▶ the mandate of the IGIS should be extended to permit 'own motion' inquiries in respect of ONA and DIO, without ministerial referral, and
- ▶ the IGIS should conduct a periodic review of ONA's statutory independence.

### **Flood implementation**

The government announced on 22 July 2004 that it had endorsed all of Mr Flood's recommendations, with the exception of the proposed retitling of ONA.

Subsequent to this announcement, the Director-General of ONA moved quickly to give effect to each of Mr Flood's recommendations which did not require statutory amendments.

The Foreign Intelligence Coordination Committee proposed by Mr Flood was established very shortly after the government announced its endorsement of Mr Flood's recommendations. The rapid creation of the FICC was assisted by the fact that it was similar in structure to an existing, albeit less formal forum, namely the Heads of Intelligence Agencies Meetings.

After a brief period of reflection on how it should be structured internally, ONA has recruited a significant number of new analysts and supported these recruits with appropriate training and resources. While it will take some time for these recruits to develop the full range of skills necessary to meet the expectations of government, a solid foundation has been laid in a short period of time.

After detailed negotiations with DFAT and the Australian Public Service Commission regarding personnel and funding issues, the Open Source Unit successfully transferred to ONA's direct control on 1 April 2005.

### **ISLA Bill**

The vehicle for effecting the various statutory amendments proposed by the Flood Review is the ISLA Bill which was introduced into parliament on 16 June 2005.

As discussed elsewhere in this report, the ISLA Bill is the product of the Flood Review recommendations, and recommendations flowing from a DPMC review of the ISA.

At the conclusion of the reporting period, the PJCAAD had, upon a motion of the Senate, initiated a review of the ISLA Bill with a view to reporting its findings in the spring sittings of parliament.

### **Review Activities**

One of the more significant recommendations made by Mr Flood, at least in terms of accountability arrangements, was that the IGIS should conduct periodic reviews of ONA's statutory independence.

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.”<sup>27</sup>*

It is proposed that this recommendation be given effect by amending section 8(3) of the IGIS Act by inserting a new sub-paragraph (c), which will empower the IGIS either at the request of the Prime Minister, or on his own motion, “to inquire into any matter in relation to the statutory independence of ONA.”

Absent legislative coverage, I did not conduct any processes during the reporting period to formally review ONA’s statutory independence but I did engage in some preliminary discussions with the Director-General on the form this review activity might take in the future.

I have also been provided with access to, and regularly read, various ONA product lines, so that I might position myself to conduct this review activity, should the proposed amendments to the IGIS Act occur.

## Training

Given that my office is likely to have a greater interaction with ONA than has previously been the case, I provided a comprehensive briefing to interested ONA staff on the role and functions of my office, and the likely impact of the changes proposed in the Flood Review. This presentation was well attended.

I also present to the AIC common induction course, to which ONA staff are regularly allocated places.

## Complaints and Inquiries

The IGIS Act, as it is presently structured, does not allow for the IGIS to pursue (at least in a direct way) complaints about ONA’s activities.

As indicated earlier, Mr Flood has proposed that the IGIS Act be amended to permit the IGIS to conduct inquiries, on his own motion, should he choose to do so. Although such a change would not permit the IGIS to deal directly with complaints, if a complainant were to raise serious issues of concern, it is likely that these would be addressed in the form of an own motion inquiry.

During the reporting period an individual contacted my office with some concerns about the transfer of the Open Source Unit function from DFAT to ONA. These concerns related to background security checking processes.

I initiated a preliminary inquiry to determine the limits on my jurisdiction. Upon being satisfied that I could not formally pursue the matter any further in the form of a formal inquiry, I then took an administrative interest in ensuring that the interests of the individual concerned, and some of that person’s colleagues, were fully appreciated. To this end, I engaged in dialogue with relevant officers in ONA, DFAT and the Australian Public Service Commission and then maintained a watching brief.

I am pleased that an acceptable outcome was achieved for the individual who contacted my office, and that the Open Source Unit successfully transferred to ONA’s control without further concerns being raised with my office.

<sup>27</sup> Flood, p. 105.



internal and external scrutiny and are accountable for their conduct.

### **DSD**

Each DSD submission to the Minister for Defence seeking a ministerial authorisation under the ISA will be reviewed.

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, and policy issues affecting compliance, as they arise. 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.

### **DIGO**

My staff and I intend to assist DIGO's incorporation into the ISA framework in whatever way we appropriately can.

Should the ISLA Bill 2005 be passed, we will review all ministerial authorisations which are sought by DIGO, for compliance with the requirements of the ISA.

We plan to assist DIGO in the development and implementation of new privacy rules, to replace the existing *Rules Governing DIGO's Activities in respect of Australia and Australians*, consistent with the requirements of the ISA.

All tasking requests which are levied on or by DIGO in respect of Australian territory or Australian interests, will be reviewed.

The frequency of our scheduled visits to DIGO Headquarters will increase from quarterly to at least bi-monthly, in respect of the above activities, and to discuss matters of common interest with relevant DIGO senior managers.

### **ONA**

We will assist ONA in the development of privacy rules, with a view to ensuring that the rules are consistent with those in use elsewhere in the AIC.

Subject to the ISLA Bill being passed, I will periodically review ONA's statutory independence.

### **DIO**

We will assist DIO in the development of privacy rules, with a view to ensuring that the rules are consistent with those in use elsewhere in the AIC.

Subject to the ISLA Bill being passed, activities consistent with the objective of testing the independence of DIO's assessments will be conducted.

### **Inquiries and Complaints**

Five inquiries under the IGIS Act were in progress at the close of the reporting year. I expect to conclude investigations into each of these cases during the first half of the new reporting year.

It is not possible to predict future inquiry workload but there is no reason to expect any significant departure from previous years' patterns.

### **Legislative Review**

Section 4(3)(b) of the *Security Legislation Amendment (Terrorism) Act 2002* (SLAT Act) requires the establishment of a committee, which includes the Inspector-General as an ex-officio member, to review the operation, effectiveness and implications of amendments made by the SLAT Act.

The proposed Counter-Terrorism Legislative Review Committee was still to be established at the end of the 2004–05 but will be active in 2005–06.

# Corporate and communications

## Support from DPMC and DSD

As a very small agency, the office relies on the assistance of the Department of the Prime Minister and Cabinet (DPMC) in handling staff and other administration issues and in providing general support. This support is provided on the basis that we are a portfolio agency and collocated with DPMC. The arrangement works well and I am grateful to DPMC for its continued support.

The other major provider of support is DSD which maintains the internal secure computer network systems within the office. I would like to record my thanks for DSD's continued assistance.

## Outcome and Outputs

The OIGIS outcome and outputs are an integral part of the accrual budgetary structure and are outlined in detail in the current portfolio budget statements.

OIGIS is committed to the endorsed outcome of providing assurance that Australia's intelligence agencies act legally, ethically and with propriety.

In the reporting period 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.

As part of the 2005–06 Budget process, these outputs were combined into the following output:

- ▶ Inspect, inquire into, and report on, the activities of the intelligence and security agencies.

The decision to change the output structure (made during the reporting period) was 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.
- ▶ 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 duties performed under the two former outputs, including complaints resolution.

## Corporate Governance

The office has an Audit Committee chaired by myself and which also includes an external member from DPMC. The Committee considers corporate governance issues such as internal and external audit findings, fraud and risk management, occupational health and safety, and significant financial issues.

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.

## 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. There were no cases of suspected fraud in the reporting period.

## Staffing and Resources

There were no changes to the staffing composition of the office during the reporting period. The salary ranges are aligned with those under the DPMC certified agreement.

## Composition of the Office

During the reporting year positions were filled as follows:

- ▶ Inspector-General of Intelligence and Security  
— Mr Ian Carnell
- ▶ Principal Investigation Officer  
— Mr Neville Bryan
- ▶ Senior Investigation Officer  
— Ms Jane Trevor
- ▶ Personal Assistant to the Inspector-General  
— Ms Jodie Williams
- ▶ Office Manager and Monitoring Officer  
— Ms Robyn Kelly

A participant on the Senior Women in Management Programme was placed in OIGIS from 13 October to 10 December 2004. My office is grateful for the additional resources that were made available through the SWIM Programme and to the officer for the contribution she made.

## 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 which characterise 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 and regard to human rights. 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*.

Given the small size of the Office, OIGIS has adopted DPMC's current Disability Action Plan. This plan was revised in 2004–05 and is to be implemented in 2005–06. The revised plan will build on and endorse the commitment to the principles of workplace diversity and equality of access.

## Occupational Health and Safety

OIGIS is covered by the DPMC Occupational Health and Safety Plan. During the reporting period the office was included in DPMC's individual workspace and workplace audit. A number of recommendations were made.

All of the workspace recommendations have been implemented and all but one of the recommendations made during the workplace audit have been implemented. This issue is receiving ongoing attention.

There were no incidents reported to Comcare Australia under the reporting requirements of section 68 of the *Occupational Health and Safety (Commonwealth Employment) Act 1991*.

Through DPMC, members of the office are able to participate in health week, the influenza vaccination programme and exercise classes.

## Management of Human Resources

The small size of the office necessitates that all staff are exposed to a wide variety of work and developmental activities. Staff attend relevant courses and information sessions as necessary.

## Purchasing

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

## Consultancy Services

During 2004–05, two new consultancy contracts were entered into at a combined cost of \$9 038. The contracts were also completed and payment made within this reporting period. Of these consultants, one was engaged to assist with an inquiry and the other to provide scribe services in a recruitment process. The selection method used in both cases was direct sourcing with the consultants selected on the basis of experience, independence and in the former instance, specialist expertise in conducting similar inquiries.

Comparable consultancy expenditure for recent financial years was \$24 900 in 2003–04 and \$3 300 in 2002–03. In 2004–05 an adjustment totalling \$690 was made in respect of consultancy work performed in 2002–03 and 2003–04.

This report does not include a separate consultancy services table as the office did not engage individual consultants to the value of \$10 000 or more during 2004–05.

There were no ongoing consultancy contracts which operated from 2003–04 into 2004–05. Nor are there any ongoing consulting contracts at the end of this reporting period.

## Contract Services

Nexis Accountants was engaged to provide financial services in 2004–05 at a total value of \$20 460. These services included the production of monthly and annual financial statements on actuals and bi-annual financial estimates. In prior years the contracted financial services were reported under consultancy services. However, for the purposes of annual reporting the nature of these services do not meet the definition of consultancy services. In 2003–04 accountancy services were purchased to the value of \$25 300 and in 2002–03 \$11 000.

Legal advice is obtained from the Australian Government Solicitor (AGS) as required. Under the Legal Services Directions national security related legal work is tied to the AGS. In 2004–05 OIGIS paid for three separate AGS legal advices at a combined cost of \$6 689.

## Competitive Tendering and Contracting

The office is not involved in competitive tendering and contracting (CTC). CTC activity relates only to the contracting out of the delivery of government activities previously performed by a government agency, to another organisation.

## Energy Saving Measures

The office through its collocation with DPMC continues to benefit from the department's commitment to energy saving measures.

The office uses an 80–20 (80 per cent recycled–20 per cent new/virgin paper) for photocopying, facsimile report and document printing. The office purchases writing pads made from recycled paper. The toner cartridges from the unclassified facsimile are recycled. Through DPMC the office is able to access unclassified waste paper recycling services.

## 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, with propriety, and with regard to human rights. Respect for these fundamental principles fosters an awareness and appreciation of social justice issues.

The office website and brochure are the main vehicles for promoting the existence and role of my office. The website is being modernised to allow future in-house maintenance of the site enabling the office to keep the site more up to date and responsive to the needs of the public. In the short term my goal has been to ensure that the website and information brochure are easily accessible and available in plain English. Over the longer term my aim is to have the brochure and the relevant section of the website available in selected other languages.

I have met with some leaders and representatives of the Islamic community to explain the role of my office. In recognition of the need for a greater understanding of the Islamic community, members of my staff have attended introductory courses on Islam.

## 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](mailto: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](mailto:hotline@nationalsecurity.gov.au).

The office also frequently 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 other 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 several subjects in which the Inspector-General 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, the practice has been not to discuss the particulars of that inquiry beyond process issues and the formal requirements of the IGIS Act.

## International Liaison

I attended the fourth biennial conference of international intelligence oversight bodies in Washington DC in October 2004. The next such conference is likely to be in South Africa in 2006.

## 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

I met with the PJCAAD on 10 May 2005 to provide a general overview of my office's activities. I appeared before the PJCAAD on 20 May 2005 in relation to the review of ASIO's questioning and detention powers and on 16 June 2005 in relation to the ISLA Bill.

I appeared before the Senate Finance and Public Administration Legislation Committee on 14 February 2005 and 23 May 2005.

The office has again received an unqualified audit report from the ANAO in relation to its financial statements.

In its Review of administration and expenditure for ASIO, ASIS, DSD, No 3 March 2005, the PJCAAD recommended that consideration be given to the development of an MOU between the Commonwealth Ombudsman and the IGIS governing possible joint reviews of combined ASIO/police operations. As indicated earlier in this report, the Ombudsman and I have agreed to develop an MOU between our offices.

## Summary of the Office's Financial Performance

The office has recorded a small operating profit of \$31 517 in 2004–05.

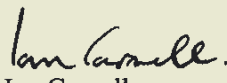
For the first time since 2001–02, the office has a positive equity position (\$408 582 in 2004–05). This position was largely achieved through:

- ▶ an equity injection of \$200 000 received in the 2004–05 Budget which has allowed the office to provide for previously unfunded leave liabilities, and
- ▶ an equity injection of \$202 000 received in the 2004–05 Additional Estimates to enhance the computer and communication networks within the office.

# Financial statements

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

In my opinion, the attached financial statements for the year ended 30 June 2005 are based on properly maintained financial records (except for the matter noted in Note 5) 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

29 September 2005

**OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY**  
**STATEMENT OF FINANCIAL PERFORMANCE**  
*for the year ended 30 June 2005*

	Notes	2004-05 \$	2003-04 \$
<b>Revenues from ordinary activities</b>			
Revenues from Government	5	931 000	741 000
Resources received free of charge	1.3	72 735	150 067
Revenue from sale of assets		700	-
<b><i>Total revenues from ordinary activities</i></b>		<b><u>1 004 435</u></b>	<b><u>891 067</u></b>
<b>Expenses from ordinary activities</b>			
Employees	1.4		
Remuneration		599 890	549 903
Superannuation		122 684	114 407
Comcare premium		2 145	1 360
Total employees		<u>724 719</u>	<u>665 670</u>
Suppliers			
Resources received free of charge	1.3	72 735	94 091
Other goods and services		147 076	140 894
Total suppliers		<u>219 811</u>	<u>234 985</u>
Assets written-off		1 587	-
Value of assets sold		68	-
Equipment depreciation		26 733	16 173
<b><i>Total expenses from ordinary activities</i></b>		<b><u>972 918</u></b>	<b><u>916 828</u></b>
<b>Net surplus /(deficit) from ordinary activities</b>		<b><u>31 517</u></b>	<b><u>(25 761)</u></b>
<b>Net credit to asset revaluation reserve</b>	3	-	9 435
<b>Total changes in equity other than those resulting from transactions with the Australian Government as owner</b>		<b><u>31 517</u></b>	<b><u>(16 326)</u></b>

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

**OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY**  
**STATEMENT OF FINANCIAL POSITION**  
*as at 30 June 2005*

	Notes	2004-05 \$	2003-04 \$
<b>ASSETS</b>			
<b>Financial Assets</b>			
Cash (notes, coins and deposits at bank)	4	412 460	247 754
Receivables	1.5		
Amounts held in the Official Public Account		308 000	-
Leave liability transfers		-	20 048
Fringe Benefits Tax refund		-	5 799
GST receivable		3 590	3 645
Other debtors		489	-
Total receivables		312 079	29 492
<b>Total financial assets</b>		<b>724 539</b>	<b>277 246</b>
<b>Non-financial assets</b>			
Plant and equipment	1.8		
Equipment (at cost)		140 660	77 229
Less: accumulated depreciation		(36 264)	(16 173)
At 2004 valuation (fair value)	6	7 235	9 435
Less: accumulated depreciation		(2 750)	-
Total plant and equipment		108 881	70 491
<b>Total non-financial assets</b>		<b>108 881</b>	<b>70 491</b>
<b>Total assets</b>		<b>833 420</b>	<b>347 737</b>
<b>LIABILITIES</b>			
<b>Provisions – employees</b>			
<b>Employee current liabilities</b>			
Salaries and wages	1.4	1 966	-
Annual leave		39 608	37 686
Superannuation		33 646	22 106
Total employee current liabilities		75 220	59 792
<b>Employee non current liabilities</b>			
Annual leave	1.4	72 181	61 700
Long service leave		259 983	228 678
Total employee non current liabilities		332 164	290 378
<b>Total provisions – employees</b>		<b>407 384</b>	<b>350 170</b>
<b>Payables</b>			
Payables - trade creditors (current)	1.5	17 454	4 597
Other payables (current)	1.5	-	17 906
<b>Total payables</b>		<b>17 454</b>	<b>22 503</b>
<b>Total liabilities</b>		<b>424 838</b>	<b>372 673</b>
<b>Net Assets</b>		<b>408 582</b>	<b>(24 936)</b>
<b>EQUITY</b>			
Asset revaluation reserve	3	9 435	9 435
Contributed equity		468 000	66 000
Accumulated results		(68 853)	(100 371)
<b>Total equity</b>		<b>408 582</b>	<b>(24 936)</b>

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 2005*

	Notes	2004-05 \$	2003-04 \$
<b>OPERATING ACTIVITIES</b>			
<b>Cash received</b>			
Appropriations		931 000	741 000
Net GST refunds		20 222	9 085
<b>Total cash received</b>		<u>951 222</u>	<u>750 085</u>
<b>Cash used</b>			
Employees		(667 506)	(654 055)
Suppliers		(146 931)	(148 454)
Cash transferred to Official Public Account		(308 000)	-
<b>Total cash used</b>		<u>(1 122 437)</u>	<u>(802 509)</u>
<b>Net cash from operating activities</b>	<b>4</b>	<u>(171 216)</u>	<u>(52 424)</u>
<b>INVESTING ACTIVITIES</b>			
<b>Cash received</b>			
Proceeds from sales of equipment		700	-
<b>Total cash received</b>		<u>700</u>	<u>-</u>
<b>Cash used</b>			
Purchase of property, plant and equipment		(66 778)	-
<b>Total cash used</b>		<u>(66 778)</u>	<u>-</u>
<b>Net cash from investing activities</b>		<u>(66 078)</u>	<u>-</u>
<b>FINANCING ACTIVITIES</b>			
<b>Cash received</b>			
Equity injection		402 000	-
<b>Total cash received</b>		<u>402 000</u>	<u>-</u>
<b>Net cash from financing activities</b>		<u>402 000</u>	<u>-</u>
<b>Net increase/(decrease) in cash held</b>		164 706	(52 424)
Cash at beginning of reporting period		247 754	300 178
<b>Cash at the end of the reporting period</b>	<b>4</b>	<u>412 460</u>	<u>247 754</u>

**STATEMENT OF COMMITMENTS AND CONTINGENCIES**

*As at 30 June 2005*

The office had no contingencies to report in either 2003-04 or in 2004-05.

The office had at the end of year an operating leasing commitment totalling \$8 199 (2003-04: \$8 199) for the provision of a motor vehicle to the Inspector-General. There are no renewal or purchase options available to the office and this lease matures within one year. No contingent rentals exist.

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

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS**  
*for the year ended 30 June 2005*

**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 is structured to meet two outputs:

Output 1: Inspect and report on the activities of the intelligence and security agencies (60% of resources), and  
 Output 2: Conduct inquiries and provide a complaint resolution service (40% of resources).

**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 Orders (or FMO's, being the *Financial Management and Accountability (Financial Statements for reporting periods ending on or after 30 June 2005)*) Australian Accounting Standards and Accounting Interpretations issued by the Australian Accounting Standards Board, and
- Consensus views of the Urgent Issues Group.

The Statements of Financial Performance and Financial Position have been prepared on an accrual basis and are in accordance with the historical cost convention. No allowance is made for the effect of changing prices on the results or the financial position.

Assets and liabilities are recognised in the Statement of Financial Position 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.

Revenues and expenses are recognised in the Statement of Financial Performance when and only when the flow or consumption or loss of economic benefits has occurred and 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 Statement of Financial Performance when and only when the flow or consumption or loss of economic benefits has occurred and can be reliably measured.

**1.3 Revenue**

*Revenues from Government*

The full amount of the departmental appropriation for office outputs for the year is recognised as revenue.

*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.

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS**  
*for the year ended 30 June 2005*

**Note 1 - Summary of Significant Accounting Policies (continued)**

**1.3 Revenue (continued)**

The main resources received free of charge in 2004-05 are office space (from the Department of Prime Minister and Cabinet) and the installation and maintenance of the OIGIS owned internal secure computer networks (from Defence Signals Directorate). In prior years DSD also provided the internal secure computer network free of charge. Other resources received free of charge include auditor remuneration as disclosed in Note 9.

**1.4 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 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.

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.

*Superannuation*

Staff of the Office of the Inspector General of Intelligence and Security are members of the Commonwealth Superannuation Scheme and the Public Sector Superannuation Scheme. The liability for their superannuation benefits is recognised in the financial statements of the Australian Government and is settled by the Australian Government in due course.

The Office of the Inspector General of Intelligence and Security makes employer contributions to the Australian Government at rates determined by an actuary to be sufficient to meet the cost to the Government of the superannuation entitlements of the office's employees.

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

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS**  
*for the year ended 30 June 2005*

**Note 1 - Summary of Significant Accounting Policies (continued)**

**1.5 Other Financial instruments**

*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 (2003–04: 30 days).

*Trade Creditors*

Trade creditors and accruals are recognised at their nominal amounts, being the amounts at which the liabilities will be settled. Liabilities are recognised to the extent that the goods or services have been received (and irrespective of having been invoiced).

All creditors are entities that are not part of the Commonwealth legal entity. Settlement is usually made net 30 days.

**1.6 Cash**

Cash means notes and coins held and any deposits held at call with a bank or financial institution. Cash is recognised at its nominal amount.

**1.7 Acquisition of Assets**

Assets are recorded at cost on acquisition.

**1.8 Plant and Equipment**

The office's fixed assets comprise of office equipment only.

*Asset Recognition Threshold*

Purchases of equipment are recognised at cost in the Statement of Financial Position, except for purchases costing less than \$2 000, which are expensed in the year of acquisition (other than where they form part of a group of similar items which are significant in total).

*Revaluations*

Plant and equipment are carried at valuation. Fair values for the one class of asset have been determined by market selling price.

Assets were recognised at fair value for the first time in 2003-04 (previously the deprival value was used).

Asset Class	Increment/ (decrement) to asset class	Contra Account
Plant and equipment	2004: \$9 435	Asset Revaluation Reserve

The total financial effect of the changed policy in 2003-04 was to increase the carrying amount of plant and equipment by \$9 435 and increase the asset revaluation reserve by \$9 435.

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS**  
*for the year ended 30 June 2005*

**Note 1 - Summary of Significant Accounting Policies (continued)**

**1.8 Plant and Equipment (continued)**

*Frequency and Conduct*

2003-04 was the first year equipment has been revalued. The valuation was conducted by an independent qualified valuer.

The Finance Minister's Orders require that all property plant and equipment assets be measured at up-to-date fair values from 30 June 2005 onwards.

*Depreciation and Amortisation*

Depreciable 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 for a change in prices only when assets are revalued.

Depreciation and amortisation rates are for 1 to 5 years for each class of depreciable assets.

**1.9 Impairment of Non-Current Assets**

Non-current assets carried at up to date fair value at the reporting date are not subject to impairment testing.

The non-current assets carried at cost, which are not held to generate net cash inflows, have been assessed for indications of impairment. The office reviewed these assets in relation to the proposed move to new premises in 2007. The result of this review was that it had no financial impact on the carrying value of these assets as they will be depreciated to nil. (If indications of impairment did exist, assets would be written down to the higher of the net selling price and, if the entity would replace the asset's service potential, its depreciated replacement cost).

**1.10 Transactions by the Government as Owner**

*Equity Injections*

Amounts appropriated as 'equity injections' for a year (less any savings offered up in Portfolio Additional Estimates Statements) are recognised directly in contributed equity in that year.

This is a change of accounting policy from 2002-03 to the extent any part of an equity injection that was dependent on specific future events occurring was not recognised until the appropriation was drawn down.

The change in policy has no financial effect in 2004-05 because the full amounts of the equity injections were recognised in the year received.

**1.11 Taxation**

The office is exempt from all forms of taxation except fringe benefits tax (FBT) and the 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.

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS**  
*for the year ended 30 June 2005*

**Note 1 - Summary of Significant Accounting Policies (continued)**

**1.12 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 Australia.

**1.13 Comparative Figures**

Comparative figures have been adjusted to conform to changes in presentation in these financial statements where required.

**1.14 Rounding**

Amounts have been rounded to the nearest dollar.

**Note 2 - Adoption of AASB Equivalents to International Financial Reporting Standards from 2005-06**

The Australian Accounting Standards Board has issued replacement Australian Accounting Standards to apply from 2005-06. The new standards are the Australian Equivalents to International Financial Reporting Standards (AEIFRS). The International Financial Reporting Standards are issued by the International Accounting Standards Board. The new standards cannot be adopted early. The standards being replaced are to be withdrawn with effect from 2005-06, but continue to apply in the meantime, including reporting periods ending on 30 June 2005.

The purpose of issuing AEIFRS is to enable Australian reporting entities reporting under the *Corporations Act 2001* to be able to more readily access overseas capital markets by preparing their financial reports according to accounting standards more widely used overseas.

AEIFRS contain certain additional provisions that will apply to not-for-profit entities, including Australian Government agencies. Some of these provisions are in conflict with IFRS, and therefore the Office of the Inspector-General of Intelligence and Security will only assert that the financial report has been prepared in accordance with Australian Accounting Standards.

AAS 29 *Financial Reporting by Government Departments* will continue to apply under AEIFRS.

Accounting Standard AASB 1047 *Disclosing the Impacts of Adopting Australian Equivalents to International Financial Reporting Standards* requires that the financial statements for 2004-05 disclose:

- an explanation of how the transition to AEIFRS is being managed
- narrative explanations of the key policy differences arising from the adoption of AEIFRS
- any known or reliably estimable information about the impacts on the financial report had it been prepared using AEIFRS, and
- if the impacts of the above are not known or reliably estimable, a statement to that effect.

The purpose of this Note is to make these disclosures.

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS**  
*for the year ended 30 June 2005*

**Note 2 - Adoption of AASB Equivalents to International Financial Reporting Standards from 2005-06 (cont)**

*Management of the transition to AEIFRS*

The Office of the Inspector-General of Intelligence and Security has taken the following steps for the preparation towards the implementation of AEIFRS:

- The office's finance personnel are tasked with oversight of the transition to and implementation of AEIFRS.
- All major accounting policy differences between current AASB standards and AEIFRS were identified by 30 June 2004.
- A transitional balance sheet as at 1 July 2004 under AEIFRS was completed.
- An AEIFRS compliant Statement of Financial Position as at 30 June 2005 was also prepared during the preparation of the 2004-05 statutory financial reports.
- The 2004-05 Statement of Financial Position under AEIFRS will be reported to the Department of Finance and Administration in line with reporting deadlines.
- The plan also addresses the risks to successful achievement of the above objectives and includes strategies to keep implementation on track to meet deadlines.
- Consultants were engaged where necessary to assist with each of the above steps.

*Major changes in accounting policy*

The office believes that the first financial report prepared under AEIFRS ie at 30 June 2006, will be prepared on the basis that the Office of the Inspector-General of Intelligence and Security will be a first time adopter under AASB 1 *First-time Adoption of Australian Equivalents to International Financial Reporting Standards*. Changes in accounting policies under AEIFRS are applied retrospectively (as if the new policy had always applied except in relation to the exemptions available and prohibitions under AASB 1). To enable the 2005-06 financial statements to report comparatives under AEIFRS an AEIFRS compliant Statement of Financial Position will need to be prepared as at 1 July 2004. When developing the accounting policies applicable to the preparation of the 1 July opening Statement of Financial Position, the office elected not to use the exemptions available to it as a first time adopter of AEIFRS.

Changes to major accounting policies are discussed in the following paragraphs.

Management's review of the quantitative impacts of AEIFRS represents the best estimates of the impacts of the changes at the reporting date. The actual effects of the impacts of AEIFRS may differ from these estimates due to:

- continuing review of the impacts of AEIFRS on the operations of the office
- potential amendments to the AEIFRS and AEIFRS Interpretations, and
- emerging interpretation as to the accepted practice in the application of AEIFRS and AEIFRS Interpretations.

*Property, plant and equipment*

It is expected that the 2005-06 *Finance Minister's Orders* will continue to require property, plant and equipment assets to be valued at fair value in 2005-06. The quantitative impact of AEIFRS on these assets for the Office of the Inspector-General of Intelligence and Security was assessed to be nil.

*Impairment of assets*

The offices' policy on impairment of non-current assets is at Note 1.9.

Under AEIFRS assets will be subject to assessment for impairment and, if there are indications of impairment, an assessment of the degree of impairment. (Impairment measurement must also be done, irrespective of any indications of impairment, for intangible assets not yet available for use. The office has no intangible assets). The impairment test is that the carrying amount of an asset must not exceed the greater of (a) its fair value less costs to sell and (b) its value in use. 'Value in use' is the net present value of net cash inflows for cash generating units or depreciated replacement cost for other assets which would be replaced if the office was deprived of them.

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS**  
*for the year ended 30 June 2005*

**Note 2 Adoption of AASB Equivalents to International Financial Reporting Standards from 2005-06 (cont)**

*Impairment of assets (continued)*

An impairment assessment of the office's assets indicated that no adjustment will be required.

*Employee Benefits*

The provision for long service leave is measured at the present value of estimated future cash outflows using market yields as at the reporting date on national government bonds. As noted in the 2003-04 Financial Report, the same discount rate will be used under AEIFRS.

AEIFRS also require annual leave that is not expected to be taken within 12 months of balance date be discounted. After assessing the staff leave profile, the office does not expect that any material amounts of the annual leave balance will be taken in the next 12 months. Consequently, there has been an adjustment for non-current annual leave. The adjustment resulted in a decrease to the non current portion of annual leave.

*Financial Instruments*

AEIFRS include an option for entities not to restate comparative information in respect of financial instruments in the first AEIFRS report. Therefore, the amounts for financial instruments presented in the office's 2004-05 primary financial statements are not expected to change as a result of the adoption of AEIFRS.

The Office of the Inspector-General of Intelligence and Security will be required under AEFIRS to review the carrying amounts of financial instruments at 1 July 2005 to ensure they align with the accounting policies required by AEIFRS. It is expected that the carrying amounts of financial instruments held by the office will not materially change as a result of this process.

The office has assessed there will be no material impact on the financial report had it been prepared using AEIFRS.

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS**  
*for the year ended 30 June 2005*

**Note 2 - Adoption of AASB Equivalents to International Financial Reporting Standards from 2005-06 (cont)**

*Reconciliation of Impacts – Australian Generally Accepted Accounting Principles to AEIFRS*

	2004-05	2003-04
	\$	\$
<b>Reconciliation of Departmental Equity</b>		
Total Departmental Equity under AGAAP	408 582	(24 936)
Adjustments to accumulated results	4 354	4 535
Adjustments to other reserves	-	-
<b>Total Equity under AEIFRS</b>	<u>412 936</u>	<u>(20 401)</u>
<b>Reconciliation of Departmental Accumulated Results</b>		
Total Departmental Accumulated Results under AGAAP	(68 854)	(100 371)
Adjustments:		
Employee provisions	4 354	4 535
<b>Total Accumulated Results under AEIFRS</b>	<u>(64 500)</u>	<u>(95 836)</u>
<b>Reconciliation of Departmental Reserves</b>		
Total Departmental Reserves under AGAAP	9 435	9 435
Adjustment:		
Asset Revaluation Reserve	-	-
<b>Total Departmental Reserves under AEIFRS</b>	<u>9 435</u>	<u>9 435</u>
<b>Reconciliation of Departmental Contributed Equity</b>		
Total Departmental Contributed Equity under AGAAP	468 000	66 000
Adjustments	-	-
<b>Total Contributed Equity under AEIFRS</b>	<u>468 000</u>	<u>66 000</u>
<b>Reconciliation of Net surplus /(deficit) from ordinary activities for the year ending 30 June 2005<sup>1</sup></b>		
Total Operating surplus / (deficit) under AGAAP	31 517	-
Adjustments:		
Employee Provisions	(181)	-
	<u>31 336</u>	<u>-</u>

1. The 30 June 2005 total represents the accumulated impacts of AEIFRS from the date of transition.

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS**  
for the year ended 30 June 2005

**Note 3 - Equity**

Item	Contributed Equity		Asset Revaluation Reserve		Accumulated Results		TOTAL EQUITY	
	2004-05 \$	2003-04 \$	2004-05 \$	2003-04 \$	2004-05 \$	2003-04 \$	2004-05 \$	2003-04 \$
Balance 1 July	66 000	66 000	9 435	-	(100 371)	(74 610)	(24 936)	(8 610)
Net revaluation increment/(decrement)	-	-	-	9 435	-	-	-	9 435
Equity injection	402 000	-	-	-	-	-	402 000	-
Operating result	-	-	-	-	31 517	(25 761)	31 517	(25 761)
Balance 30 June	468 000	66 000	9 435	9 435	(68 854)	(100 371)	408 581	(24 936)
Total equity attributable to the Commonwealth	468 000	66 000	9 435	9 435	(68 854)	(100 371)	408 581	(24 936)

**Note 4 - Cash Flow Reconciliation**

	2004-05 \$	2003-04 \$
<b>Reconciliation of Cash per Statement of Financial Position to Statement of Cash Flows:</b>		
• Cash at year end per Statement of Cash Flows	412 460	247 754
• Statement of Financial Position items comprising above cash - 'Financial Asset - Cash':		
a) Cash on Hand	87	159
b) Cash at Bank	412 373	247 595
	<u>412 460</u>	<u>247 754</u>
<b>Reconciliation of net surplus to net cash from operating activities:</b>		
Net surplus / (deficit)	31 517	(25 761)
Depreciation	26 733	16 173
(Profit)/Loss on disposal of assets	(632)	-
Write-off of assets	1 587	-
Resources received free of charge capitalised	-	(55 976)
Increase/(Decrease) in provision for employee liabilities	57 214	39 372
Increase/(Decrease) in supplier trade creditors	(5 049)	1 862
(Increase)/Decrease in other assets	25 358	(24 820)
(Increase)/Decrease in GST receivable	56	(3 274)
(Increase)/Decrease in transfers to the Official Public Account	(308 000)	-
<b>Net cash flow from operating activities</b>	<u>(171 216)</u>	<u>(52 424)</u>

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS**  
*for the year ended 30 June 2005*

**Note 5 – Appropriations**

Note 5A – Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund (Appropriations from Acts 1 and 3)

Particulars	Departmental	Total
<b>Year Ended 30 June 2005</b>	<b>\$</b>	<b>\$</b>
Balance carried from previous year	185 399	185 399
Unspent prior year appropriation – invalid s31 <sup>1</sup>	(105 014)	(105 014)
Appropriation Act (No.1) 2004-2005	759 000	759 000
Appropriation Act (No.3) 2004-2005	172 000	172 000
GST credits (FMA s30A)	13 544	13 544
30 June 2005 – variation s31 <sup>2</sup>	105 714	105 714
Total Appropriations available for payments	1 130 643	1 130 643
Payments made (GST inclusive)	807 816	807 816
<b>Balance carried to next year</b>	<b>322 827</b>	<b>322 827</b>
Represented by:		
Cash	319 238	319 238
Add: Receivables – Net GST Receivable from the ATO	3 589	3 589
<b>Total</b>	<b>322 827</b>	<b>322 827</b>
<b>Year Ended 30 June 2004</b>		
Balance carried from previous year	234 549	234 549
Appropriation Act 1 – basic appropriation	709 000	709 000
Appropriation Act (No.3)	32 000	32 000
GST credits (FMA s30A)	12 359	12 359
Annotations to ‘net appropriations’ (FMA s31)	-	-
Total Appropriations available for payments	987 908	987 908
Payments made (GST inclusive)	802 509	802 509
<b>Balance carried to next year</b>	<b>185 399</b>	<b>185 399</b>
Represented by:		
Cash	181 754	181 754
Add: Receivables – Net GST Receivable from the ATO	3 645	3 645
<b>Total</b>	<b>185 399</b>	<b>185 399</b>

- 1 The unspent prior year appropriation of (\$105 014) is derived from the year-by-year analysis summarised in the table to follow later in this Note.
- 2 The 30 June 2005 variation of \$105 714 to section 31 receipts is the amount of:
  - total s31 receipts affected, \$157 946, plus
  - s31 receipts appropriated in 2004-05, \$700, less
  - the amount spent prior to 2004-05 of \$52 932.

Under section 31 of the *Financial Management and Accountability Act 1997* (the FMA Act), the Minister for Finance and Administration may enter into a net appropriation agreement with an agency Minister. Appropriation Acts numbers 1 and 3 (for the ordinary annual services of government) authorise the supplementation of an agency’s annual net appropriation by amounts received in accordance with its section 31 agreement (for example, receipts from charging for goods and services).

One of the conditions that must be satisfied under section 31 of the FMA Act in order for annual net appropriation to be increased lawfully is that an agreement is made between the Finance Minister and the agency Minister or by officials expressly delegated (where permitted) or authorised by them. An agency’s Chief Executive is taken to be so authorised.

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS**  
*for the year ended 30 June 2005*

**Note 5 – Appropriations (continued)**

Note 5A – Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund (Appropriations from Acts 1 and 3 continued)

The section 31 agreement covering the period 1 July 1999 to 20 February 2005 operated and the section 31 monies were recorded as though a valid agreement existed. However the Department of Finance and Administration signatory did not have an express delegation or authority for signing the agreement, with the result that the agreement was ineffective.

The current section 31 agreement was made on 21 February 2005 between the Inspector-General, OIGIS and the Minister for Finance and Administration. Acknowledging the status of prior agreements, this agreement was varied on 24 June 2005, with effect from 30 June 2005, to capture retrospectively all monies that were subject to the ineffective prior agreement. This variation does not validate past breaches of section 83 of the Constitution.

Accordingly:

- amounts disclosed in previous financial years as available for spending under departmental outputs appropriations up to 30 June 2004 were overstated by \$157 946. Of this amount, \$105 014 was unspent as at 30 June 2004 and was incorrectly reflected in the balance brought forward to 1 July 2004
- the 30 June 2005 variation to the s31 agreement increased the appropriation by the amount of invalid receipts (\$158 646). Of this amount \$52 932 from 1999 to 2005 has already been spent, and
- spending up to and including 30 June 2004 totalling \$52 932 was made without the authority of the Parliament, in contravention of section 83 of the Constitution.

A year-by-year analysis of the overstatement of the departmental output appropriations and overspending is given below.

Particulars	1999-00	2000-01	2001-02	2002-03	2003-04	Sub-total	2004-05	Total 1/7/99 to 30/6/05
Receipts Affected	113 768	19 247	21 917	3 014	-	157 946	700	158 646
Unspent	60 836	19 247	21 917	3 014	-	105 014	700	105 714
Amount spent, without appropriation	52 932	-	-	-	-	52 932	-	52 932

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS**  
*for the year ended 30 June 2005*

Note 5B – Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund (Appropriations from Acts 2 and 4)

<b>Particulars</b>	<b>Departmental</b>	<b>Total</b>
<b>Year Ended 30 June 2005</b>	<b>\$</b>	<b>\$</b>
Balance carried from previous year	66 000	66 000
Appropriation Act (No.2) 2004-2005	200 000	200 000
Appropriation Act (No.4) 2004-2005	202 000	202 000
GST credits (FMA Act s30A)	6 678	6 678
Total Appropriations available for payments	474 678	474 678
Payments made (GST inclusive)	73 456	73 456
<b>Balance carried to next year</b>	<b>401 222</b>	<b>401 222</b>
Represented by:		
Cash	93 222	93 222
Add: Receivables – Receivable from the Official Public Account	308 000	308 000
<b>Total</b>	<b>401 222</b>	<b>401 222</b>
<b>Year Ended 30 June 2004</b>		
Balance carried from previous year	66 000	66 000
Appropriation Act (No.2) 2003-04	-	-
Appropriation Act (No.4) 2003-04	-	-
GST credits (FMA Act s30A)	-	-
Total Appropriations available for payments	66 000	66 000
Payments made (GST inclusive)	-	-
<b>Balance carried to next year</b>	<b>66 000</b>	<b>66 000</b>
Represented by:		
Cash	66 000	66 000
Add: Receivables – Receivable from the Official Public Account	-	-
<b>Total</b>	<b>66 000</b>	<b>66 000</b>

Note 5C – Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund (Appropriations from Acts 2 and 4)

The office received \$66 000 as an equity injection in the financial year ended 30 June 2001. The office did not spend any of this appropriation during the current or prior years.

The office received a further \$402 000 as an equity injection in the financial year ended 30 June 2005. The office spent \$73 456 of this appropriation during the current year. The office holds \$308 000 of this amount in the Official Public Account to fund the non-current portion of accrued leave liabilities.

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS**  
*for the year ended 30 June 2005*

**Note 6 – Analysis of Plant and Equipment**

Note 6A – Reconciliation of the Opening and Closing Balances of Plant and Equipment

Item	Plant and Equipment
<b>As at 1 July 2004</b>	
Gross book value	86 664
Accumulated depreciation	(16 173)
<b>Opening Net book value</b>	<b>70 491</b>
Additions	
by purchase	66 778
Depreciation expense	(26 733)
Disposals	
Write-offs	(1 587)
Other disposals	(68)
<b>As at 30 June 2005</b>	
Gross book value	147 895
Accumulated depreciation	(39 014)
<b>Net book value</b>	<b>108 881</b>

Note 6B – Assets at Valuation

Item	Plant and Equipment
<b>As at 30 June 2005</b>	
Gross Value	7 235
Accumulated depreciation	(2 750)
<b>Net book value</b>	<b>4 485</b>
As at 30 June 2004	
Gross Value	9 435
Accumulated depreciation	-
<b>Net book value</b>	<b>9 435</b>

All revaluations are independent and are conducted in accordance with the revaluation policy stated at Note 1. In 2003-04, the revaluations were conducted by an independent valuer A.F. Graham (Certified Practicing Valuer).

**Note 7 - Reporting of Outcomes**

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

Note 7A – Net Cost of Outcome Delivery

The net cost of this outcome in 2004-05 was \$900 183 (Appropriation: \$931 000).

Note 7B – Agency Revenue and Expenses by Output Group

The decision to attribute resources on a 60:40 basis, (60% monitoring and 40% conducting inquiries and providing a complaint resolution service), originated from the Samuel's Inquiry (1995) and has been reinforced by more recent legislative changes.

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS**  
*for the year ended 30 June 2005*

**Note 7 - Reporting of Outcomes (continued)**

Note 7B – Agency Revenue and Expenses by Output Group (continued)

	Output Group 1		Output Group 2		OUTCOME TOTAL	
	2005	2004	2005	2004	2005	2004
	\$	\$	\$	\$	\$	\$
Operating revenues						
Revenues from government	558 600	444 600	372 400	296 400	931 000	741 000
Other income	44 061	90 040	29 374	60 027	73 435	150 067
<b>Total operating revenues</b>	<b>602 661</b>	<b>534 640</b>	<b>401 774</b>	<b>356 427</b>	<b>1 004 435</b>	<b>891 067</b>
Operating expenses						
Employees	434 831	399 402	289 888	266 268	724 719	665 670
Suppliers	131 887	140 991	87 924	93 994	219 811	234 985
Assets written-off	952	-	635	-	1 587	-
Value of assets sold	41	-	27	-	68	-
Equipment depreciation	16 040	9 704	10 693	6 469	26 733	16 173
<b>Total operating expenses</b>	<b>583 751</b>	<b>550 097</b>	<b>389 167</b>	<b>366 731</b>	<b>972 918</b>	<b>916 828</b>

**Note 8 - Executives Remuneration – in excess of \$100 000**

	2004-05	2003-04
\$130 000 to \$139 999	-	1
\$200 000 to \$209 999	-	1
\$340 000 to \$349 999	1	-
The aggregate amount of total remuneration of executives shown above	\$349 672	\$338 894
The aggregate amount of separation and redundancy/termination benefit payments during the year to executives shown above.	Nil	Nil

**Note 9 – Remuneration of Auditor**

Financial statement audit services are provided free of charge to the office. No other services were provided by the Auditor-General.

The fair value of audit services provided was: **\$16 500**      \$13 000

**Note 10 – Staffing Level**

The average staffing level for the office in 2004-05 was 5 (2003-04: 5).

**Note 11 - Act of Grace Payments, Waivers, Defective Administration Scheme, and Payments made under s73 of the Public Service Act 1999**

No 'Act of Grace' payments were made during the reporting period, (2003-04: nil).

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS**  
*for the year ended 30 June 2005*

No waivers of amounts owing to the Commonwealth were made during the reporting period, (2003-04: nil).

No payments were made under the 'Defective Administration Scheme' during the reporting period, (2003-04: nil).

No payments were made under section 73 of the *Public Service Act 1999*, (2003-04: nil).

**Note 12 – Financial Instruments**

Note 12A – Interest Rate Risk

Financial Instruments (Recognised)	Floating interest rate		Non-Interest Bearing		Total		Weighted Average Effective Interest Rate	
	04-05	03-04	04-05	03-04	04-05	03-04	04-05	03-04
	\$	\$	\$	\$	\$	\$	\$	\$
<b>Financial Assets</b>								
Cash on hand	-	-	87	159	87	159	n/a	n/a
Cash at Bank	-	-	412 373	247 595	412 373	247 595	n/a	n/a
Receivables for goods or services (gross)	-	-	312 079	29 492	312 079	29 492	n/a	n/a
<b>Total</b>			<b>724 539</b>	<b>277 246</b>	<b>724 539</b>	<b>277 246</b>		
<b>Total Assets</b>					<b>833 420</b>	<b>347 737</b>		
<b>Financial Liabilities</b>								
Trade Creditors	-	-	17 454	4 597	17 454	4 597	n/a	n/a
Other Payables	-	-	-	17 906	-	17 906	n/a	n/a
<b>Total</b>	-	-	<b>17 454</b>	<b>22 503</b>	<b>17 454</b>	<b>22 503</b>		
<b>Total Liabilities</b>					<b>424 838</b>	<b>372 673</b>		

No funds were invested at a fixed interest rate.

Note 12B – 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.

Note 12C – 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 Statement of Financial Performance.

The office has no significant exposure to any concentrations of credit risk. All figures for credit risk referred to do not take into account the value of any collateral or other security.

**Note 13 – Special Accounts**

The office has two special accounts established under section 20 of the FMA Act. The accounts established are "Other Trust Moneys and Services for the Government" and "Non Agency Bodies Account". These accounts have never been active.



## INDEPENDENT AUDIT REPORT

To the Prime Minister

### Matters relating to the Electronic Presentation of the Audited Financial Statements

This audit report relates to the financial statements published in both the annual report and on the website of the Office of the Inspector-General of Intelligence and Security for the year ended 30 June 2005. The Office's Inspector-General is responsible for the integrity of both the annual report and the web site.

The audit report refers only to the financial 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

#### *The financial statements and Inspector-General's responsibility*

The financial statements comprise:

- Statement by the Inspector-General;
- Statements of Financial Performance, Financial Position and Cash Flows;
- Schedules of Commitments and Contingencies; and
- Notes to and forming part of the Financial Statements

of the Office of the Inspector-General of Intelligence and Security for the year ended 30 June 2005.

The Inspector-General is responsible for preparing financial statements that give a true and fair presentation of the financial position and performance of the Office of the Inspector-General of Intelligence and Security, and that comply with accounting standards, other mandatory financial reporting requirements in Australia, and the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*. The Inspector-General is also responsible for the maintenance of adequate accounting records and internal controls that are designed to prevent and detect fraud and error, and for the accounting policies and accounting estimates inherent in the financial statements.

### ***Audit approach***

I have conducted an independent audit of the financial statements in order to express an opinion on them to you. My audit has been conducted in accordance with the Australian National Audit Office Auditing Standards, which incorporate the Australian Auditing and Assurance Standards, in order to provide reasonable assurance as to whether the financial statements are free of material misstatement. The nature of an audit is influenced by factors such as the use of professional judgement, selective testing, the inherent limitations of internal control, and the availability of persuasive, rather than conclusive, evidence. Therefore, an audit cannot guarantee that all material misstatements have been detected.

While the effectiveness of management's internal controls over financial reporting was considered when determining the nature and extent of audit procedures, the audit was not designed to provide assurance on internal controls.

I have performed procedures to assess whether, in all material respects, the financial statements present fairly, in accordance with the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, accounting standards and other mandatory financial reporting requirements in Australia, a view which is consistent with my understanding of the Office of the Inspector-General of Intelligence and Security's financial position, and of its performance as represented by the statements of financial performance and cash flows.

The audit opinion is formed on the basis of these procedures, which included:

- examining, on a test basis, information to provide evidence supporting the amounts and disclosures in the financial statements; and
- assessing the appropriateness of the accounting policies and disclosures used, and the reasonableness of significant accounting estimates made by the Inspector-General.

### ***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.

### **Audit Opinion**

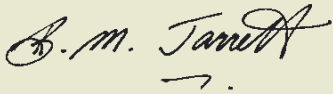
In my opinion, the financial statements of the Office of the Inspector-General of Intelligence and Security:

- (a) have been prepared in accordance with the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*; and
- (b) give a true and fair view of the Office of the Inspector-General of Intelligence and Security's financial position as at 30 June 2005 and of its performance and cash flows for the year then ended, in accordance with:
  - (i) the matters required by the Finance Minister's Orders; and
  - (ii) applicable accounting standards and other mandatory financial reporting requirements in Australia.

**Additional Statutory Disclosure**

As detailed in Note 5 of the financial statements, the Office of the Inspector-General of Intelligence and Security has contravened section 83 of the Constitution.

Australian National Audit Office

A handwritten signature in black ink, appearing to read "B. M. Jarrett". The signature is written in a cursive style with a horizontal line underneath.

Brandon Jarrett  
Executive Director

Delegate of the Auditor-General  
Canberra

29 September 2005



# Annex 1—Complaint and inquiry statistics

**Table 1—IGIS Act inquiries actioned between 1 July 2004—30 June 2005**

Agency	Source	Date of Receipt	Type of Inquiry <sup>28</sup>	Conclusion Notified	Current Status
ASIS	Own motion	27/11/03	Full	12/11/04	Closed
ASIO	Public	15/02/04	Full	22/02/05	Closed
DIO	Minister	04/05/04	Full	30/11/04	Closed
ASIO	Public	12/05/04	Full	02/03/05	Closed
ASIO	Public	15/06/04	Preliminary	23/07/04	Closed
DSD	Public	15/06/04	Preliminary	23/07/04	Closed
ASIO	Public	21/06/04	Preliminary	30/09/04	Closed
DSD	Public	21/06/04	Preliminary	30/09/04	Closed
ASIO	Public	21/06/04	Preliminary	16/07/04	Closed
ASIO	Public	30/07/04	Full	13/09/04	Closed
DSD	Public	16/08/04	Preliminary	29/11/04	Closed
DSD	Public	25/08/04	Preliminary	22/12/04	Closed
ASIO	Public	10/09/04	Preliminary	16/09/04	Closed
DSD	Public	16/09/04	Preliminary	08/11/04	Closed
ASIO	Public	28/09/04	Full	08/12/04	Closed
ASIO	Public	12/10/04	Preliminary	27/10/04	Closed
ASIO	Public	14/10/04	Preliminary	20/10/04	Closed
ASIO	Ex-employee	21/10/04	Preliminary	27/10/04	Closed
ASIO	Public	03/11/04	Preliminary	04/02/05	Closed
ASIO	Public	23/11/04	Preliminary	02/02/05	Closed
ASIO	Public	23/11/04	Preliminary	25/11/04	Closed
ASIO	Public	17/12/04	Preliminary	02/02/05	Closed
ASIO	Public	22/12/04	Preliminary	11/01/05	Closed

<sup>28</sup> A preliminary inquiry allows the Inspector-General to determine whether the issues raised fall within the jurisdiction of the Inspector-General and whether a full inquiry should be conducted. A full inquiry allows the Inspector-General to use the complete range of statutory powers in the IGIS Act.

Agency	Source	Date of Receipt	Type of Inquiry <sup>28</sup>	Conclusion Notified	Current Status
ONA	Public	13/01/05	Preliminary	03/02/05	Closed
ASIO	Public	17/01/05	Preliminary	22/03/05	Closed
ASIO	Public	17/01/05	Preliminary	03/03/05	Closed
ASIO	Ex-employee	25/01/05	Full		Open
ASIO	Public	31/01/05	Preliminary	11/04/05	Closed
ASIO	Public	31/01/05	Preliminary	11/04/05	Closed
ASIO	Public	01/02/05	Preliminary	28/02/05	Closed
ASIS	Public	16/02/05	Preliminary	04/04/05	Closed
ASIO	Public	24/02/05	Full	17/06/05	Closed
ASIO	Public	12/04/05	Preliminary	12/05/05	Closed
ASIO	Public	20/04/05	Preliminary	19/05/05	Closed
ASIO	Public	26/04/05	Preliminary	20/05/05	Closed
ASIO	Own motion	18/05/05	Preliminary	09/06/05	Closed
ASIS	Own motion	18/05/05	Preliminary	23/05/05	Closed
ASIO	Public	08/06/05	Preliminary		Open
ASIO	Public	16/06/05	Preliminary		Open
ASIO	Public	17/06/05	Preliminary	28/06/05	Closed
ASIO	Public	23/06/05	Preliminary		Open
ASIO	Public	27/06/05	Preliminary		Open

**Table 2—Concerns about agencies that were handled without need for inquiry action  
1 July 2004 – 30 June 2005**

Agency	Source	Date of complaint	Former complainant	Current status
ASIO	Public	08/07/04	Yes	Closed
ASIO	Ex-employee	16/07/04	No	Closed
ASIO	Public	20/07/04	Yes	Closed
ASIO	Public	21/07/04	Yes	Closed
DIO	Public	28/07/04	No	Closed
ASIO	Public	02/08/04	Yes	Closed
ASIO	Public	11/08/04	Yes	Closed
ASIO	Public	31/08/04	Yes	Closed
ASIO	Public	02/09/04	No	Closed
DIO	Public	06/09/04	No	Closed
DSD	Public	11/09/04	No	Closed
ASIO	Public	13/09/04	No	Closed

<b>Agency</b>	<b>Source</b>	<b>Date of complaint</b>	<b>Former complainant</b>	<b>Current status</b>
ASIS	Public	17/10/04	Yes	Closed
ASIO	Public	30/10/04	Yes	Closed
ASIO	Public	18/11/04	No	Closed
ASIO	Public	26/11/04	No	Closed
ASIO	Public	26/11/04	No	Closed
DSD	Employee	01/12/04	No	Closed
ASIO	Public	01/12/04	Yes	Closed
ASIO	Public	01/12/04	Yes	Closed
ASIO	Public	01/12/04	No	Closed
ASIO	Public	07/12/04	Yes	Closed
ASIO	Public	10/12/04	No	Closed
ASIO	Public	11/12/04	Yes	Closed
ASIO	Public	18/01/05	No	Closed
ASIO	Public	22/02/05	No	Closed
DSD	Public	02/03/05	No	Closed
ASIO	Public	11/03/05	No	Closed
ASIO	Public	29/03/05	No	Closed
ASIS	Public	27/04/05	No	Closed
ASIO	Public	29/04/05	No	Closed
ASIO	Public	29/04/05	No	Closed
ASIO	Public	05/05/05	No	Closed
ASIO	Public	10/05/05	No	Closed
ASIO	Public	22/05/05	Yes	Closed
ASIO	Employee	25/05/05	No	Closed
ASIO	Public	30/05/05	No	Closed
ASIS	Public	07/06/05	No	Open
ASIO	Public	08/06/05	Yes	Closed
ASIO	Public	17/06/05	No	Closed
ASIO	Public	30/06/05	No	Open

**Table 3—Immigration related concerns that were handled without need for inquiry action  
1 July 2004 – 30 June 2005**

<b>Agency</b>	<b>Source</b>	<b>Date of complaint</b>	<b>Former complainant</b>	<b>Current status</b>
ASIO	Public	03/02/05	Yes	Closed
ASIO	Public	07/02/05	Yes	Closed
ASIO	Public	01/03/05	No	Closed
ASIO	Public	10/03/05	Yes	Closed
ASIO	Public	15/03/05	No	Closed
ASIO	Public	15/03/05	No	Closed
ASIO	Public	11/04/05	No	Closed
ASIO	Public	15/04/05	Yes	Closed
ASIO	Public	15/04/05	Yes	Closed
ASIO	Public	20/04/05	Yes	Closed
ASIO	Public	27/04/05	No	Closed
ASIO	Public	04/05/05	Yes	Closed
ASIO	Public	04/05/05	Yes	Closed
ASIO	Public	16/05/05	Yes	Closed
ASIO	Public	18/05/05	Yes	Closed
ASIO	Public	01/06/05	Yes	Closed
ASIO	Public	23/06/05	Yes	Closed



effectiveness and appropriateness of agency procedures in regard to legality, propriety and consistency with human rights.

9. There has not been a requirement to date to use the inquiry power in respect of warrants issued in accordance with section 34D of the ASIO Act. My predecessor (Mr Bill Blick PSM) and I have relied on the general powers conferred by section 9A of the IGIS Act and section 34HAB of the ASIO Act, to witness at first hand, the conduct of questioning under the section 34D warrants issued so far.

10. Section 34HAB of the ASIO Act expressly refers to the right of the Inspector-General to perform this function:

“To avoid doubt, for the purposes of performing functions under the Inspector-General of Intelligence and Security Act 1986, the Inspector-General of Intelligence and Security, or an APS employee assisting the Inspector-General, may be present at the questioning or taking into custody of a person under this Division.”

### **Specific safeguards involving IGIS**

11. The legislative provisions that provide ASIO with access to questioning and detention powers run to over 40 pages. The length of Division 3 of Part III of the ASIO Act reflects the considerable efforts of the Parliament to incorporate strong safeguards into the various sections of this Division.

12. Those safeguards which specifically involve the Inspector-General include the following:

- ▶ Section 34C(3A)(a)(i) requires that the IGIS be consulted in the development of a written statement of procedures to be followed in the exercise of authority under section 34D of the ASIO Act.
- ▶ Section 34E(1)(e)(i) requires the Prescribed Authority (who supervises the questioning, and is usually a former Judge) to explain to the subject of a section 34D warrant that they have the right to make a complaint to the IGIS about ASIO, either orally or in writing.
- ▶ Section 34F (9)(c) requires that anyone holding a person in custody or detention under Division 3 of the ASIO Act must give the person facilities for contacting the IGIS.
- ▶ Section 34HAB of the ASIO Act ensures that the IGIS (or his staff) can be present at the questioning or taking into custody of such a person.
- ▶ Section 34HA of the ASIO Act provides that where the IGIS has a concern about impropriety or illegality in connection with the exercise of powers under that warrant, they may raise that concern with the Prescribed Authority, who must consider the Inspector-General's concern.
- ▶ Section 34Q of the ASIO Act details those materials which ASIO is required to provide to the IGIS in respect of section 34D warrants. These materials include a copy of any draft requests for a warrant given to the Attorney-General, any warrants issued, a copy of any video recordings made of the questioning of subjects, and a statement containing details of any seizure, taking into custody, or detention.
- ▶ Section 34QA imposes a reporting requirement on the IGIS where multiple warrants are issued in respect of an individual.

13. Comments on how these have operated in practice are set out below.

### **Protocol**

14. In respect of the first dot point at paragraph 12 immediately above, my predecessor was fully consulted in the development of a protocol made pursuant to the requirements of subsection 34C(3A) of the ASIO Act. He provided a written statement on 28 July 2003 that he had no concerns with its contents.

15. The protocol, which sets out the standards applicable in relation to the detention and questioning of a person who is the subject of a warrant issued under section 34D of the ASIO Act, was tabled in the Commonwealth Parliament on 12 August 2003.

16. So as to give the protocol wide exposure, I included it as an annex in my most recent annual report, and it is also accessible via the website for my office.

### ***Explanations by Prescribed Authority***

17. The second safeguard referred to above, is the requirement for the Prescribed Authority to explain to the subject of a section 34D warrant that they have the right to make a complaint to the IGIS, either orally or in writing. This requirement has been satisfied on each occasion a section 34D warrant has been executed.

### ***Facilities to contact***

18. The requirement under section 34F (9)(c) of the ASIO Act that persons held in custody or detention must be provided with facilities for contacting the IGIS, has not been tested as no person has thus far been the subject of detention.

### ***Attendance by IGIS or staff***

19. The Director-General of Security has placed on the public record that in the 2003/04 financial year, ASIO executed section 34D warrants against three persons (see the publicly available ASIO Annual Report 2003–2004, pp 39–40).

20. Either Mr Blick, myself, or one of my staff, were present on all days when the subjects of these three warrants were questioned, for the full duration of the questioning, with the exception of a relatively brief period on one day (approximately three hours), which was video-taped and for which a full written transcript was also provided to my office.

21. I or one of my staff have since attended on at least the first day of questioning for questioning warrants issued so far in 2004/05. We have usually not attended on subsequent days. I decided that we should make a judgement after the first day on whether further attendance was necessary. Considerations underpinning this approach are:

- ▶ If a problem were to arise it is most likely to do so on the first day that the subject is required to attend for questioning.
- ▶ Based on our attendance at the first three questioning warrants, my predecessor and I have been satisfied that proper regard has been paid to the legislative requirements and the welfare of the subjects of the warrants.
- ▶ Supervision by the Prescribed Authorities has been effective.
- ▶ I, or a member of my staff, can be contacted by phone or by other electronic means should the subject of a section 34D warrant wish to lodge a complaint and we are not physically present.
- ▶ Section 34K(1) of the ASIO Act requires that a video recording must be made of a person's appearance before a prescribed authority for questioning under a warrant, and section 34Q(b) requires that a copy of any such recording must be given to the IGIS.
- ▶ As a matter of practice, the Director-General of Security also provides a copy of the transcript of all questioning conducted under section 34D warrants. These are read carefully and if appropriate, relevant sections of the video recording can be viewed.

22. Importantly, on the basis of the questioning observed at first hand and scrutinised by means of the transcripts and video recordings, I can say that the subjects have been treated humanely (as required by section 34J). The questioning has been conducted in an appropriate manner and the individuals who have been the subject of questioning have been accorded dignity and respect. On some occasions this has been in the face of abusive or evasive comments—nonetheless professionalism was maintained by ASIO and Australian Government Solicitor staff involved.

### **Capacity to raise concern**

23. Section 34HA provides the IGIS with the capacity to raise any concerns about impropriety or illegality with the Prescribed Authority, who must consider that concern.

24. This mechanism has been used in one instance, when I raised with the Prescribed Authority whether the warrant was specific enough in setting out the relevant terrorism offences. This issue was discussed with me by the subject's legal representative prior to questioning commencing and using the section 34HA mechanism was a means of having the matter considered by the Prescribed Authority.

25. The Prescribed Authority heard argument from the AGS officer representing ASIO and from the subject's legal representative. Having considered those submissions the Prescribed Authority ruled that the warrant was not flawed. This was a suitable resolution of the issue and questioning then proceeded.

### **Provision of material**

26. Section 34Q requires that certain materials be provided to the IGIS, as soon as practicable (eg. a copy of any draft request for a warrant given to the Attorney-General, a copy of any warrant issued, a copy of any video recording which is made under the questioning etc.). These requirements have been satisfied by ASIO.

27. The provision of the draft warrant provides me with an opportunity to check that the legislative requirements to that point have been complied with and that, on the face of the material, there is sufficient justification for seeking a warrant. I have not needed to query anything with the Director-General in this regard.

### **Multiple warrants**

28. As mentioned in paragraph 12, section 34QA of the ASIO Act imposes a reporting requirement on the Inspector-General where multiple warrants are issued in respect of an individual. It has not been necessary to fulfil this requirement as no multiple warrants have yet been issued.

### **Other issues**

29. Mr Blick and I have corresponded with the Director-General of Security, giving our views on how the new powers have worked in practice and also raising several other issues (of a largely procedural nature) including:

- ▶ whether lawyers representing the subjects of such warrants should be given additional scope to address the Prescribed Authority
- ▶ distinguishing between 'questioning time' and 'procedural time' for the purposes of determining when questioning under a warrant should cease,
- ▶ the provision of legal aid to the subjects of warrants,
- ▶ the payment of expenses for the subjects of section 34D warrants,
- ▶ the degree of privacy which is afforded to the subject of such warrants to meet their religious obligations, consult their legal representatives or lodge complaints, and
- ▶ the timeliness of the reporting of outcomes to the Attorney-General.

### **Role of lawyers**

30. The role of lawyers representing the subjects of section 34D warrants is limited by the provisions of section 34U of the ASIO Act.

31. The practical effect of this section is that a subject's legal representative may only provide legal advice during breaks in the questioning, and they may not intervene in the questioning of their client, except to request clarification of an ambiguous question.

32. Section 34U is constructed this way to ensure that questioning is not unduly disrupted. While this limitation exists for good reason, it has the potential to be the cause of some frustration when lawyers wish to raise procedural queries with the Prescribed Authority, but are unable to do so due to the limitations described above.

33. The subjects of section 34D warrants, as opposed to their legal representatives, are able to raise queries directly with the Prescribed Authority, but not surprisingly can sometimes have difficulty in fully expressing their point.

34. The Prescribed Authorities have, to date, generally interpreted section 34U fairly strictly, by not permitting any questions to be put to them by the lawyers of the subjects of section 34D warrants, other than to clarify ambiguity. Prescribed Authorities have, however, shown some flexibility on occasion eg in allowing a legal representative the opportunity to respond to an ASIO request that questioning be allowed to continue.

35. I would suggest that there should be clearer authority in the ASIO Act for legal representatives to address the Prescribed Authority, at least on some matters; and that in conjunction with another change this would not risk disruption to the questioning itself.

36. This second change would be to make clearer in the legislation the concepts of "procedural time" and "questioning time".

37. Section 34HB of the ASIO Act provides guidance on the periods of time during which individuals can be questioned. The provisions are expressed in terms of the calculation of time when 'questioning' occurs rather than the simple elapse of eight hour periods of time.

38. In practice, the Prescribed Authority and an ASIO timekeeper keep a strict log of periods during which questioning occurs. These timesheets are compared at regular intervals (eg. lunch and the end of the day) to ensure they coincide. The agreed timesheets form a record of the time during which questions were put (or 'questioning time').

39. The notion of 'procedural time' encompasses all other time when the Prescribed Authority is present. For example the Prescribed Authority is required to explain the meaning of the warrant when the subject first attends (section 34E refers). This process can often take 30 or more minutes. The explanation is often repeated in briefer form on subsequent days.

40. The Prescribed Authority must also break from questioning periodically to deal with 'housekeeping' matters (eg. to permit audio and video tapes to be changed), or to address the needs of the subject of the warrant (eg. to permit religious observance, attendance to medical conditions).

41. As mentioned, I believe there would be merit in clearly distinguishing between 'questioning time' and 'procedural time' in the ASIO Act for the purposes of section 34D warrants. If this were to occur the limitation on legal representatives during 'questioning time' could be maintained, but there would be an opportunity for legal representatives to raise procedural and other issues during periods of 'procedural time' (which does not count in the calculation of time during which questioning has occurred).

### ***Legal aid***

42. Another issue of interest identified by this office relates to the provision of legal aid. I am advised that when a warrant is served on a person pursuant to Division 3 of Part III of the ASIO Act, they are also provided with guidance on the Special Circumstances Scheme administered by the Attorney-General's Department, which may cover reasonable legal costs and related expenses, depending on an applicant's eligibility. The provision of legal aid under this scheme is discretionary and ASIO plays no part in the approval process.

43. I understand that all applications to date have been personally considered by the Secretary of the Attorney-General's Department and that all have been granted some level of assistance.

44. In the particular circumstances in which questioning warrants are sought, where the purpose is to obtain intelligence that cannot ordinarily be used in other proceedings, an argument can be made that there should be automatic provision of necessary legal assistance to the subject of these warrants, at the rate applicable under the Special Circumstances Scheme.

45. In practice this does not appear to have been an issue to date, but the Committee may wish to explore the point further.

### **Expenses**

46. The Committee might also wish to consider whether reasonable expenses should be paid to persons required to attend for questioning, at least in some instances.

47. The strict secrecy provisions attached to section 34D warrants, and the requirement that subjects must make themselves available at a specified place and time for an initially undefined duration, have the potential to present employment related issues for the subjects of section 34D warrants.

48. The subjects of section 34D warrants may, if they are employed, experience practical difficulties in obtaining leave from their employment given that they are generally prohibited from advising their employer why they require leave and they are unaware of the likely period of their absence. Such difficulties are compounded if the individual concerned does not have leave entitlements upon which they can call.

49. While ASIO and the Prescribed Authorities have shown some flexibility in determining when questioning sessions occur there will be circumstances when such flexibility is not possible or advisable.

50. While the payment of reasonable 'witness' expenses would not alleviate all of these problems, it would assist such individuals to meet their commitments, if they are not to be left out of pocket as a consequence of their compliance with a direction to attend.

51. In some instances the subject of a section 34D warrant has been in receipt of income support from Centrelink. ASIO representatives have indicated that if there could be a clash between attending a questioning session and Centrelink obligations, they will approach Centrelink to ensure there is no disruption to the income support payments by reason of attending the questioning session. I believe this is an appropriate approach.

### **Privacy**

52. Another issue raised with the Director-General of Security concerns the degree of privacy which is afforded to the subject of section 34D warrants to meet their religious obligations, consult their legal representatives, or lodge complaints.

53. I can advise that after some very minor teething problems at the outset, the provision of facilities for the above purposes has been appropriate. ASIO and the various Prescribed Authorities have shown appropriate sensitivity to the needs of the subjects of section 34D warrants.

### **Reporting outcomes**

54. A further issue which I have raised with the Director-General of Security concerns the timeliness with which the Organisation reports the outcome and value of warrants issued under section 34D of the ASIO Act.

55. Section 34P of the ASIO Act simply requires ASIO to provide a written report for each warrant issued under section 34D, on the extent to which action taken under the warrant has assisted the Organisation in carrying out its functions. No time frame is specified for the provision of these reports.

56. ASIO is required under section 17 of the *Telecommunications (Interception) Act 1979* to provide a report in writing to the Attorney-General on the extent to which the interception of communications made under the authority of a warrant, has assisted the Organisation, within three months of the expiry or revocation of those warrants.

57. As the use of section 34D powers is no less sensitive or intrusive than the use of telecommunication interception warrants, I think it would be reasonable to impose a similar reporting requirement on the use of section 34D warrants as exists for telephone interception warrants.

58. I am advised that in practice the Director-General provides an early oral report to the Attorney-General, but in my view it is important that there be a documentary record within a reasonable time.

### **Further possible legislative refinements**

59. In addition to the above suggestions, there are two further legislative refinements which the Committee could consider.

60. There would be merit in having the greatest possible clarity in distinguishing between those provisions which are specific to 'questioning and detention' warrants, from those provisions which refer specifically to 'questioning' only warrants. This comment also applies to the protocol required by the ASIO Act.

61. The current arrangement is complex in parts and any move to simplify the existing structure would assist subjects, their legal representatives and the community generally to understand an important and sensitive piece of legislation.

62. The second issue concerns ASIO's practice of creating a transcript of each questioning session conducted under a section 34D warrant. The transcript is created by ASIO for its own purposes, but may be relied upon in court proceeding should the subject of a section 34D warrant be prosecuted for deliberately providing false or misleading information.

63. The Director-General of Security has kindly provided me with a copy of each transcript, as it becomes available, but this has been at his discretion.

64. I find these transcripts to be of significant value as it enables me to effectively monitor the questioning of the subjects of section 34D warrants, on those occasions when this office is not physically represented.

65. Section 34Q of the ASIO Act could be readily amended to require that when a transcript is produced, a copy must be provided to the Inspector-General.

### **Conclusion**

66. Although I have proposed a number of technical amendments to Division 3 of Part III of the ASIO Act, I do not wish to convey a negative impression of its use to date. To the contrary, I have been reassured by what I have witnessed.

67. My predecessor, my staff and I have come to the same general conclusions in respect of each section 34D warrant we have witnessed being executed, namely:

- ▶ the questioning of the subjects of s34D warrants has been conducted in a professional and appropriate manner
- ▶ the individuals who have been the subject of questioning have been accorded dignity and respect
- ▶ the facilities used for each questioning session have been appropriate
- ▶ due consideration has been given in each case to the subject's physical comfort and religious needs, and
- ▶ the existing commitments of subjects have been properly taken into account in determining the timing of questioning.

68. I would be pleased to appear before the Committee to amplify any of the points made in this submission, should it so wish.

30 March 2005



For the purposes of my examination, I posed the following questions:

1. Is there additional material from the inquiry by Capt Toohey or in Lt Col Collins' letter to the Prime Minister dated 18 March 2004, which mean the inquiry by the IGIS completed in May 2003 should be re-opened?
2. Are the procedural criticisms by Lt Col Collins and Capt Toohey of that IGIS inquiry correct and significant?
3. Are the concerns of Lt Col Collins about the Jenkins case and alleged comments and actions by a senior officer in 1998 relevant to my jurisdiction?
4. Are there other issues contained in those documents which might appropriately be the subject of an inquiry by me?

My detailed consideration of these is set out in Attachments A–D\*. A summary is set out below.

### Question 1

The previous IGIS, Mr W J Blick, considered three issues:

- (a) Whether DIO had acted in mid-1998 to quash early warning, included in an assessment prepared by Lt Col Collins, of problems developing in East Timor which would require ADF deployment.
- (b) Whether DIO assessments were relatively soft on Indonesia, reflecting a DIO view that related more to its perception of an Australian policy line than a professional assessment of the situation.
- (c) Whether access to an intelligence database had been deliberately cut by DIO in December 1999.

On the first of these Mr Blick concluded that what Lt Col Collins interpreted as an attempt to quash contrary views appear to be legitimate expressions of concern about parts of the content of his assessment and about his wide distribution of assessments and comments. I think this is a correct reading of the written evidence. There is no new material on this in Capt Toohey's report or the attached evidence.

I therefore cannot see a case for re-opening this issue.

The second issue is one on which Mr Blick and Capt Toohey reached very different conclusions. Capt Toohey relies on oral evidence from several people he interviewed to find that a "pro-Jakarta lobby" exists in DIO, reporting "what the Government wants to hear". I examined the transcripts of the relevant interviews by Capt Toohey and found that four support the specific notion of a pro-Jakarta lobby in DIO.

I then read carefully all the available relevant DIO material. I looked in particular for the sort of features said by Lt Col Collins and some others to evidence a pro-Jakarta/policy driven approach to assessments by DIO.

The assessments do not uniformly or generally have the characteristics criticised by Lt Col Collins and others (although it must be acknowledged that some are present in a small number). The allegation of a pro-Jakarta lobby in DIO is not supported by the body of written assessments.

While not all of the people who commented to Capt Toohey and Mr Blick support the notion of a pro-Jakarta lobby in DIO, there are some blunt criticisms of the quality of DIO assessments for other reasons. I am not in a position to resolve whether these criticisms of quality including utility to ADF operations, are justified. I note that the current Inquiry into Australian Intelligence Agencies by Mr Philip Flood AO is considering issues such as DIO's performance.

In my view there is no basis for re-opening this aspect of Mr Blick's inquiry.

The available evidence in respect of item (c) supports Mr Blick's conclusion that the loss of access to an intelligence database resulted from technical problems rather than a deliberate decision by DIO. Mr Blick

---

\* These attachments are classified and cannot be released into the public domain.

examined the written records, including available e-mails, and had statutory declarations from five people. Capt Toohey concluded access was deliberately cut, but I can see nothing specific in his report and attached material which would cast into doubt Mr Blick's conclusion.

However, I must point out while Mr Blick's investigation was comprehensive it was not exhaustive, in that evidence was not obtained from three people with some involvement in the events. Nor did Capt Toohey have evidence available to him from these people. Given their immediate involvement it would seem desirable to attempt to obtain evidence from them.

You could, should you wish, request me to inquire into the issue pursuant to Section 8 (3)(a)(ii) of the IGIS Act.

## Question 2

After careful examination, I do not agree with comments that there were procedural defects and incorrect weighing up of the evidence by Mr Blick's inquiry. Capt Toohey concluded that there was a procedural defect in not allowing Lt Col Collins to have a legal representative at a meeting. However, Lt Col Collins is apparently articulate and not afraid to express his point of view. He did not stand accused of anything. The files indicate that Lt Col Collins was given adequate opportunity to express his views and produce material relevant to the issues being considered by Mr Blick.

I cannot see that there was any disadvantage to Lt Col Collins or limitation effected on the inquiry by the absence of a legal representative at that meeting.

## Question 3

Two issues raised by Lt Col Collins in December 2000 were referred to the Department of Defence rather than being dealt with by Mr Blick. One of these related to the inquiry by Mr A S Blunn AO on behalf of my predecessor concerning the investigation into alleged security breaches by the late Mervyn Jenkins. None of the material I have examined justifies further pursuit of that matter by my office.

The other issue is not within my jurisdiction and any advice you require on it will no doubt be available from the Department of Defence.

## Question 4

I have examined the allegations of malicious actions by the Director of DIO towards Lt Col Collins. The transcripts of evidence of key witnesses to Capt Toohey's inquiry do not support the specific allegations made in the redress of grievance. Indeed, one speaks of the Director's intention to "play the ball, not the man". Capt Toohey has commented publicly that he had the advantage of observing the demeanour and body language of those he interviewed. However, a finding of malicious action is very serious and I have cannot agree with reaching such a conclusion in the absence of some specific evidence on the record.

I cannot see any basis on the available material for a formal inquiry by me into allegations of malicious actions by the Director of DIO.

Lt Col Collins also has grievances about his career management and support by the Army. I understand that the Army is dealing with these.

I would be happy to discuss any of these issues with you, if you feel that would be helpful.

I have copied this letter and attachments to General Cosgrove, for his information.

Yours sincerely

Ian Carnell  
Inspector-General of  
Intelligence and Security

3 May 2004

# Annex 4—Abridged IGIS report—Lt Col Lance Collins

## Report of inquiry into the loss of access by Dili users to an intelligence database in December 1999

### Background

On 20 December 1999 several ADF intelligence officers attached to the INTERFET force in Dili, East Timor, lost access to a particular intelligence database hosted by the Defence Intelligence Organisation (DIO). That remained the case until the evening of 21 December 1999.

2. Following subsequent representations to the then Minister for Defence by one of these officers, Lieutenant Colonel Lance Collins, this issue was one of three matters inquired into by my predecessor, Mr Bill Blick PSM. Mr Blick reported in May 2003. On this issue he said, relying significantly on a report from DIO and five statutory declarations, that the loss of access appeared to result from technical problems rather than a deliberate policy decision by DIO.

3. In April 2004 the Chief of the Defence Force, General Peter Cosgrove AC MC, sent to me various papers associated with a redress of grievance by Lt Col Collins. I examined these and other available relevant papers, to consider whether Mr Blick's inquiry should be re-opened and whether there were any other issues which might be within my jurisdiction.

4. Under the *Inspector-General of Intelligence and Security Act 1986* ("IGIS Act") as it currently stands, the Inspector-General of Intelligence and Security can only conduct a formal inquiry into the activities of DIO at the request of the Minister for Defence.

5. In May 2004 I advised Senator the Hon Robert Hill, the Minister for Defence, that there was one issue only which he might consider should be the subject of a further inquiry. This was the loss of access to the particular database on 20 December 1999.

6. Senator Hill then requested me, pursuant to section 8(3)(a) of the IGIS Act, to inquire into how and why the loss of access occurred.

### Approach taken

7. At my request the Department of Defence made available forensic IT expertise from the Defence Security Authority. The two officers who assisted me had no prior involvement in the events under examination and they brought a critical and unbiased perspective to the exercise. I should express my appreciation for the quality and thoroughness of their work.

8. The logs of relevant servers were restored and reviewed. Other components of the IT infrastructure relevant to the provision of access to that database were also examined. Additional e-mails of relevance were identified.

9. The two IT experts and I also spoke to and obtained information from a range of people. As the inquiry progressed I decided that the formal questioning powers in section 18 of the IGIS Act should be used. I therefore required 12 people to appear before me to compulsorily answer questions relevant to the matter under inquiry. Either an oath or an affirmation that the evidence they would give would be true, was administered. One key person was required to appear twice, and one person three times.

### **How access was denied**

10. What is clear from my examination is that this particular denial of access to the relevant Dili users was indeed deliberate. It was not the result of technical failure or technical faults in any part of the system.

11. In the early afternoon (Australian Eastern Summer Time) of 20 December 1999 [a named person], gave a series of commands which disabled the access by the relevant Dili users to the database of concern to this inquiry. A more detailed technical account of this is attached.\*

12. The IT records show that the total period in which the relevant Dili users were denied this means of accessing the database in question was approximately 26 hours.

13. I formally questioned [this person]. He has no recollection of the events [words deleted] but he agreed with my experts' advice that the logs show the denial was deliberate. The expert advice to me was that the change was done by the quickest and easiest means of removing access for a particular group of users. The manner in which the denial was effected, and the state of the logs, do not indicate any attempt to be devious about, or to cover up, what was being done.

14. Two additional e-mails located during the inquiry also point to the denial being deliberate.

15. Furthermore, [another person—Mr A], has told me, on oath, that he instructed [the other person referred to in paragraphs 11 and 13 above] to remove the access.

### **Significance of the loss**

16. It is important to note that we are talking about access to one specific database, not the general availability of intelligence to the users in Dili. The loss of access to the particular database of itself does not seem to have been a critical deficiency in operational terms. The database did not contain real-time intelligence or threat indicators and warning. Such operationally vital information was collected locally, or sent to the deployed forces via other means—Defence computer and communication systems, secure telephone, fax and e-mail—and was not affected by the short-term loss of access to the particular database.

17. Notwithstanding the above, one can readily understand the sensitivity of those in the field to any change, without consultation, in intelligence access arrangements.

18. In this instance, however, the issue was not what was done, but rather the means by which it was done and what was said about it afterwards.

### **Why the access was removed**

19. [Mr A] said that on 20 December 1999 he went and spoke to the Director of DIO, with no third person being present. He asserted that the discussion was one in which the Director made a decision to cut the access of the relevant Dili users while security changes were made in the system to limit access to some categories of sensitive information. [Mr A] said that there was pressure that certain sources of sensitive information were likely to be cut off if security was not improved. He said that [another named person] was not present for this discussion, although in a later interview said that after giving [the person

---

\* All 16 attachments to this report are classified and cannot be released publicly. References to attachments have been deleted from this abridged version for the sake of readability. All significant matters are supported by detailed material in the attachments.

referred to in paragraphs 11, 13 and 15 above] the direction to cut the access, he had gone and spoken to [that other person].

20. I questioned him on whether the Director, in this alleged meeting, had properly understood that the relevant Dili users would lose access, but he still asserted it was probable that the Director had understood. I should note that [Mr A] made his disclosures early in the first interview, before any robust questioning. However, there are issues about the reliability of [Mr A's] testimony which I will discuss later in this report.

21. The Director, DIO gave sworn testimony (key extracts at Attachment D) that he had not directed a cut in access and did not recall a meeting on 20 December 1999 with [Mr A]. He said that on the morning of 21 December 1999 he was told that technical problems were responsible for the loss of access. He said that he did not direct immediate restoration, while consideration was given to whether security limitations could be introduced quickly; on being told this was not possible, he directed restoration of access and this occurred later on 21 December 1999. He was confident that had he had a discussion on 20 December 1999 of the sort outlined by [Mr A], or even one which touched on Dili users, he would have recalled it the next morning in these discussions.

22. What the Director said was consistent with a statutory declaration he made on 10 January 2002:

*"I did not, in December 1999 or at any other time, authorise a cut in the access of INTERFET forces to [the system] or [the database], nor was I then nor am I now aware of any decision by any other DIO officer to cut such access. Prior to discussions with [several named persons] on 21 December 1999 on this issue, I was not even aware that the INTERFET forces had [database] access. I was informed at those discussions that the cut was due to technical problems."*

23. I should note that access by the relevant Dili users to the particular database was not part of the formal intelligence support plan and that the actual access was facilitated by another area of Defence. Comment on the manner in which this was done is contained in a 7 May 2004 ministerial submission by the Department of Defence.

24. Which of [Mr A's] or the Director's account—or a variation on either of them—is to be believed?

25. In order to form a view on this it is useful to look at what is in the contemporary written record. A set of 18 key e-mails and documents is attached. There are also the statutory declarations made to my predecessor in December 2001/January 2002 (Attachment M).

26. On 20 December 1999 there was an e-mail by a [non-DIO officer] to his (non-DIO) senior officers. It includes:

[extract from e-mail text deleted].

27. I will discuss this e-mail further (and the testimony of [the sender of this e-mail and of another person]) later in this report, but should point out now that it [is relevant to Mr A's account].

28. Also sent on 20 December 1999 was an e-mail by Lt Col Collins which objected to the loss of access and mentions he had been advised that it had occurred "on the order of Director, DIO".

29. On 21 December there were discussions between [several named people]. The allegation in paragraph 28 was in front of these [people]. There are no minutes of these discussions. However, [people] did make statutory declarations in December 2001/January 2002.

30. [One person] included in his declaration:

*"In regard to LTCOL Collins' specific concerns, I am not aware of any decision in DIO to turn off [the database] to the [system] in East Timor. At no time did I authorise a feed to be cut off nor am I aware that anyone else did. My clear understanding is that there was a technical problem which resulted in [the database] to Dili failing. I am not certain of the exact nature of the technical problem. [the database] and the IT systems were [rest of sentence deleted]."*

[A meeting was organised]. *At the meeting it was confirmed that the outage was technical. The problems of [the system] not being accredited to have [the database] on it were raised as well as how much Dili needed access to [the database]. A statement of requirement was sought from Dili.*

31. [Another person] declared that:

*With regard to [the database] support, I did not make any recommendation or decision to turn off [the database] support to the [system] terminal for CTF 645. Similarly, to the best of my knowledge there was no decision taken by DDIO to turn off [the database] support to the [system] terminal for CTF 645.*

*To the best of my recollection, refreshed to some extent by a perusal of filed emails and documents originated at the time, I was advised by the DIO IT staff that technical problems associated with security had caused [the database] to be not available to the deployed element. . . I recall that at about the same time, [a named person] noted that in the rush to get the deployable system established in Dili earlier that month, there had been no formal paperwork done to establish a business case for the deployed element to have access to this sensitive material. In anticipation of this becoming an issue (and the Christmas break imminent), [LTCOL Collins was asked] to provide some justification for a business case for the deployed element to have direct access. . ."*

32. [Yet another person] declared that:

*"I have no recollection of any decision by me that CTF 645 should not have [the database] support through the [system]. The cut was, at least in part, a result of technical problems associated with the need to implement more stringent need-to-know access controls for [sensitive] material following the leaks of DIO analysis.*

*After DIO IT reported the [database] problem a decision was taken [that access] should not be restored immediately and that DIO IT should attempt to put in place controls required on [certain] reporting and should investigate whether or not only [certain] related reporting could be provided to the intelligence staff in Dili. I cannot recall the exact details of what was put in place or the exact nature of the technical fault, but we could not put in all of the restrictions we had hoped to. [Sentence deleted]."*

33. On 21 December 1999 Lt Col Collins responded to [the] request for access justification, and included a comment: "It is interesting that [a named person] reported that DDIO did not order the denial of intelligence. Some faceless bureaucrat assumed far too much."

34. On that day [a named person] prepared a draft minute to Lt Col Collins which included:

*"The purpose of this minute is to formally advise you that DDIO has agreed to the restoration of full [database] services to [the system] within CTF 645 provided certain conditions are met. While DDIO did not direct the removal of the [database] feed, he is concerned at the scope and level of reporting and assessment being produced by you and your staff on events that are outside the INTERFET area of operations."*

35. This minute was not sent. Instead the Director prepared his own minute on 22 December 1999 to Lt Col Collins, copied to Maj Gen Cosgrove. It included:

*"Full [database] services to [the system] within CTF 645 have been restored. I did not direct the removal of the [database] feed, but I did authorise a short delay in its restoration until certain issues had been clarified—namely, access on a need-to-know basis and protection of the material accessed, and respective responsibilities for the production of intelligence. This minute outlines those issues."*

36. My inquiry also located another message sent early on 22 December 1999, from [one person] to another DIO staff member. Apparently unaware that access had been restored on the evening of 21 December, this minute said:

*"I have spoken to [a named person] on this matter. If there are no security implications with the [intelligence] staff having access to [the database] and they have found it to be valuable, I can't see why it should be cut off. Apparently [Mr A] discovered they had access, went and spoke to DDIO and [the same named person] then cut it off."*

37. Neither the [sender or the person to whom he had spoken]—when formally questioned by me—could recall the discussion alluded to in this minute. However, there is no reason to doubt that it records [the sender's] genuine understanding at the time. Importantly, it does not state that the Director or [the person named in the e-mail] actually instructed that the access be cut; it is ambiguous in that regard. And I recognise that its hearsay nature means caution is warranted. However, it does provide some support for the view that there was at least one discussion of some sort involving DIO management on 20 December 1999 prior to the access cut.

38. [The named person in the e-mail referred to in paragraph 36], advised me in sworn testimony that he has no firm recollection of what occurred on 20 and 21 December 1999. This is somewhat frustrating given the positioning of [that person] in relation to these events. However, it is four and a half years since the events and after carefully questioning him twice, I must accept that there is nothing he can add beyond what is in his statutory declaration.

39. Upon request, the Director made available his hard copy diary from that time. I also had access to his electronic diary. The entries on 20 December 1999 do not include one referring to [Mr A]. This suggests that if there was indeed a discussion, the Director did not at the time consider it a particularly significant one. If this were the case, it is also quite likely that he would not recall it either two years later (for Mr Blick's inquiry), or four and a half years later (when queried by me).

40. [Two named people] were not able, when interviewed by me recently, to recall the events in a specific way which adds much to what is contained in their statutory declarations. Both could vaguely recall that there was some surprise on the morning of 21 December 1999 (when they met with the Director) that it had been alleged the access might have been cut deliberately. [Two sentences deleted].

41. There is arguably further support, at least in part, for the account in paragraph 19 by [Mr A] of a meeting on 20 December 1999 from [another named person]. [This other person] told me on oath that he could recall in a general way [Mr A] [words deleted] at sometime prior to Christmas and saying that the Director had ordered a cut in the access of Dili users. In the broad I accept his account.

42. This suggests [Mr A] may have thought he had been given such a direction, but it does not confirm that the Director had intended such an outcome. Equally, it does not support a hypothesis that [Mr A] acted unilaterally on 20 December 1999 and is now saying the Director was involved, to diminish his own responsibility for what occurred.

43. It was suggested to me that [Mr A] may have been covering up his actions right from the start (ie. in December 1999)—and by implication that this sort of comment was “staged”—but I do not find that credible after reflecting upon the general views of others about [Mr A]. [One colleague of Mr A] commented that “[Mr A] was always very positive in supporting deployed elements”.

44. Nor do I think it is credible to suggest that there was some sort of a conspiracy in the IT area of DIO. The IT area was under pressure and security was an important issue, but it was also an area which “routinely worked excessive hours in order to ensure the best possible support was provided”.

45. I think it is plausible that some sort of a discussion did occur on 20 December 1999 between the Director and [Mr A]. There is the contemporaneous record of the e-mail quoted in paragraph 36, and there is the account given by [a named person] (paragraph 41). But if it did occur what did such a discussion involve?

46. There are some strong reasons to not accept the detail proffered to me by [Mr A]. These flow from consideration of:

- (a) the statutory declaration he made in December 2001,
- (b) the account given of a meeting in December 2001 by [a named person] (an officer in DIO), and
- (c) the e-mail sent on 20 December 1999 [words deleted] (already mentioned in paragraph 26).

47. On 12 December 2001 [Mr A] made a statutory declaration for my predecessor (copy in Attachment M), in which he stated:

*"To the best of my recollection, having read through correspondence and recovered documents at the time, the technical problem which resulted in [the database] support to CTF645 failing on 20 December 1999 resulted from actions by DIO IT to put in place enhanced security on [the database] for Dili users."*

48. [The person referred to in paragraph 46(b)] told me in sworn testimony that he could recall being present at a discussion in December 2001 involving [rest of, and next sentence deleted].

49. I should note that [this person] had no direct involvement with the events being considered, [rest of sentence deleted].

50. [This person] recalled that in this December 2001 discussion:

*"[Mr A] was saying 'I think we cut it' and then Frank was saying 'well that's not what you told me at the time, ... are you sure of this?' He said 'oh'. He tended to waver on whether it was or was not..."*

51. According to [this person] the last thing that the Director said when they left the room was "make sure it's the facts and that you are confident in what you say". I questioned [this person] on whether the discussion included any suggestion of bullying by the Director of [Mr A], or whether the two of them seemed to be "cooking up a story"; but he did not believe either of these applied and I accept his assessment.

52. Noteworthy in the description by [this person] of the Director's comments to him during the 2001 inquiry, is the absence of any indication that the Director thought he had anything to hide. Indeed, the contrary is indicated:

*"He said, 'No, provide everything. There's nothing to hide from. Provide everything that's there. The facts will speak for themselves."*

53. I also asked [Mr A] whether the Director approached him on 21 December 1999 or in the days after to suggest a discreet silence or that a certain "line" be taken by both of them about what had occurred on 20 December. He could not recall any such approach. Nor does he believe the Director would "hide anything".

54. Also relevant to [Mr A's account] is the e-mail sent on 20 December 1999 [words deleted] which included:

[Extract from text deleted].

55. [Discussion of credibility]. [Mr A] suggested that [extract deleted]. I interviewed the author of the e-mail and while he could not recall the specifics of the conversation, [rest of sentence deleted].

56. [Discussion of credibility]. But while I am not prepared to accept [Mr A's] specific account of 20 December 1999, I am also not prepared to accept that he acted unilaterally and acted deviously on 20–21 December 1999 (see paragraph 43). [Sentence deleted].

## Statutory Declaration

57. I discussed with [Mr A] whether his statutory declaration of 12 December 2001 was truthful. He argued that the "technical problem" (see the extract in paragraph 47) was that sensitive intelligence might be withdrawn by an outside source unless certain restrictions were introduced within the system to enhance security. I pointed out that word "failing" later in the sentence added to an impression of technical systems failure or fault, rather than a deliberate action.

58. Even if his interpretation of that element of his statutory declaration is accepted—and it was not the one taken by my predecessor or [another named person]—part of the declaration must still be heavily criticised for omission and its apparent deliberate ambiguity.

59. [Mr A] attempted to explain it in these terms:

**IGIS:** *But, at the time that you signed this, did you think that that was a truthful statement or not?*

**[Mr A]:** *It was probably the best result I could get.*

**IGIS:** *Why do you say that?*

**[Mr A]:** *Because between myself and Frank we were the only two people in that room at the time and he did not recall the conversation. It was a technical problem, the security issue."*

60. When I put it to him that Mr Blick and [a named person] read his declaration in the way that I believe most people would, ie. that work to introduce limitations within the system had accidentally caused a technical systems failure, he responded as follows:

*"It might. The words were crafted in such a way that it appeared to be a bit one or the other. For me, it read there was a technical problem, a security problem being a technical problem, resulting in failing. Information from DIO IT they've put basically enhanced security. The word "failing" there, I probably was not all that happy with at the time."*

61. [Mr A] intimated that the statutory declaration had been drafted for him [by a named person] and that some of the final words were not ones with which he was necessarily comfortable. When I put it to him that the final declaration didn't appear to be a truthful statement he responded:

*"Correct, and it wasn't in the original draft I put up."*

62. However, he did not allege that [the person referred to in paragraph 61] was attempting a "cover-up" and I have seen no evidence that there was such an attempt. I questioned [four named persons] closely about the statutory declaration process; and reviewed what electronic records there were about it: I am satisfied the exercise as a whole was not a "cover-up".

63. [The account of a named person] of the finalisation of [Mr A's] declaration is different and one which I accept. He said that he did a first draft (based on discussions with [Mr A], and because [several words deleted] and that [Mr A] had suggested amendments (which were made) and finalised the declaration [several words deleted].

64. I do not consider [Mr A's] attempts at explanation justify what he did. A forthright statutory declaration would have indicated the doubts he had about what occurred; not one which used words meant to ambiguously cover quite different possibilities.

65. [Paragraph deleted]

66. This does not cause me to lessen my criticism. There seems to have been specific attention by [Mr A] to the second paragraph of the statutory declaration (see paragraphs 59–60 above).

## Director's role

67. As concluded earlier, it is plausible—but by no means certain—that there was a brief discussion on 20 December 1999 involving the Director and [Mr A]. However, I do not accept the detail of [Mr A's] version. There is absolutely nothing in the Director's behaviour (at the time or subsequently), which indicates he gave the alleged direction. It does not seem credible—particularly given his personal style—that he would immediately start dissembling on the morning after he had given an instruction of that sort. Even [Mr A] does not assert that (see paragraph 53).

68. Perhaps the discussion was one about the need to introduce some further controls on access to the database, in order to protect certain categories of raw intelligence and to establish communities of interest. Perhaps [Mr A] spoke in general terms of a problem and the Director said "fix it", without the implications being discussed or appreciated. In any case, the important conclusion I have reached, on the evidence, is that the Director did not give an instruction to cut the access of the Dili users.

69. I have reflected on whether the true cause of the loss of access should have been identified on 21 December 1999. The Director submitted to me that there was advice from the IT area that a technical problem was the cause, and he had no reason to query this. He correctly points out that the system had been experiencing a number of technical problems. On the other hand one could argue that senior managers should seek plain English explanations of technical problems, their cause and their likely duration; so assessments can be made of the wider potential ramifications and what it indicates about the state of the IT arrangements. It can be risky to leave it to the experts. And on this morning there was also in front of [people] an allegation that the loss of access had been ordered by the Director. Such an allegation should arguably have prompted some questioning of [words deleted] about what had actually occurred.

70. Hindsight is, of course, extremely accurate; and it must be acknowledged that the main issue on 21 December 1999 was whether there should be access for the Dili users. The attention to this was timely and access was restored that day.

71. I have also reflected on whether the Director should be accountable in a general sense for what occurred. Heads of agencies are not always held "strictly liable" for everything their agency does and says. They are clearly accountable for matters such as governance, influencing culture, and the overall effectiveness of internal controls and internal communication. Whether the Director should be held accountable in a more general sense for what occurred on this occasion can only be judged fairly [by others].

## Conclusions

72. On the basis of my independent investigations, I have reached the following conclusions:

- (a) The denial of access to the relevant Dili users on 20–21 December 1999 was deliberate and not the result of technical failure or technical faults in any part of the system.
- (b) It is possible that the Director and [Mr A] had a brief discussion on 20 December 1999, but I do not accept that the Director gave an instruction to cut the access. [Mr A] later instructed [another person] to effect a denial of access for the relevant Dili users, and this was done.
- (c) [Mr A] may have [made statements in 2001 that potentially raise issues of a legal or administrative nature].

## Recommendations

73. Given these conclusions, I recommend that my report be referred to the Secretary of the Department of Defence for him to consider whether an investigation should be conducted [into issues of a legal or administrative nature].

74. It should be noted that use of the testimony given to me is generally precluded by section 18(6) of the IGIS Act from being admitted as evidence [words deleted] in any court or in any other proceedings before a person authorised to hear evidence. This may have a bearing on what action is reasonably open to the Secretary of the Department of Defence. [Comment on feasibility and desirability of certain actions].

75. Developments since 1999 appear to have overtaken what might otherwise have leant themselves to general recommendations about security policy and practice. These have been enhanced as a result of my predecessor's review of the Wispelaere matter.

Ian Carnell  
Inspector-General of  
Intelligence and Security

