

Australian Security  
Intelligence Organisation

# Report to Parliament

## 2003–2004

© Commonwealth of Australia

ISSN 0815-4562

ISBN 0-9751485-1-6

This document is the property of the Commonwealth of Australia.  
Its contents must not be copied or disseminated.

This is an exempt document under subsection 7(1) of *the Freedom of Information Act 1982*.

Produced and printed by the Australian Security Intelligence Organisation.

**Australian Security Intelligence Organisation**

GPO Box 2176 Canberra City ACT 2601 Telephone 02 6249 6299 Facsimile 02 6257 4501

Office of the Director-General

Reference Number: eA903327  
November 2004

The Hon. Philip Ruddock, MP  
Attorney-General  
Parliament House, Canberra

Dear Attorney-General

In accordance with section 94 of the *Australian Security Intelligence Organisation Act 1979*, I am pleased to submit the Annual Report on ASIO for the year ending 30 June 2004.

The distribution of this classified Annual Report is limited. I also present to you an unclassified version (shorter by about one-third) for tabling in the Parliament.

Yours sincerely

  
Dennis Richardson  
Director-General of Security



## Contents

---

ASIO and its Annual Report .....	ix
PART 1: OVERVIEW .....	1
The Year in Review .....	3
Agency Overview .....	8
PART 2: OUTPUT PERFORMANCE .....	11
Output 1: Security Intelligence Analysis and Advice .....	14
Output 2: Protective Security Advice .....	29
Output 3: Security Intelligence Investigation and Capability .....	36
Output 4: Foreign Intelligence .....	45
PART 3: MANAGEMENT AND ACCOUNTABILITY .....	47
Corporate governance .....	49
Accountability .....	50
Interaction with the public .....	53
Our people .....	54
Information management .....	59
Security of ASIO .....	60
Building management .....	61
Purchasing .....	62
Consultants .....	62
Competitive tendering and contracting .....	62
PART 4: FINANCIAL STATEMENTS .....	65
PART 5: APPENDICES .....	101
A. Membership of the Parliamentary Joint Committee on ASIO, ASIS & DSD ..	103
B. Contact information .....	104
C. Staffing statistics .....	105
D. Workplace diversity statistics .....	106
E. ASIO salary classification structure .....	107
F. Assumed identities .....	108
Glossary.....	109
Compliance Index .....	110
General Index .....	111



## Our Vision

---

The intelligence edge for a secure Australia

## Our Mission

---

To provide advice to protect Australia and its people from threats to national security

## Our Values

---

Accountability

Integrity

Innovation and Learning

Quality

Respect

Responsiveness

Security

Working Together



The Hon. Philip Ruddock, MP  
Attorney-General



Mr Dennis Richardson, AO  
Director-General of Security



## ASIO and its Annual Report

---

### What ASIO does

The Australian Security Intelligence Organisation (ASIO) is Australia's security service. ASIO was established in 1949 and operates under the *Australian Security Intelligence Organisation Act 1979*.

The ASIO Act defines security as protection of Australia and its people from politically motivated violence, including terrorism; promotion of communal violence; espionage; sabotage; attacks on Australia's defence system; and acts of foreign interference. Under legislation, ASIO carries responsibility for these matters 'whether directed from, or committed within, Australia or not.' ASIO also has responsibility for 'the carrying out of Australia's responsibilities to any foreign country' in relation to the same matters.

ASIO provides Government with security intelligence and protective security advice and contributes to Australia's national counter-terrorism response capability. ASIO also collects foreign intelligence within Australia at the request of the Minister for Foreign Affairs or the Minister for Defence.

ASIO's corporate vision, mission and values are contained in its *Corporate Plan 2002–2006*, available on [www.asio.gov.au](http://www.asio.gov.au).

### This report

ASIO produces two versions of its *Annual Report*.

The first version is classified and contains an account of ASIO's performance over the previous year, including sensitive reporting on security risks and details of investigations that cannot be released publicly. That report is provided to the Attorney-General, the Prime Minister, members of the National Security Committee of Cabinet and the Leader of the Opposition.

An abridged *Report to Parliament* is then prepared for tabling in Parliament, excluding classified information in accordance with section 94 of the ASIO Act.



Part 1

# Overview



## The Year in Review

---

Terrorist attacks in Indonesia, Spain, Turkey, Morocco, Saudi Arabia and some in Iraq over the past year underlined the continuing intent and capability of groups such as al-Qa'ida and Jemaah Islamiyah that are driven by an extreme militant interpretation of the Koran.

The overall terrorist threat level in Australia remained at *Medium* throughout the year, and at *High* for Australian interests in much of South-East Asia, South Asia, the Middle East and parts of East Africa. The picture is unlikely to alter significantly any time soon.

That Australia is a terrorist target was brought home by the presence of French al-Qa'ida suspect Willy Brigitte in Australia in 2003 and the attack on the Australian Embassy in Jakarta on 9 September 2004.

Born in the Caribbean, introduced to militant Islam in France and trained as a terrorist in Pakistan, Brigitte embodied the global nature of international terrorism. But for the cooperative work of the French authorities, ASIO, the Australian Federal Police (AFP) and the NSW Police, it is likely that Brigitte and his associates would have carried out a terrorist attack in Australia.

## Role

In the counter-terrorism environment ASIO's role is to contribute to:

- the prevention of terrorist attacks in Australia and against Australian interests overseas
- the identification of people in Australia, and elsewhere, involved with terrorism
- the provision of protective security advice, including for national critical infrastructure
- Australia's counter-terrorism response capability.

## Objectives

In broad terms, ASIO's objectives are to:

- prevent the entry into Australia of people assessed to be connected to terrorism
  - since 11 September 2001, a total of 10 people, including 2 in 2003–04, have been refused entry into Australia because of their assessed involvement in terrorist activities
- where legally possible, prevent the travel overseas of Australians assessed to be involved in terrorist activities
  - since 11 September 2001, a total of 20 (including 6 in 2003–04) Australian passports have been cancelled or denied by the Minister for Foreign Affairs following an adverse security assessment by ASIO (about a million Australian passports are issued each year)

- identify and monitor individuals and groups in Australia with links to terrorists overseas, especially individuals who, themselves, have received terrorist training
  - while small in absolute terms, the number of Australians confirmed or assessed to have undertaken terrorist training continues to grow
- identify and, where lawful, monitor individuals and groups in Australia committed to the militant ideology espoused by the likes of Usama bin Laden and Abu Bakar Bashir
- assist law enforcement agencies in investigations leading to prosecutions for terrorism offences
  - to date, one Australian, Jack Roche in Perth, has been convicted and sentenced for terrorism-related offences
  - four Australians (all in Sydney) are awaiting trial on terrorism offences
    - : other investigations are continuing which could lead to the arrest of other individuals in Australia on terrorism offences
  - one person in Perth is awaiting trial on a charge of conspiracy to murder in Iraq
  - two Australians have been tried and sentenced in absentia for terrorism offences in Lebanon
  - one Australian is awaiting trial in Lebanon on terrorism charges
  - one Australian was released in Lebanon after serving a short sentence on a terrorism-related offence
  - one Australian is in custody in Kazakhstan since being convicted in 2001 of a terrorism offence
  - two Australians are in Guantanamo Bay awaiting trial before a United States Military Commission
- assist overseas liaison partners with investigations where there is an Australian connection, work with our liaison partners in identifying Australians overseas involved in terrorism and work with our liaison partners on matters relating to threats to Australian interests abroad and threats to their national interests in Australia.

## Strategies

In seeking to fulfil our role and meet our objectives, ASIO strategies encompass the following:

- collecting and assessing relevant open source information
  - the establishment in 2002 of a 24 x 7 Research and Monitoring Unit has been central to our efforts in this area
- overt interviews
- surveillance
- the recruitment of agents

- collecting and assessing information through the lawful use of ASIO's special powers
  - such as telecommunications interception and overt and covert enter and search operations
- the lawful application of ASIO questioning and detention powers
  - in 2003–04 ASIO sought and received approval for questioning warrants in respect of three people. ASIO did not seek any detention warrants in the reporting period
    - : the questioning warrants have provided valuable information
  - one person is currently awaiting trial on, among other charges, providing false and/or misleading information under a questioning warrant
- assessments to government about terrorist groups which might be considered for proscription
  - as of 30 June 2004, 17 terrorist groups were proscribed by law in Australia, of which 4 were proscribed in 2003–04
- management of the ASIO component of the Movement Alert List and the provision of security assessments for people seeking entry into Australia and who are referred to us by the Department of Immigration and Multicultural and Indigenous Affairs (DIMIA)
  - in 2003–04, 44 722 visa applications were referred to us, a 12.1% increase over 2002–03
- security assessments for people in government requiring access to national security information
  - 16 206 in 2003–04, a 13.5% increase over 2002–03
  - three qualified, but no adverse, assessments were issued
- security checking in respect of people working in specified areas, such as airports
  - 58 000 checks up to 30 June 2004
- following up National Security Hotline and other public line calls
  - 13 381 Hotline calls were referred to ASIO in the year ending 30 June 2004. Of these, 2602 required the initiation of some investigation, of which 160 were continuing as of 30 June 2004
  - the importance of proper follow up of such calls was demonstrated by ASIO's failure to follow up public line calls by Jack Roche in mid-2000. As a result of that failure our procedures were reviewed and we now have a system of 'fall-back checking' of public calls
- threat assessments for Australia, foreign interests in Australia and Australian interests overseas
  - the establishment of the National Threat Assessment Centre significantly boosted our capability in this area, providing multi-agency coverage 24 x 7
  - over 2000 threat assessments were issued in 2003–04, with a significant increase in those concerning Australian interests abroad

- at the request of the National Counter-Terrorism Committee (NCTC), the development and maintenance of a database of national critical infrastructure assets based on information provided by Commonwealth, State and Territory authorities and by the private owners of such assets
  - 28 critical infrastructure-related threat assessments were produced in the year ending 30 June 2004
- protective security advice to government authorities and, with the Attorney-General's approval, to the private sector
  - with an increase of over 30% in demand for such advice in 2003–04
- sharing information with, and working with, other Australian agencies and our overseas liaison partners
  - cooperative arrangements are working well, reinforced by a strong commitment from senior managers
    - : issues still arise and mistakes occur, but not as a result of destructive competitiveness among agencies
    - : the total flow of information into ASIO has increased fivefold since 11 September 2001
  - ASIO officers are now seconded to a range of other agencies and departments and our overseas representation has also expanded. Within ASIO, officers are seconded from the AFP, the Australian Secret Intelligence Service (ASIS), the Department of Foreign Affairs and Trade (DFAT), the Defence Imagery and Geospatial Organisation (DIGO), the Defence Intelligence Organisation (DIO), the Department of Transport and Regional Services (DOTARS), the Defence Signals Directorate (DSD), the Defence Science and Technology Organisation (DSTO) and the Office of National Assessments (ONA).

## Counter-espionage, counter-proliferation and foreign intelligence

While the overwhelming focus of the Organisation remained on counter-terrorism, both counter-espionage and counter-proliferation remained important, with the latter growing in significance, especially given the known interest of some terrorist groups in acquiring chemical, biological, radiological and/or nuclear capabilities.

ASIO also continued to make a valuable contribution to the collection of foreign intelligence in Australia.

## Budget and people

In order to meet the growing workload the government has increased ASIO's annual budget from \$62.935m in 2000–01 to \$152.7m in 2004–05. This has enabled the Organisation to enhance collection, technical and analytical capabilities and to increase the number of staff from 584 as of 30 June 2001 to 805 as of 30 June 2004. The number of staff will increase further to about 1000 by mid-2006.

ASIO staff numbers grew by 145, or over 21%, in 2003–04. The rapid growth imposed a considerable strain on our recruitment and training/staff development efforts.



Finding the right people in the required numbers has not been easy. Also, the Organisation's growth has contributed to an experience gap, which will grow, at least out to 2006–07:

- at present about 50% of staff have been with the Organisation for five years or less
  - this imposes additional demands on experienced officers and supervisors/managers, who must mentor and lead in a demanding operational environment.

In staff development, we need to further develop leadership skills and the skill sets needed for human source operations.

In addition to the people challenge, the Organisation has numerous initiatives on which to deliver, among the most significant being the need to enhance our information management systems to ensure better integration of data for analysts and collectors.

## Public interaction

Community, business and parliamentary interest in the Organisation's work remained high:

- ASIO continues to face a challenge in gaining confidence across the community, with some believing we unfairly target Australian Islamic communities
- our interaction with the private sector is expanding significantly, reflected at both the working level and at senior management levels
- I appeared before Parliamentary Committees on 10 separate occasions during 2003–04.

## 2004–05

Looking ahead, there will be no let up in the operational tempo or the external environment in which ASIO now works. We will need to continue to manage growth sensibly, ensuring that new staff receive proper training and development and that we deliver on the additional funding provided by government.

Dennis Richardson

Director-General of Security

## Agency Overview

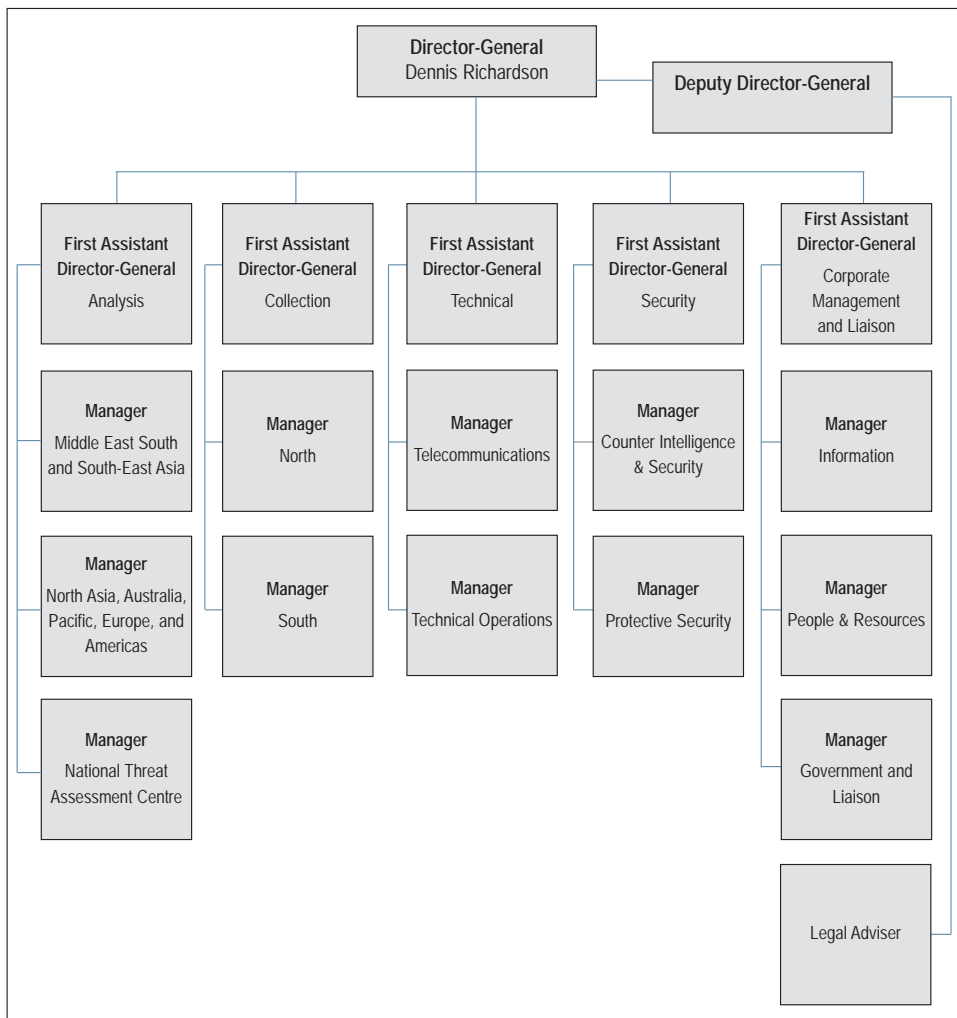
### Organisational structure

ASIO's chief executive, the Director-General of Security, reports to the Attorney-General. The current Director-General, Dennis Richardson, was first appointed in 1996 and was reappointed for a further five years from October 2001.

The multi-agency National Threat Assessment Centre was opened by the Prime Minister on 5 May 2004. Operating 24 x 7, the centre brings together officers from ASIO, AFP, ASIS, DFAT, DIO, the DOTARS and ONA.

ASIO's management structure at 30 June 2004 is at Figure 1.

**Figure 1. ASIO's management structure at 30 June 2004**



## Government Outcome and ASIO's Outputs

ASIO contributes to the Government Outcome – 'A secure Australia for people and property, for government business and national infrastructure, and for special events of a national and international significance' – which supports the Government's policy aim of 'A secure Australia in a secure region'. To support this Outcome ASIO delivers Output Group 1 – Security Intelligence, which includes four Outputs.

### Output 1.1 Security Intelligence Analysis and Advice

This Output includes:

- security intelligence analysis and reporting
- threat assessments
- advice on visa entry and archives issues
- advice on deterrence action
- contributions to the external policy framework.

### Output 1.2 Protective Security Advice

This Output includes:

- advice on personnel security (security clearances)
- advice on physical security, including protective security reporting and risk management
- advice on security equipment standards
- advice on technical surveillance counter-measures
- contributions to the external policy framework.

### Output 1.3 Security Intelligence Investigation and Capability

This Output includes:

- information collection from human and open sources and by technical means
- surveillance capabilities
- counter-terrorism response capabilities
- technical research and development
- deterrence action
- national and international liaison
- contributions to the external policy framework.

### Output 1.4 Foreign Intelligence

This Output includes foreign intelligence collected in Australia at the request of the Minister for Foreign Affairs or the Minister for Defence.

## **Executive Services**

The governance, legal advisory and coordination functions, including high-level coordination and policy advice.

## **Enabling Services**

The corporate functions, including people development and management, financial services, information management, facilities management, internal security and policy advice.

Part 2

# Output Performance



## ASIO's Performance

The performance of ASIO's four Outputs is the focus of Part 2. ASIO's impact on the Government Outcome of 'A secure Australia' is measured by:

- the contribution of ASIO's action and advice to managing and reducing risk to
  - people and property
  - government business and national infrastructure
  - special events of national and international significance
- the security of ASIO's activities.

This section outlines the performance of each of ASIO's Outputs. Funding for 2003–04, expressed in terms of the total price of Outputs, was \$103.023m (compared to \$88.945m in 2002–03).

**Table 1. ASIO funding – price of outputs (\$m)**

Output	Actual 2002–03	Estimated 2003–04	Actual 2003–04	% of total funding
<b>Output Group 1: Security Intelligence</b>	88.945	101.493	103.023	100%

## Counter-terrorism capabilities

In 2003–04 additional funding was provided to ASIO for:

- the establishment of the National Threat Assessment Centre, which operates 24 x 7
- the upgrade of our overseas communications network
- the establishment of a capability to provide security checking advice on Aviation Security Identification Card (ASIC) holders
- additional capacity to contribute to the National Counter-Terrorism Committee (NCTC) training exercises.

## Output 1: Security Intelligence Analysis and Advice

ASIO contributes to the Government Outcome of 'A secure Australia' by providing useful and timely security intelligence analysis and advice on:

- foreign-influenced politically motivated violence including terrorism
- local politically motivated violence
- threat levels in Australia and to Australian interests abroad
- foreign interference and espionage
- protecting critical infrastructure
- visa security checking
- release of archival documents.

ASIO prepares assessments, reports and briefings for government decision-makers and client agencies to help them manage risks and take appropriate steps to protect people, property, and government business and infrastructure.

### Performance

ASIO conducts an annual survey of key clients from Commonwealth departments and police services. In 2003–04, 93.7% of clients surveyed rated ASIO product as almost always or generally useful (Table 2).

In large part, client satisfaction has been positive, although there continues to be the occasional comment on the relevance of some reporting – indicating we need to be more strategic in the targeting of our information – and on timeliness, although this has improved since the previous reporting period.

**Table 2. Client feedback survey – usefulness and timeliness of ASIO product**

	Almost always useful (%)		Generally useful (%)		Sometimes useful (%)		Rarely useful (%)	
	2003	2004	2003	2004	2003	2004	2003	2004
<b>Commonwealth</b>	70	62.4	30	29.3	0	8.3	0	0
<b>Police</b>	71	66.5	29	29	0	4.5	0	0
<b>Total</b>	70.5	64.5	29.5	29.2	0	6.4	0	0

## Threat from foreign-influenced politically motivated violence

Al-Qa'ida and associated groups have regarded Australia and Australian interests as legitimate targets since before 11 September 2001. Continuing reference to Australia in statements by Usama bin Laden and his deputy, Ayman al-Zawahiri, show Australian interests will continue to be at heightened threat for the foreseeable future.



### ***Investigative and analytical priority***

Foreign-influenced politically motivated violence remained our key priority in 2003–04 with investigations into Islamist extremism, including Australian links to al-Qa’ida and Jemaah Islamiyah, absorbing the majority of operational and analytical resources.

During the reporting period four Australians were charged with terrorism offences; the first, Zeky Mallah, in December 2003 with one count of ‘acts in preparation for terrorist acts’ under section 101.6 of the *Criminal Code Act 1995*. Three others – Izhar ul Haque, Faheem Khalid Lodhi (see page 17) and Belal Khazaal (see page 18) – were charged in 2004. All are awaiting trial.

### **Jemaah Islamiyah (JI)**

JI is the regional expression of an extremist religious ideology that supports terrorism to achieve its objectives – similar to that of al-Qa’ida – and is a continuing threat in the South-East Asian region. Australian, US and other Western and regional government entities continue to be at risk of attack. On 27 October 2002 the Australian government proscribed JI as a terrorist organisation under the *Criminal Code Act 1995*.

Regional cooperation between law enforcement and intelligence agencies has continued to disrupt JI operations and terrorist planning activity in the region. But JI retains a high capability to carry out attacks. Key JI identities remain at large and there are indications that JI operatives continue to plan for attacks in Indonesia and elsewhere. Investigations continue to provide information concerning JI–al-Qa’ida linkages, and it is clear that JI is fostering contacts with other terrorist groups.

The suicide bombing attack against the Australian Embassy in Jakarta on 9 September 2004 was almost certainly the work of JI. The failure of the attack to significantly penetrate the secured premises and inflict Australian casualties could influence future JI planning. Australian interests remain at high threat in Indonesia.

Trials of JI members suspected of involvement in the Marriott attack were continuing in Indonesian courts at the end of the reporting period. One JI member, Sardono Siliwangi, was sentenced to 10 years imprisonment and a second, Muhammad Rais, was sentenced on 18 May 2004 to 7 years. On 15 June, Slamet Widodo and Lutfi Fadilah were both sentenced to three years imprisonment for withholding information on an act of terrorism. The trial of Rusman Gunawan, younger brother of Riduan bin Isomuddin, also known as Hambali, began on 21 June. He is charged with helping to finance the Marriott bombing.

More broadly, the threat environment for Australian interests in South-East Asia will remain high for the foreseeable future. JI’s central control and planning is less effective because of increased scrutiny and law enforcement action – but, equally, central coordination is not necessarily a prerequisite for attacks by JI operatives. Attacks may take a variety of forms, with attacks like the Bali and Marriott bombings a continuing threat. Other attacks, such as assassinations, are also possible.

### ***JI in South-East Asia – outlook***

The joint AFP–Indonesian Police criminal investigation into the Bali bombing of 12 October 2002 resulted in the conviction in Indonesia of 33 JI members for the planning and execution of the bombing. Four were sentenced to death, another four were

imprisoned for life, and the remainder received jail sentences ranging from 3 to 16 years. The trial of a 34th JI suspect (Idris) was still underway at the end of the reporting period. In August 2003 JI's operational planner and al-Qa'ida contact, Hambali, was arrested in Thailand and remained under interrogation at the end of the reporting period.

But JI has a history of quickly replacing captured members, helped by porous regional borders, local disputes and conflicts with an ethnic, religious or separatist flavour. And key JI members remain at large, including Dr Azahari bin Husin, Zulkarnaen and Noor Din Top, who are assessed to have had roles in the planning of the Bali bombing.



Hambali

### ***JI in Australia – current status***

JI's presence in Australia has been investigated by ASIO since December 2001 when Singaporean authorities uncovered a plot to attack Western targets in Singapore, including the Australian High Commission. ASIO investigation confirmed a JI support group in Sydney, Perth and Melbourne, under the leadership of Abdul Rahim Ayub, an Australian citizen of Indonesian descent.

### ***Jack Roche***

The trial of Jack Roche, arrested on 18 November 2002 by the AFP on charges of conspiracy to commit offences under the *Crimes (Internationally Protected Persons) Act 1976*, began in Perth on 17 May 2004. The prosecution presented evidence alleging that in 2000 Roche had undertaken reconnaissance of the Israeli Embassy in Canberra and Consulate in Sydney at the direction of al-Qa'ida for a proposed terrorist attack.

On the 10th day of the trial (28 May), Roche pleaded guilty to the charges and on 1 June 2004 was sentenced to 9 years in prison with a 4½ year non-parole period.

In the course of the trial Roche said that he had attempted to contact ASIO in mid-2000 to volunteer information about his travel to Afghanistan and possible Australian links to al-Qa'ida. In sentencing Roche, His Honour Judge Healy said: 'I don't accept those calls [to ASIO] as being evidence necessarily of your withdrawal from the conspiracy' and 'I'm unable to find that you had formed an intention to withdraw when you first rang the ASIO in July and in my view you didn't commence to withdraw until you were ordered to by Abu Bakar Bashir in August.'

But the failure of ASIO to follow up Roche's calls showed up inadequacies in our handling of public line callers. Accordingly, we reviewed and changed our procedures and now have a system of 'fall-back checking' so that appropriate follow-up is assured. This process was instituted in 2003 and has been independently reviewed and validated by a former Inspector-General of Intelligence and Security.

## Usama bin Laden and al-Qa'ida

### *Threat to Australia*

Between the 11 September 2001 attacks and 30 June 2004, Australia was specifically named in five public statements by Usama bin Laden and one by his deputy and mentor, Ayman al-Zawahiri. Australia was also mentioned in media and Internet statements by other Islamist extremists.

In 2003–04 ASIO continued to monitor groups in Australia with links to al-Qa'ida or its affiliates. Identifying Australians or people in Australia who have undertaken terrorist training overseas, or facilitated such training by others, remains a priority.

We contributed to counter-terrorism investigations by liaison partners.

### *Willy Brigitte*

On 22 September 2003 the French security service, the Direction de la Surveillance du Territoire (DST), advised us that French national Willy Virgile Brigitte had participated in military training in Pakistan and/or Afghanistan and that they believed he had travelled to Australia in May 2003. Late on Friday 3 October (Australian time) DST sent a second message advising they considered Brigitte to be 'possibly dangerous'. The communication was actioned on Tuesday 7 October.

ASIO briefed NSW Police and the AFP and on 9 October Brigitte was detained and placed into Immigration custody for breaching his visa conditions. He was interviewed by ASIO and police before his departure, but refused to discuss his activities. He was returned to France under police escort on 17 October.

On arrival in Paris, Brigitte was detained by DST. The French were keen to have him back and we considered they were better placed to question him as their investigation was a lot more advanced than our own.

We continue to work closely with French and other overseas authorities to identify and assess Brigitte's links and intentions in Australia.



Willy Brigitte

It is clear that Brigitte travelled to Australia intending to do harm. As a result of the investigation, two individuals were arrested by the AFP and charged under anti-terrorism legislation. On 15 April 2004, Izhar ul Haque was arrested and charged with training with a proscribed terrorist organisation. On 22 April 2004, Faheem Khalid Lodhi was arrested and charged with terrorism offences and for making false or misleading statements, contrary to Section 34G of the ASIO Act.

### *Terrorism training*

Australian citizens have received terrorism training overseas.

Since 11 September 2001, a total of 20 (including 6 in 2003–04) Australian people assessed or suspected of receiving or facilitating terrorism training overseas have had their Australian passports cancelled or denied by the Minister for Foreign Affairs following an adverse security assessment by ASIO.

## Australians and al-Qa'ida

### **Belal Khazaal**

Belal Khazaal is a Lebanese-born Australian citizen resident in Sydney.

On 2 June 2004 the AFP arrested Khazaal on a terrorism-related offence and charged him under section 101.5 of the *Criminal Code Act 1995* with knowingly collecting or making documents connected with preparation for, the engagement of a person in, or assistance in a terrorist act. Khazaal was released on bail. An appeal against the grant of bail by the Commonwealth Department of Public Prosecutions was unsuccessful – but strict bail conditions were set.

Separately, on 20 December 2003, a Beirut Military Tribunal sentenced Khazaal and his brother Maher in absentia to 10 years imprisonment with hard labour for their involvement with a series of bombings against fast food outlets, liquor stores and supermarkets in Lebanon between May 2002 and April 2003.

Khazaal's Australian passport was cancelled on 1 February 2002 after ASIO issued an adverse security assessment. Khazaal lodged an appeal with the Administrative Appeals Tribunal (AAT), which is yet to be finalised. Maher Khazaal's passport was cancelled on 23 December 2003 on the basis of an ASIO adverse assessment.

### **Omar Abdi Mohamed**

Omar Abdi Mohamed, a Somali national with US residency, visited Australia five times between December 2000 and December 2003.

On 22 January 2004, Mohamed was charged with immigration fraud by US authorities. US authorities have advised that Mohamed was not on any US terrorism watch list when he visited Australia.

### **David Hicks and Mamdouh Habib**

David Hicks, an Australian citizen from Adelaide now in detention at Guantanamo Bay, was captured by the Northern Alliance in Afghanistan and transferred to US custody on 17 December 2001. Hicks was interviewed by ASIO and the AFP in 2001, with ASIO conducting further interviews – one with the AFP – in 2002 and 2003. Hicks was also interviewed by US agencies.

Mamdouh Habib, an Egyptian-born Australian citizen from Sydney, was detained in Pakistan in October 2001 and transferred to Guantanamo Bay in May 2002. He was interviewed by ASIO and the AFP in Pakistan in October 2001 with ASIO conducting further interviews – one with the AFP – in 2002 and 2003.

During the reporting period, ASIO interviewed Hicks and Habib once in November 2003. Hicks and Habib are awaiting trial before a US military commission.

## Proscribed terrorist organisations

Division 102 of the *Criminal Code Act 1995* creates a series of offences relating to terrorist organisations, and provides a means by which identified organisations may be specified in regulations as terrorist organisations for the purposes of the legislation. In 2003–04, ASIO advised the Attorney-General on a number of organisations for this purpose.

The legislation was amended on 10 March 2004 to remove the requirement that an organisation considered for listing must first be identified in a decision of the United Nations Security Council relating wholly or partly to terrorism, or has been identified using a mechanism established under such a decision.

As at 30 June 2004, the Government had listed 17 organisations as terrorist organisations under the Act: Abu Sayyaf, al-Qa'ida, Ansar al-Islam, Armed Islamic Group, Asbat al-Ansar, Egyptian Islamic Jihad, Harakut-ul-Mujahideen, Islamic Army of Aden, Islamic Movement of Uzbekistan, Jaish-e-Mohammed, JI, Lashkar-I-Jhangvi, Salafist Group for Call and Combat, HAMAS's Izz al-Din al-Qassam Brigades, Hizballah's External Security Organisation (ESO), Lashkar-e-Tayyiba, and Palestinian Islamic Jihad; the last four in 2003–04.

## **Terrorist finance investigations**

ASIO continued to undertake financial investigations as an important component of terrorism investigations.

ASIO worked closely with other Commonwealth agencies to implement the *Charter of the United Nations (Terrorism and Dealing with Assets) Regulations 2002*. These are administered by DFAT and were instituted by the Government in response to *UN Security Council Resolution 1373 (2001)*, which requires member states to take measures to suppress terrorist financing. The regulations allow the Minister for Foreign Affairs to list terrorist persons and entities in the *Commonwealth Gazette*.

### **Gazetted entities**

Entities gazetted to date include al-Qa'ida and Taliban-associated persons and entities, JI, the Abu Sayyaf Group, HAMAS, Hizballah, the Liberation Tigers of Tamil Eelam, and a number of Irish, European and South American terrorist entities.

## **Counter-proliferation**

In 2003–04 ASIO focused on identifying attempts by nations and terrorist groups to acquire chemical, biological, radiological and nuclear (CBRN) weapons including related knowledge, technology and equipment.

### **CBRN terrorism**

We provided threat assessment advice and briefings on CBRN terrorism to Commonwealth and State government agencies responsible for emergency management and threat mitigation activities.

Parts of the performance report have been excluded from this unclassified *Report to Parliament* because of security sensitivity.

## Threat from local politically motivated violence

### *Investigative and analytical priority*

Investigation of groups and individuals prepared to use violence to achieve their goals remained a high priority against the background of protests over Australian involvement in Iraq and immigration and education policies.

We continued to liaise closely with Defence agencies on potential threats to Australia's Defence system by individuals or groups. And we provided threat assessments and advice about Defence establishments, personnel, exercises and visiting US navy ships. These assessments informed clients' risk assessments and helped them put in place appropriate response mechanisms.

### Attacks on the Islamic community

There were fewer reported incidents of harassment of Australian Muslims over the last year but incidents occurred, including taunts about being 'terrorists'. There were two incidents against mosques resulting in minor damage – one in Western Australia and another in Sydney.

ASIO maintains contact with Islamic community leaders and works closely with police services in relation to threats and attacks on the Islamic community.

### Threat to Israeli and Jewish interests in Australia

We issued threat assessments relating to threats to Israeli and Jewish interests in Australia, and threats to Australian interests in Israel.

The number of reported incidents of anti-Jewish harassment during the year, including physical damage, threats, anti-Semitic graffiti, hate mail and verbal abuse, was slightly lower than in previous years. Incidents included:

- in August 2003 plastering of the Liverpool Regional Museum building in Sydney with anti-Semitic stickers during its hosting of the Courage to Care holocaust exhibition
- in September 2003 hate mail containing white powder, found to be innocuous, sent to the Jewish Museum in Darlinghurst, Sydney

ASIO maintains regular contact with representatives of the Jewish community and works closely with police services in relation to threats to Israeli and Jewish interests.

Parts of the performance report have been excluded from this unclassified *Report to Parliament* because of security sensitivity.

## Threat from foreign interference and espionage

ASIO investigates covert activity conducted by foreign governments, including espionage and attempts to interfere in the lives of people in Australia or in political processes here or overseas. We advise Government of attempts by foreign intelligence officers to collect sensitive official, military or political information, or scientific and technical equipment and knowledge. We also monitor and report attempts to intimidate people in Australia who are regarded as dissidents by foreign governments.

The performance report was excluded from this unclassified *Report to Parliament* in its entirety.

## Critical infrastructure protection

Critical infrastructure (CI) encompasses systems, facilities and networks which, if destroyed or damaged, would affect the nation's social or economic well-being, or its defence and security capabilities. It includes banking and finance; transport and distribution; energy and utilities; health; communications; delivery of key government services; and government institutions, national symbols and prominent buildings.

Protection of CI has been included in the National Counter-Terrorism Plan. ASIO's role is to assess and advise Government and (where appropriate) the private sector on threats to CI.

### Performance

In accordance with the National Counter-Terrorism Committee's (NCTC) *Principles for a National Counter-Terrorism Strategy for CI Protection*, ASIO developed a database of critical infrastructure assets of national significance.

We prepared 12 threat assessments for critical infrastructure assets identified as nationally 'vital'.

### Aviation security

Aircraft and aviation infrastructure have been targets for terrorist attack for many years. At the request of DOTARS, ASIO has for a number of years provided an annual assessment of the threat to aviation interests in Australia and Australian aviation interests overseas. The current assessment was distributed in July 2003. ASIO also worked with DOTARS in the latter half of 2003 to prepare the first detailed assessment of the threat to Australia's regional and general aviation. This assessment was distributed in December 2003.

In April 2004 ASIO produced a detailed assessment of the threat to Australia's shipping and port infrastructure:

- ASIO, in conjunction with other relevant Australian government departments, briefed state and territory governments and relevant industry representatives
- these threat assessments informed government reviews of aviation and maritime security policy settings.

We continued to engage with the owners and operators of critical infrastructure:

- ASIO is a member of the Critical Infrastructure Advisory Council (CIAC), which is the lead committee for the Trusted Information Sharing Network (TISN)



coordinated by the Attorney-General's Department. The TISN involves business representatives and Governments at all levels working together to ensure the robustness and security of critical infrastructure. We attended meetings of the Industry Assurance Advisory Group (IAAG) chaired by the Attorney-General's Department to help forge ties with appropriate business contacts. We also provided unclassified briefings on the terrorist threat to some IAAG meetings

- we met with private sector owners and operators of critical infrastructure in support of the preparation of threat assessments.

### **Outlook**

In 2004–05 ASIO's priorities will be to:

- review the database of critical national infrastructure
- prepare threat assessments on further 'vital' critical infrastructure assets
- improve processes for disseminating threat information to infrastructure owners in cooperation with other Commonwealth departments and State and Territory police services
- produce threat assessments for other CI sectors such as urban mass transit, land transport, telecommunications, health, banking and finance, food, energy and utilities.

Parts of the performance report have been excluded from this unclassified *Report to Parliament* because of security sensitivity.

## **Threat levels in Australia and for Australian interests overseas**

ASIO is responsible for preparing threat assessments in respect of Australia and Australian interests overseas.

Threat assessments include:

- Australian dignitaries at home and abroad
- foreign dignitaries visiting Australia
- foreign interests in Australia
- Australian interests abroad
- national critical infrastructure
- sites and buildings of national/government significance.

### **National Threat Assessment Centre (NTAC)**

On 17 October 2003, the Government announced the establishment of the NTAC in ASIO, extending existing arrangements for threat assessments to provide a dedicated round-the-clock threat assessment centre which:

- comprehensively monitors and analyses all available threat intelligence and information relating to terrorism
- prepares assessments of the likelihood and probable nature of terrorism and other acts of politically motivated violence.



Limited NTAC operations began immediately following the announcement of the initiative in October 2003 and full 24-hour operations commenced on 3 May 2004. The NTAC draws together staff from ASIO, AFP, ASIS, DIO, DFAT, DOTARS and ONA. DSD has a computer terminal in the NTAC and provides staff as required; there is capacity to involve other agencies as appropriate.

The round-the-clock NTAC presence has allowed a quicker response to emerging threat issues and crises occurring out of hours. The ability of seconded officers to reach back into their home agencies' information systems has also helped speed up the flow of threat information.



The Prime Minister, John Howard, and Attorney-General, Philip Ruddock, opened the NTAC on 5 May 2004

The interagency cooperation on threat assessment is enhanced by the work of the Terrorist Threat Crisis Group (TTCG) a committee chaired by ASIO with representatives of the AFP, ASIS, DFAT, DIGO, DIO, DSD, ONA and PM&C. The TTCG meets weekly to discuss threat assessments and is a mechanism for resolving issues relating to the handling of threats to national security. The TTCG also meets in ad hoc emergency sessions to provide interagency coordination of the intelligence response to urgent and serious threats.

### ***Threat assessments and travel advisories***

Travel advisories – which provide advice on a range of issues, including terrorism, for Australians travelling overseas – are the responsibility of DFAT. NTAC threat assessments are used by DFAT in preparing travel advisories, form a basis for determining the national counter-terrorism alert level, and inform government decision-making about security measures. ASIO and DFAT meet regularly to discuss changes to travel advisories, threat assessments for Australian interests overseas and related matters. DFAT consults ASIO on changes to travel advisories relating to all countries where the assessed threat level to Australian interests is *High*.

- the overall threat level in Australia remained at *Medium* throughout the year. Threat levels for US, UK and Israeli interests in Australia remained at *High*
- the threat to Australian interests in a number of countries in South-East Asia, South Asia and the Middle East remained at *High*
- a major assessment of the threat to oil and gas production and transport infrastructure was produced.

## Performance

Although the number of assessments produced in 2003–04 was similar to the previous year, there was a change in the balance of types of assessment (Table 3). There was a drop in demand for assessments of threats to visiting and Australian dignitaries, reflecting the number of visitors and events requiring such assessments, and an increase in demand for assessments of threats to Australian interests overseas.

**Table 3. Threat assessments issued**

Subject of assessment	1999–00	2000–01	2001–02	2002–03	2003–04
Visiting dignitaries	131	79	237	674	480
Australian dignitaries	552	503	834	739	624
Australian interests overseas	–	122	176	375	559
Protective security	34	27	25	22	35
Demonstration notifications	48	100	193	149	38
Diplomatic premises	164	77	108	55	36
Other threat assessments	75	51	66	29	245
Special events	342	383	147	–	–
WTO	–	–	–	12	–
<b>Total</b>	<b>1346</b>	<b>1342</b>	<b>1786</b>	<b>2055</b>	<b>2017</b>

## Trends

The increase in assessments of threats to Australian interests overseas reflects the changed international security environment generally and the fact that Australia is a declared terrorist target.

Parts of the performance report have been excluded from this unclassified *Report to Parliament* because of security sensitivity.

## Visa security checking

ASIO is the principal source of advice to the Department of Immigration and Multicultural and Indigenous Affairs (DIMIA) on the entry to Australia of people of security significance. The primary objective is to minimise the likelihood of terrorists and other individuals of security concern gaining entry to Australia. ASIO does not conduct assessments of all visa applicants. A risk-management approach is used to identify those people most likely to pose a security risk.

Visa applications are referred to ASIO if the applicant matches a name ASIO has entered into DIMIA's Movement Alert List (MAL) or if the applicant fits one of a

number of profiles. DIMIA and DFAT also refer applications to ASIO if they suspect the applicant may be involved in activities prejudicial to Australia's national security. Where ASIO investigations indicate a security risk we provide a prejudicial security assessment to DIMIA or DFAT, and they deny the visa on security grounds.

In 2003–04, 90% of temporary visa applications and 62% of permanent visa applications were assessed within agreed timeframes. Delays in assessments were largely due to an increase in the number of visa assessments conducted in 2003–04 (Table 4).

### Trends

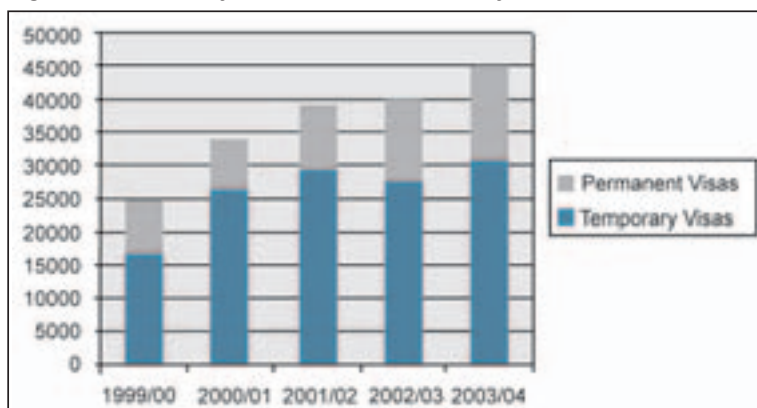
ASIO completed a record number of visa security assessments in 2003–04. We recorded a substantial rise in assessments following the reduced level in 2002–03, which was probably influenced by the Bali bombing, Iraq war and SARS.

**Table 4. Visa security assessments 1999–00 to 2003–04**

Type of entry	1999–00	2000–01	2001–02	2002–03	2003–04
Temporary	16 483	26 527	29 437	27 534	30 841
Permanent	8 371	7 392	9 584	12 355	13 881
<b>Total</b>	<b>24 854</b>	<b>33 919</b>	<b>39 021</b>	<b>39 889</b>	<b>44 722</b>

**Note:** These figures do not include security assessments of unauthorised arrivals held in detention.

**Figure 2: Visa security assessments conducted by ASIO**



### Visa refusals and cancellations

- On ASIO advice two visa applicants were refused entry to Australia because of their assessed involvement in terrorist activities.
- On ASIO advice one visa applicant was refused entry to Australia because the applicant was assessed as likely to engage in espionage activities.

**Table 5. Prejudicial security assessments for visa applicants 1999–00 to 2003–04**

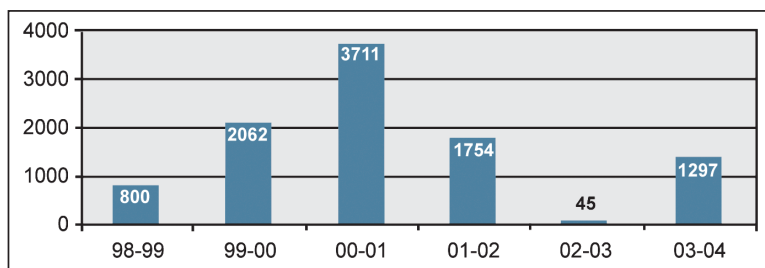
	1999–00	2000–01	2001–02	2002–03	2003–04
<b>Prejudicial assessments</b>	4	5	5	8 <sup>(1)</sup>	3

<sup>1</sup>The total includes one diplomat expelled on advice from ASIO.

### Unauthorised arrivals

Only one unauthorised boat arrived in Australia during 2003–04, and all passengers were repatriated to Indonesia. There were 14 unauthorised arrivals by air and 11 stowaways.

Unauthorised arrivals granted three-year Temporary Protection Visas require a new assessment prior to being granted a Further Protection Visa. In 2003–04 ASIO reassessed 1297 unauthorised arrivals whose original security assessments had lapsed or had been resubmitted for further consideration. There were no adverse assessments. DIMIA and ASIO continue to work closely together to ensure timely processing and assessment of these cases.

**Figure 3: Security assessments – unauthorised arrivals**

Parts of the performance report have been excluded from this unclassified *Report to Parliament* because of security sensitivity.

## Release of archival documents

ASIO is an exempt agency under the *Freedom of Information Act 1982*, but is a participating agency in relation to release of its records under the *Archives Act 1983*.

### Access to records

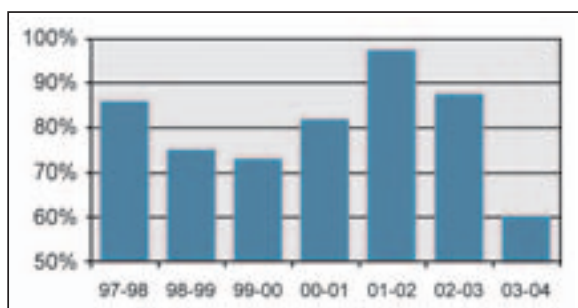
Members of the public can apply to the National Archives of Australia for access to ASIO records that are at least 30 years old (described as the open access period). When the National Archives does not already hold records on the subject it passes the access applications to ASIO. We locate and assess relevant records and provide advice to the National Archives about whether they contain information that should be exempted from public release under section 33 of the *Archives Act 1983*. ASIO only recommends exemptions where disclosure of the information could damage national security or expose the existence or identity of a confidential source. We balance the commitment to release information with the need to protect national security.

Only in rare cases is ASIO informed of the identity of the applicant. The National Archives usually only takes this step to facilitate contact between ASIO and the applicant where greater information is needed to identify the relevant records or where the applicant has lodged a large number of applications which ASIO needs to prioritise. ASIO does not investigate or open files on applicants/researchers.

### **Performance**

In 2003–04, 60% of applications due to be completed were finalised within 90 days, against a benchmark of 80%. This reflects the impact of the large numbers of applications lodged in the last 16 months and the need to commit resources to other priorities. The impact of several large requests lodged by a small number of researchers in this period and in the last reporting period is also reflected in the lower completion rate. One researcher lodged 54 applications in 2003–04 while another lodged 83 applications in 2002–03. Owing to the size and complexity of the tasks involved, many applications could not be completed within 90 days.

**Figure 4. Percentage of archival requests satisfied within 90 days**



### **Trends**

We received applications for access to 307 separate items or subjects which were due to be completed in 2003–04 compared to 244 in the previous year, 296 in 2001–02 and 231 in 2000–01.

- With the agreement of the Inspector-General of Intelligence and Security, ASIO gives priority to requests from people seeking records on themselves or members of their family. Some 121 family requests were due for completion in the last financial year (compared to 92 in the previous year and 132 in 2001–02). Of these, 94.75% were completed within 90 days (compared to 96.75% last financial year and 99% in 2001–02), against a benchmark of 100%.
- Some 13.25% of applications were for items that were not recorded in our indexes (compared to 9% last year).
- Many requests related to ASIO's records on war criminals, anti-apartheid and Vietnam moratoriums/public order demonstrations.
- Several large requests from individual/non-family researchers were also received. In some cases special arrangements were made to accommodate these requests. Similar requests from researchers lodged last year continued to be processed during this financial year.

The total number of folios (pages) examined was 32 708, compared to 19 382 in the previous year and 30 550 in 2001–02. Table 6 shows the distribution of exemption decisions made with respect to these folios.

**Table 6. Distribution of exemption claims across assessed folios**

Subject of assessment	2000–01	2001–02	2002–03	2003–04
Folios released without exemption	28%	31%	33%	35%
Folios released with part of text claimed as exempt	58%	57%	56%	58%
Folios claimed as totally exempt and not released	14%	12%	11%	7%
Total folios assessed	100%	100%	100%	100%

The number of folios claimed as exempt or with exemptions can vary in response to the types of files examined. For example, policy files typically have a much greater percentage of documents released without exemption than do files relating to ASIO's human sources.

## Appeals

Applicants who are dissatisfied with exemptions claimed by ASIO can request an internal reconsideration of the decision. This process is undertaken in conjunction with the National Archives. Applicants still dissatisfied may then appeal to the AAT, which may uphold the original decision or grant access to all or part of a previously exempted record. One appeal from the last reporting period was settled before going to hearing. No appeals were lodged in the reporting period.

Five internal reconsiderations were actioned within the reporting period. One was outstanding from the last reporting period – it was also the subject of the only appeal to the AAT last year. One was lodged by a researcher who did not believe ASIO held as little information on him as the initial assessment revealed. Two were lodged by one applicant who did not believe ASIO did not have any records on the two subjects on which he had requested information. In all three cases further searches of our databases did not produce additional information.

Parts of the performance report have been excluded from this unclassified *Report to Parliament* because of security sensitivity.

## Output 2: Protective Security Advice

---

ASIO advises Government departments and agencies on the protection of Government business and national infrastructure.

Output 2 contributed to the Government Outcome of 'A secure Australia' by:

- providing advice on personnel security (security assessments for people requiring access to classified national security information or secure places) and administrative security practices
- providing advice on physical security (the security of government buildings and infrastructure), including electronic 'sweeping' of sensitive areas to protect against unauthorised monitoring of government meetings.

## Security in Government

### *Inter-Agency Security Forum*

ASIO continues to manage the Inter-Agency Security Forum (IASF), which was formed following the Government's endorsement of the *Inquiry into Security Issues* recommendations in 2000. The IASF has representatives from PM&C, Treasury, Defence, DFAT, Attorney-General's, DIMIA and the Australian Intelligence Community (AIC) agencies. Having moved beyond the implementation of recommendations from the inquiry, the IASF continues to drive the development and implementation of enhanced protective security policies and procedures across the AIC and related policy departments. New security initiatives implemented in 2003–04 include:

- production of a guide to assist IASF members with the development of agency-specific security plans
- production of the first annual *Emerging Issues in Protective Security* paper, which informs the forward work program for the IASF.

### *Status of Security Report*

IASF agencies are required to submit an annual security status report to PM&C for consideration by the Secretaries Committee on National Security and the National Security Committee of Cabinet, detailing protective security issues relevant to the AIC and other departments and agencies that handle large volumes of classified national security material. In addition to producing its own *Status of Security Report*, ASIO is responsible for producing an overview report on behalf of IASF members.

ASIO's *Status of Security Report* and the IASF overview report were completed in August 2003.

## Personnel security

Before granting a security clearance for designated positions, Commonwealth agencies are required to assess candidates' general suitability for access. ASIO then



provides a security assessment advising whether anything in a candidate's background or activities is a cause for security concern. This advice is usually based on an assessment of material provided by the requesting agency, but ASIO may also interview people to resolve security issues. Any psychological testing is the responsibility of the agency and does not involve ASIO.

ASIO will either advise the agency that it does not recommend against a candidate or will issue an adverse or qualified assessment.

- An adverse assessment is a recommendation that a person should not be granted the access proposed.
- A qualified assessment does not recommend against access, but provides information for the agency to consider in decision-making. Qualified assessments also provide the agency with information to help minimise the potential for the compromise of sensitive information.

The decision to grant or deny a security clearance rests with the requesting agency.

## Performance

Performance was affected by the number of security assessment requests received and the temporary loss of some assessment officers to higher priorities. Output improved in the second half of the year, with 85% of requests completed within three weeks, just outside the benchmark, for the last five months.

**Table 7. Personnel security assessments – performance against benchmarks**

Performance measure	Target	Performance			
		2000–01	2001–02	2002–03	2003–04
Complete within 14 days	75%	14.7%	74.7%	56.3%	22.6%
Complete within 21 days	90%	15.3%	86%	66.1%	44.5%
Incomplete after 12 weeks	1%	55.4%	1.3%	1.4%	1.7%

## Appeals

Individuals have a right of appeal to the AAT in respect of an adverse or qualified ASIO security assessment. No appeals were lodged in 2003–04. An appeal against an adverse security assessment issued in 2001–02 was heard and the assessment upheld. Two other appeals from 2001–02 were also heard, one against a qualified assessment and the other against an adverse assessment. The tribunal upheld the ASIO assessments in both cases. An appeal lodged in 2002–03 against a qualified assessment was withdrawn following mediation.

## Trends

ASIO received 16 206 requests for security assessments, a 13.5% increase on 2002–03. Increases seen in 2002–03 and 2003–04 were caused by Department of Defence efforts to reduce its security clearance backlog and an increase in clearances needed for government employees working on counter-terrorism issues.



Table 8. Personnel security assessments – annual workloads

Level of access	1998–99	1999–2000	2000–01	2001–02	2002–03	2003–04
Confidential	1038	1163	969	1431	1542	1611
Secret	5909	6658	5803	6595	7618	9577
Top Secret	4453	4650	4335	4329	5112	5018
Total	11 400	12 471	11 107	12 355	14 272	16 206

### *Adverse and qualified assessments*

Two qualified assessments and no adverse assessments were issued (Table 9).

Table 9. Adverse and qualified personnel security assessments

	1999–00	2000–01	2001–02	2002–03	2003–04
Qualified assessments	12	10	6	3	2
Adverse assessments	1	2	3	2	0
Total	13	12	9	5	2

The reduction in prejudicial assessments issued in recent years is not a result of changes in policy or procedures.

### *Vetting for the AIC*

The *Inquiry into Security Issues* recommended that where an appointment to the most senior levels of an agency is dependent on a positive vetting security clearance, or where revalidation is required, the vetting process must be conducted by a suitably qualified agency, for which the vettee has no managerial responsibility. As a result of this recommendation, ASIO now undertakes some TSPV clearances for ASIS, Defence, DIMIA and ONA.

### *Aviation and maritime security*

In November 2003 ASIO commenced security checks on Aviation Security Identification Card (ASIC) holders as part of Government initiatives to enhance aviation security. A reissue of all existing ASIC cards incorporating the ASIO security check was to be completed by 30 June 2004, but was extended until 31 August. ASIO completed 58 000 checks by the end of June and 67 000 checks by the end of August – 2000 more than the estimated number required. While a number of investigations were undertaken, no adverse or qualified assessments were issued.

Security checking for ASICs is continuing for new card holders and will include employees at additional airports as the aviation security program is expanded.

Another aviation security initiative is the security checking of pilots and trainee pilots not covered under the ASIC scheme. This commenced in July 2004 and involves an ASIO check, as is done for ASICs.

A review of maritime security policy settings by the Secretaries Committee on National Security recommended a maritime security identification card be introduced for people working in the maritime industry, along the lines of the ASIC scheme. This has been agreed and ASIO will work with government and the maritime industry to see its implementation in 2005.

Computer equipment was upgraded to meet the extra workload of ASIC checking, business processes were refined and software specifications were developed to improve the speed and reliability of the checking process. At the end of the year new searching and matching software was being tested prior to implementation. Funding for IT improvements was provided in the 2002–03 budget while the ongoing costs of security checking for ASICs is funded through cost recovery. Other background security checking will also be on a cost-recovery basis, with budget funding sought to increase IT capacity to meet the checking volume.

### ***Ammonium nitrate security***

In June the Council of Australian Governments agreed on a national approach to ban access to ammonium nitrate for other than authorised users. Each jurisdiction is establishing a licensing scheme, which will include an ASIO security check, to enforce this decision.

### ***Polygraph trial***

ASIO has completed the polygraph trial and will present a report to the Government in 2004–05.

### ***Contact reporting***

ASIO continues its coordination and management of the Commonwealth Contact Reporting Scheme with the aim of identifying attempts by hostile foreign intelligence services to acquire information relevant to national security. The scheme requires people working for, or on behalf of, the Commonwealth, both within and outside Australia, to report any unsolicited or suspicious contact or encounters with foreign government officials. Additional staff appointed in early 2004–05 will enhance this program.

## **Protective security advice**

ASIO provides protective security policy advice to government, and specific advice to departments and agencies, including:

- protective security risk reviews and risk management advice
- physical security advice about access control systems, perimeter security, locks and alarms, CCTV systems and security containers, security of new buildings, security audits and guarding arrangements
- development of security plans
- certification of the security measures for Top Secret facilities
- security equipment evaluation and testing, and production of the *Security Equipment Catalogue*
- specialised protective security training
- technical surveillance counter-measures (electronic sweeps).

With the approval of the Attorney-General, ASIO also provides protective security advice to non-Commonwealth agencies, including State and Territory agencies and owners of critical infrastructure.

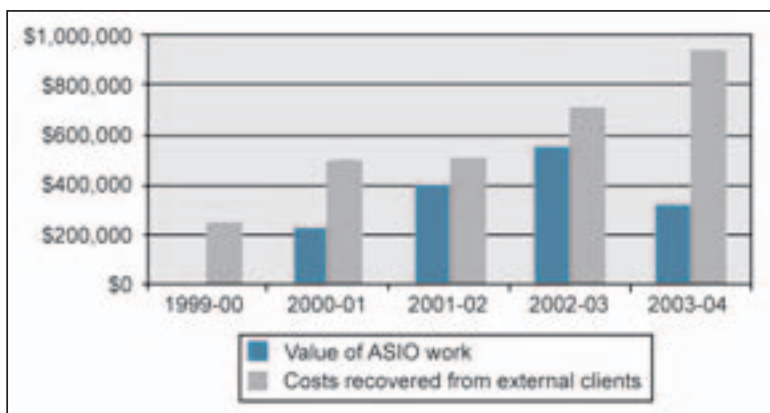
## Cost recovery

### Performance

ASIO's protective security advice and services are provided on a cost recovery basis. In 2003–04, \$923 045 was recovered from clients, a 31% increase on 2002–03. Demand for ASIO's protective security advice continued to increase in response to the heightened security environment, particularly in relation to critical infrastructure protection.

As a major review of the security of ASIO offices had been conducted in the previous reporting year, fewer tasks were undertaken within ASIO, for which notional charges of \$313 179 were attributed.

**Figure 5. Protective security – value of ASIO work and external work**



## Protective security and risk management advice

In response to the heightened terrorist threat environment, ASIO's protective security focus was increasingly on protection of government business, government employees and critical infrastructure. This work was balanced against the more traditional provision of advice on protection of government information.

Particular areas of growth included risk reviews and security audits, development of security plans, and protection of critical infrastructure assets and repositories of materiel that could be used in chemical, biological, radiological or nuclear terrorist attacks.

Significant contributions to improved security across government and key elements of Australia's critical infrastructure included:

- risk reviews for the NSW EPA Radioactive Waste Repository, uranium ore concentrate mines and associated transport facilities, the Department of Education, Science and Training, the Australian Bureau of Statistics and the Treasury
- security audits of selected overseas missions on behalf of the Australian National Audit Office

- physical security advice on South Australian Water's water treatment and storage assets and on the Northern Territory Work Health Authority's explosive storage facilities
- a review of physical and procedural security for the Australian Crime Commission.

### ***Top Secret certification***

Thirty-three Top Secret (TS) facilities within Australia were inspected during 2003–04. Twenty-one facilities were certified, and the remainder were provided with reports detailing physical security improvements required to meet minimum standards for TS certification. Re-certification of facilities is required every five years or following significant structural changes.

TS certification inspections were provided to commercial companies required to secure classified information acquired in their dealings with government agencies, including Raytheon Lockheed Martin and BAE Systems. Other levels of certification were provided to government and private sector agencies, including Highly Protected sites, SATIN High sites and IT providers.

### ***Accredited Locksmith Scheme***

ASIO, on behalf of the Interdepartmental Security Construction and Equipment Committee (SCEC), tests and accredits locksmiths to maintain manifoil combination locks and fit locks on secure area doors. During 2003–04 ASIO accredited 16 new locksmiths and arranged for a TAFE college in Brisbane to provide training in the maintenance of specific locks.

### ***Safehand and overnight couriers***

On behalf of the SCEC, ASIO endorses safehand and overnight courier services to securely transport classified information. During 2003–04, four additional companies were endorsed.

### ***Protective security training***

Independent security consultants and security equipment manufacturers were provided with training in the security standards required by government, with particular emphasis on high-grade security systems. Completion of this training results in endorsement by the SCEC and will contribute to improved security across government as agencies use endorsed consultants to design, oversee installation, commission and certify best-practice security systems.

ASIO provided lectures on protective and physical security and general security threats to Protective Security Coordination Centre (PSCC) training courses, and provided risk management training to the Navy.

Combination lock maintenance courses were provided to Defence Force personnel to enable them to service these locks in operational circumstances.

### ***Gatekeeper/PKI accreditation***

Gatekeeper/Public Key Infrastructure (PKI) accreditation permits private sector companies to undertake processing of non-national-security data on behalf of government agencies. Demand for accreditation remained steady, with one IT company certified through a joint ASIO–DSD program in 2003–04. ASIO provided advice to three other companies seeking DSD Gatekeeper accreditation.

## Security equipment standards

### *Security Equipment Catalogue*

ASIO, on behalf of the SCEC, tests and evaluates a wide range of security products to determine suitability for use in government departments and agencies. Endorsed products are published in the *Security Equipment Catalogue*. A revised catalogue was prepared for release in July 2004.

### *Equipment testing*

Twenty-four security products were evaluated by ASIO in 2003–04, including:

- biometric access control readers, fingerprint readers and iris recognition systems
- security fencing and intruder detection systems
- demountable B-Class rooms, security doors and secure containers
- glazing products
- electronic and mechanical combination and mortice locks
- secure pouches and briefcases, safehand bags, wafer seals and document shredders.

### **Technical surveillance counter-measures (TSCM)**

ASIO conducts physical and electronic surveys ('sweeps') and monitors government offices and meeting rooms to protect sensitive and classified discussions from unauthorised monitoring.

Parts of the performance report have been excluded from this unclassified *Report to Parliament* because of security sensitivity.

## Output 3: Security Intelligence Investigation and Capability

---

To investigate threats to national security ASIO must develop and maintain specialised human and technical capabilities in a continually changing security and operational environment.

Output 3 is delivered through a range of integrated activities; each is a key contributor to ASIO's security intelligence collection capability. These include:

- counter-terrorism response capabilities
- warrant operations, which may include
  - computer access
  - telecommunications interception
  - overt or covert entry and search of premises
  - interception of postal and delivery service articles
  - the use of listening devices and tracking devices
  - ASIO questioning/detention warrants.
- human source intelligence collection
- surveillance
- collection of information from open sources
- liaison with other Australian stakeholders
- liaison with overseas security and intelligence partners
- technical research and development.

ASIO operational activity must comply with the Attorney-General's *Guidelines for the Collection of Intelligence*, which require ASIO to use only methods of investigation that are appropriate to the assessed risk. The guidelines are available on ASIO's website.

### Performance

Output 3 contributed to the Government Outcome of 'A secure Australia' by:

- investigating threats to security – particularly threats from terrorism and other forms of politically motivated violence – to contribute to Output 1 (Security Intelligence Analysis and Advice) and Output 2 (Protective Security Advice)
- maintaining and enhancing investigative capabilities.

A large part of the performance report has been excluded from this unclassified *Report to Parliament* because of security sensitivity.

## Legislative amendments

### ASIO Legislation Amendment Act 2003

In response to practical issues identified in planning and executing questioning warrants the ASIO Act was amended in December 2003 by the *ASIO Legislation Amendment Act 2003* (the Amendment Act).

The questioning regime was enhanced by:

- extending the maximum time available for questioning where interpreters are used
- minimising the possibility of flight risk by making it a criminal offence if the subject of a warrant leaves Australia after being notified of the issuing of a warrant or if the subject fails to hand over all passports issued to them
- inserting secrecy provisions, which prohibit
  - (i) while a warrant is in force, disclosure of the existence of the warrant and any fact relating to the content of the warrant or to the questioning or detention of a person under the warrant
  - (ii) while a warrant is in force and during the period of two years after the expiry of the warrant, disclosure of any ASIO operational information acquired as a direct or indirect result of the issue of a warrant, unless the disclosure is a permitted disclosure
- clarifying the ability of the prescribed authority to direct, in limited circumstances and where the warrant authorised questioning only, that the subject of a questioning warrant be detained.

The Amendment Act was passed by Parliament on 5 December 2003, received Royal Assent on 17 December 2003 and commenced on 18 December 2003.

### ***Telecommunications (Interception) Amendment Act 2004***

The *Telecommunications (Interception) Act 1979* was amended in April 2004.

Two of the amendments related to ASIO. They were to:

- exclude from the definition of interception the acts of listening to, recording, reading or viewing communications to publicly listed ASIO numbers
- remove the requirement for the Director-General of Security to advise the Managing Director of a carrier of the issuing of a warrant, and to give the Managing Director a copy of the warrant, if the execution of the warrant does not involve the taking of action by the carrier or its employees.

The *Telecommunications (Interception) Amendment Act 2004* received Royal Assent on 27 April 2004 and commenced on 28 April 2004.

## **Counter-terrorism response capabilities**

ASIO is a member of the two major committees coordinating Australia's counter-terrorism capability:

- the National Counter-Terrorism Committee (NCTC)
- the Australian Government Counter-Terrorism Committee (AGCTC).

ASIO is involved at every level of Australian Government counter-terrorism arrangements. Under the National Counter-Terrorism Plan (NCTP):

- we help prevent terrorism through intelligence collection and reporting, and by participating in counter-terrorism training courses and exercises
- we actively respond to terrorist incidents through intelligence collection and reporting, managing the National Intelligence Group (NIG), which coordinates intelligence collection and strategic assessments during a terrorist incident, and providing intelligence support to States and Territories
- we contribute to counter-terrorism policy development and crisis contingency planning, including the protection of Australia's critical infrastructure.

### ***Support to the NCTP***

In 2003–04 ASIO was one of a number of agencies involved in developing the new *National Counter-Terrorism Handbook* which supplements the NCTP.

### ***National counter-terrorism exercises and training***

In 2003–04 ASIO participated in the inaugural NCTC Multi-Jurisdictional Exercise (MJEX), MERCURY 04, in Tasmania, Northern Territory, South Australia and Victoria, deploying intelligence support to all jurisdictions and activating the NIG. ASIO also participated in two State-based counter-terrorism exercises in New South Wales and Queensland, and three nationally coordinated counter-terrorism training courses (one in each of Victoria, the Northern Territory and New South Wales).

ASIO is part of the DFAT-led Inter-departmental Emergency Task Force (IDETF) arrangements for responding to a terrorist incident overseas involving Australia or Australian interests. ASIO maintains a capability to support these arrangements through hosting an intelligence coordination centre and deploying intelligence support overseas. ASIO participated in the Counter-Terrorism Overseas Response Group (CTORG) exercise in New Zealand in September 2003.

### ***Technical Support Unit (TSU)***

ASIO's TSU can be called on to assist the AFP and State and Territory police manage a terrorist incident. It provides technical support to the police commander managing the incident and to police technical units gathering intelligence at the scene. The TSU is maintained in a high state of readiness and is regularly involved in counter-terrorism exercises.

In March 2004 TSU staff were deployed to the MJEX in Tasmania and the Northern Territory to assist State and Territory police technical units.

## **Warrant operations**

### ***Special powers***

Legislation enables ASIO, subject to a warrant approved by the Attorney-General, to use intrusive methods of investigation such as telecommunications interception, listening devices, entry and search of premises, computer access, tracking devices, and the examination of postal and delivery service articles.



### ***Warrant approvals***

Only the Director-General can seek a warrant. A written statement, specifying the grounds on which it is considered necessary to conduct an intrusive investigation, must accompany each warrant.

Warrants submitted for the Attorney-General's approval go through a system of checks within ASIO, including examination by ASIO's Legal Adviser. A senior official of the Attorney-General's Department independently advises the Attorney-General on whether the statutory requirements have been met.

The legislation also enables ASIO, subject to the Attorney-General's consent, to seek warrants for questioning people for the purposes of investigating terrorism, from an independent issuing authority (a Federal Magistrate or Judge). The warrants may authorise police officers to detain people in limited circumstances.

Any questioning under a warrant must be undertaken in the presence of a prescribed authority (a former or serving senior Judge, or the President or Deputy President of the Administrative Appeals Tribunal) under conditions determined by that authority. The Inspector-General of Intelligence and Security may attend during any questioning or detention under the warrant.

Warrants are issued for specified periods. At the expiry of each warrant ASIO must report to the Attorney-General on the extent to which the operation helped ASIO carry out its functions. The Inspector-General of Intelligence and Security has access to all warrant material and regularly monitors the process.

The number of warrants varies over time, in response to the changing security environment.

### ***Security intelligence warrants***

All warrant requests put to the Attorney-General in 2003–04 were approved, although some proposals were rejected or modified before they were submitted to the Attorney-General as part of the normal consideration of warrant requests within ASIO.

### ***Emergency warrants***

The Director-General may issue warrants for up to 48 hours in emergency situations. The Attorney-General is to be advised of any such warrants.

### ***Questioning warrants***

Questioning warrants enhanced ASIO's capability in 2003–04 by authorising the questioning of people for the purposes of investigating terrorism. During the period ASIO executed three warrants under its new powers.

The following information is provided in accordance with the reporting requirements of section 94(1A) of the ASIO Act:

- (a) the number of requests made under section 34C to issuing authorities during the year for the issue of warrants under section 34D: 3
- (b) the number of warrants issued during the year under section 34D: 3

- (c) the number of warrants issued during the year that meet the requirement in paragraph 34D(2)(a) (about requiring a person to appear before a prescribed authority): 3
- (d) the number of hours each person appeared before a prescribed authority for questioning under a warrant issued during the year that meets the requirement in paragraph 34D(2)(a) and the total of all those hours for all those persons:

Person 1	Person 2	Person 3	Total hours
15 hours 57 minutes	10 hours 32 minutes	42 hours 36 minutes (interpreter required)	69 hours 5 minutes

- (e) the number of warrants issued during the year that meet the requirement in paragraph 34D(2)(b) (about authorising a person to be taken into custody, brought before a prescribed authority and detained): 0
- (f) the number of times each prescribed authority had people appear for questioning before him or her under warrants issued during the year: 3 people appeared before the same authority for questioning.

### External scrutiny

The Inspector-General of Intelligence and Security examines and audits all ASIO warrant documentation. The Inspector-General's *Annual Report* can be found at [www.igis.gov.au](http://www.igis.gov.au).

## Telecommunications interception

Telecommunications interception (TI) requires the establishment and maintenance of:

- interception capabilities within the networks or facilities of telecommunications carriers and carriage service providers (C/CSPs)
- delivery capabilities to transmit the intercepted communications to ASIO monitoring facilities
- processing and monitoring capabilities within ASIO offices.

The *Telecommunications Act 1997* requires all C/CSPs, including Internet service providers (ISPs), to develop, install and maintain interception capabilities unless specifically exempted. C/CSPs bear the costs of these capabilities. The Act also requires C/CSPs to develop, install and maintain delivery capabilities to enable the intercepted communications to be transmitted to the monitoring facilities of ASIO and law enforcement agencies. C/CSPs are able to recover these costs from ASIO and law enforcement agencies. Agencies must develop and maintain their own processing and monitoring capabilities.

ASIO has a 'lead house' role in developing interception and delivery capabilities for use by Commonwealth and State law enforcement agencies as well as ASIO.

### ***The commercial environment***

Continued growth in the number of C/CSPs has required significant investment by ASIO. Since 1995, the number of licensed carriers in Australia has increased from 3 to 133, of which 105 remain current. There are now approximately 800 CSPs (including some 670 ISPs).

### ***Contribution to policy***

As part of its 'lead house' role, ASIO continued to work with the Attorney-General's Department in developing TI-related policy.

ASIO provided comment and input to development of legislation affecting TI, including the Communications Legislation Amendment Bill (No. 2) 2003, Telecommunications (Interception) Amendment Bill 2004, Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 and amendments to the *Crimes Act 1914* in relation to telecommunications offences. ASIO provided a submission to the Senate Legal and Constitutional Legislation Committee Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2004. ASIO also commented on the *Report of the Review of Named Person Warrants and Other Matters*.

## **Human source intelligence collection**

In addition to the overt collection of information through declared interviews of members of the public or people under investigation, ASIO obtains information from human sources. These are people who are recruited and managed by ASIO to obtain information of security interest about individuals, groups or foreign intelligence organisations.

A well-placed human source can provide ASIO with valuable and unique intelligence, but can take substantial time and resources to recruit, train and manage. Developing and maintaining effective human source coverage of target activity is crucial to our collection capacity, as is developing the human source management skills of our intelligence officers.

### ***Human source management issues***

Managing human sources can be a difficult and time-consuming activity. ASIO regularly reviews its human source base to ensure cases are managed effectively and are appropriately targeted.

## **Surveillance**

ASIO surveillance teams report on people of security interest. This includes identifying the movements, contacts and activities of targets and assisting in the execution of other covert operational action.

We have expanded our surveillance capacity by recruiting and training new surveillance officers. This expansion will continue during the next reporting period.

## **Open source information collection**

ASIO makes extensive use of open source information for its analysis and reporting activities. Unclassified information, from hard-copy and electronic sources, provides a valuable adjunct to covert intelligence collection.

### **Research and Monitoring Unit**

The Research and Monitoring Unit (RMU) operates 24 x 7 and focuses on:

- timely identification of critical classified and unclassified information that is pertinent to ASIO assessments about, and responses to, the global security environment
- provision of research services drawing on unclassified publications and electronic sources as an adjunct to covert collection strategies.

The RMU also produces a daily unclassified compilation of security reporting to raise counter-terrorism awareness in relevant Commonwealth and State agencies.

Strong demand for open source research services continued, especially after the commencement of NTAC operations, reflecting the value of unclassified material in ASIO's work. To better manage the volume of public domain information relevant to ASIO, particularly on the Internet, the RMU trialled several new software applications. These applications are expected to be in production in 2004–05.

### **National Security Hotline**

The National Security Hotline, established in December 2002, had referred 13 381 calls to ASIO by 30 June, of which 2602 contained sufficient information to initiate investigations; 160 were still being pursued at the end of the reporting period.

## **Liaison with Australian agencies**

ASIO's engagement with Federal, State and Territory police and other law enforcement agencies continued to expand in 2003–04 on counter-terrorism investigations, threat assessments and protective security issues, including critical infrastructure protection.

### **Police**

Each ASIO office maintains weekly or fortnightly management-level meetings with police to coordinate major investigations and discuss emerging threats, as well as, in many cases, a daily exchange at the working level on intelligence matters. Coordination of National Security Hotline calls was the focus of regular liaison in all jurisdictions to ensure effective follow-up of leads. ASIO senior managers meet regularly with senior police about the security environment, emerging policy issues and major investigations.

In New South Wales ASIO worked closely with NSW Police and the AFP on the Willy Brigitte investigation, including sharing intelligence, surveillance and other operational and investigative resources. Both police agencies assisted in the entry and search operations, conducted under ASIO warrants, in connection with the investigation.

ASIO provided intelligence support and staff for counter-terrorism exercises as well as input on the security environment for police training courses.

State and Territory police in all jurisdictions continue to provide important assistance and input by sharing information on individuals of security interest, accompanying ASIO officers on selected interviews, and providing logistical and surveillance assistance.

The increasing incidence of ASIO information and staff being involved in the support of prosecutions has required careful management to achieve law enforcement outcomes while protecting the identity of ASIO officers and sources and methods.

### ***Joint Counter-Terrorism Intelligence Coordination Unit***

The Joint Counter-Terrorism Intelligence Coordination Unit (JCTICU) was created to enhance collaboration on counter-terrorism investigations and related operations. It includes officers from ASIO, the AFP, ASIS, DIGO and DSD.

In August 2003 a review of JCTICU processes and methods of operation endorsed the broad thrust of JCTICU operating arrangements but recommended a range of process improvements.

The JCTICU continued to focus on developing closer investigative collaboration between member agencies. It refined mechanisms for inter-agency cooperation while undertaking investigations requiring a broad range of investigative and operational capabilities.

### ***Other agencies***

A large number of ASIO operations and enquiries relate to travellers to and from Australia passing through airports. The Australian Customs Service (ACS) continues to assist ASIO through its intelligence and operational support for interviews and early warnings of travel.

Other Federal, State and local government agencies, and some private corporations, continue to assist the Organisation in a range of capacities. DIMIA and DFAT are key agencies in this regard.

## **Liaison with overseas partners**

During the reporting period the Attorney-General approved new liaison relationships with 15 agencies, contributing to our efforts to identify and counter threats to Australians and Australian interests. Some supplement or replace our liaison relationships with other agencies in the same country; others open up new liaison relationships. ASIO now has 251 relationships in 110 countries.

These liaison relationships increase the diversity of our liaison network. Some offer a wide liaison potential, others only a narrow but vital channel of information.

### ***Significant visits***

During 2003–04 we received 19 high-level visits. During the same period senior ASIO officers visited a number of overseas liaison partners.

### ***Special events***

*Athens Olympics:* ASIO was a member of the Greek Olympics Advisory Security Group (OAG) formed by the Greek Government for the Athens 2004 Olympics. ASIO officers visited Athens 13 times in 2003–04 to discuss Olympics security. ASIO had a liaison team based in the Australian Embassy in Athens in the lead-up to and during the Olympics and Paralympics period.

*Beijing Olympics:* ASIO will maintain ongoing exchanges with Chinese authorities in the lead-up to the 2008 Olympics.

*ANZAC Ceremony:* ASIO provided advice on the threat to Australians and Australian interests in Turkey.

*Commonwealth Heads of Government Meeting (CHOGM):* ASIO worked with liaison partners and with DFAT in support of security arrangements for CHOGM, which was held in Abuja on 5–8 December 2003.

## Technical capabilities

ASIO's engineering development group provides design solutions to enhance ASIO's technical collection capability. The group provides effective tactical engineering support through equipment customisation and deployment advice. As part of the latter process it plays an active role in testing equipment and training officers in its use.

### *Cooperation with Australian agencies*

ASIO has productive relationships on technical matters with a range of agencies including the AFP, ASIS, DSD and DSTO. We also have a strong relationship with the new Scientific, Engineering and Technology Unit in PM&C. ASIO has an officer seconded to the unit and is represented on its steering committee. We also engage closely with the AFP and State and Territory law enforcement agencies in a number of technical areas and anticipate such cooperation will increase as prosecutions against targets of terrorist concern similarly increase.

Parts of the performance report have been excluded from this unclassified *Report to Parliament* because of security sensitivity.

## Output 4: Foreign Intelligence

---

Output 4 contributes to the Government Outcome of 'A secure Australia' by:

- collecting foreign intelligence in Australia on behalf of ASIS and DSD at the request of the Minister for Foreign Affairs or the Minister for Defence
- collecting foreign intelligence incidentally through ASIO's security intelligence investigations and liaison with overseas partners.

The performance report has been excluded in its entirety from this unclassified *Report to Parliament* because of security sensitivity.





## Part 3

# Management and Accountability



## Corporate governance

Corporate governance in ASIO is exercised through a Corporate Executive, chaired by the Director-General, which sets overall strategic directions and oversees resource management. The Corporate Executive meets fortnightly. A Consultative Council, comprising representatives from management and the ASIO Staff Association, provides a forum for employment and conditions of service issues.

The Corporate Executive is supported by the Audit and Evaluation Committee, which is chaired by the Deputy Director-General and includes a senior officer from the Australian National Audit Office (ANAO).

**Figure 6. ASIO's corporate committees**



ASIO reports annually to the Attorney-General by means of a classified *Annual Report*, which is also provided to the National Security Committee of Cabinet and the Leader of the Opposition, and an unclassified *Report to Parliament*. Financial activities are regularly audited, and certain budgetary details are published in the annual budget papers.

## Corporate planning

ASIO's *Corporate Plan 2002–06* sets the broad framework for how ASIO does its business, measures its performance and achieves outcomes. The plan, which will be reviewed in 2005, identifies five areas of business focus for 2002–06: competing for the best people, staying ahead of technology, maintaining best security practice, leveraging partnerships and satisfying customers. A public document, the plan is available on the ASIO website at [www.asio.gov.au](http://www.asio.gov.au).

The *Corporate Plan 2002–06* is supported by a range of other plans, including:

- the (classified) *Information Management Strategic Plan 2004–2008*
- the (classified) *Security Management Plan 2001–04*, which was under review at the end of the reporting period. *The Security Management Plan 2005–08* will be introduced in early 2005.

### ***Business continuity***

ASIO's business continuity plans were updated in response to government and AIC initiatives in this area.

## **Accountability**

ASIO adheres to a range of accountability and safeguard arrangements that govern the way we operate – internal evaluations, audit and fraud control measures, and external accountability, including through the Inspector-General of Intelligence and Security.

### **Audit, evaluation and fraud control**

ASIO's program of internal reviews and evaluations, overseen by the Audit and Evaluation Committee, continued in 2003–04.

#### ***Fraud Control Plan***

ASIO completed a fraud risk assessment in early 2004 that provided the basis for updating ASIO's *Fraud Control Plan*. A special program on ethics and accountability also commenced in 2004 to ensure all staff have a clear understanding of their obligations and responsibilities. The program includes a substantial component covering ASIO's approach to fraud control and its expectations of staff. All officers are required to attend this program at least every three years.

No fraud investigations were undertaken in 2003–04.

#### ***Evaluations***

One evaluation, of the receipt and handling of highly sensitive material, commenced during the year and will conclude in the first half of 2004–05. Its recommendations will be implemented in 2004–05.

#### ***Audits***

Eight internal audits were completed, including:

- compliance with the *Commonwealth Crimes Act 1914*
- compliance with the *NSW Law Enforcement and National Security (Assumed Identities) Act 1998*
- cash policy and procedures
- payroll compliance
- public line calls and calls from the National Security Hotline
- three compliance audits to satisfy the requirements of state legislation and memoranda of understanding.

Remedial action to redress any administrative or procedural shortcomings arising from these audits was finalised or is continuing. No loss of monies or assets was reported.

## External scrutiny

External scrutiny of ASIO's activities occurs through oversight by the Attorney-General, the Inspector-General of Intelligence and Security, the Auditor-General and the Parliamentary Joint Committee on ASIO, ASIS and DSD.

Section 21 of the *Australian Security Intelligence Organisation Act 1979* requires the Leader of the Opposition be kept informed on security matters. The Leader of the Opposition receives a copy of ASIO's classified *Annual Report* and is briefed by the Director-General as required.

## Budget oversight

Our financial program is included in the Attorney-General's *Portfolio Budget Statement*, which is scrutinised by the Senate Legal and Constitutional Legislation Committee. The Director-General attends committee hearings.

## The Attorney-General

Ministerial oversight of ASIO is the responsibility of the Attorney-General.

- All warrants for the exercise of ASIO's special powers must be approved by the Attorney-General.
- In addition to warrant requests, in 2003–04 we provided the Attorney with 268 briefing papers and submissions on significant security and ASIO-related issues (compared to 214 in 2002–03).
- ASIO operational activity must comply with the Attorney-General's *Guidelines for the Collection of Intelligence*, which require the use of methods commensurate with the assessed risk.
- The Attorney-General receives reports from the IGIS on inquiries relating to ASIO, including complaints.

## The Inspector-General of Intelligence and Security (IGIS)

The IGIS's role is to ensure ASIO acts legally and with propriety, complies with ministerial guidelines and shows due regard for human rights. The IGIS may initiate inquiries, respond to requests by the Attorney-General or the Government, or investigate complaints. The IGIS regularly reviews ASIO's actions, including:

- operational activity
- use of intrusive powers under warrant
- provision of information to, and liaison with, law enforcement agencies
- official use of alternative documentation to support assumed identities
- access to, and use of, financial transaction reporting information obtained from the Australian Transaction Reports and Analysis Centre (AUSTRAC)
- access to, and use of information obtained from, the Australian Taxation Office
- compliance with the *Archives Act 1983*.

The IGIS meets as required with the Director-General, senior managers and the President of the Staff Association.

In his 2003–04 *Annual Report* the IGIS noted his office conducted preliminary inquiries into 10 new complaints about ASIO and initiated full inquiries into 2 new complaints (compared to 21 in 2002–03 and 16 in 2001–02). Nine outstanding complaints were carried over from the previous reporting period. Thirty-five complaints were concluded without proceeding to a full or preliminary inquiry (compared to 32 such cases in 2002–03).

The IGIS's *Annual Report* can be found at [www.igis.gov.au](http://www.igis.gov.au).

### ***The Parliamentary Joint Committee on ASIO, ASIS and DSD (PJCAAD)***

The PJCAAD has a mandate to review ASIO administration and expenditure. It can also enquire into matters referred to it by the Government or by the Parliament. Committee members are listed at Appendix A.

The PJCAAD's functions do not include review of operational matters, intelligence gathering priorities or individual complaints.

The PJCAAD may request the heads of the relevant agencies and the IGIS to provide briefings for the purpose of performing its functions. In 2003–04, the Director-General briefed the Committee on:

- 25 November 2003 about the security environment
- 6 May 2004 about administration and expenditure
- 3 June 2004 on the listing of Palestinian Islamic Jihad as a proscribed organisation.

The Committee visited ASIO's Central Office on 21 June 2004 to inspect the NTAC.

### ***Other Parliamentary Committees***

In 2003–04 the Director-General appeared before other Parliamentary Committees inquiring into intelligence and security matters, including:

- 18 September 2003 – Parliamentary Joint Committee of Public Accounts & Audit: Review of Aviation Security in Australia
- 24 September 2003 – Senate Foreign Affairs, Defence and Trade References Committee Inquiry into the Assessment of Threats to the Security of Australians in South-East Asia
- 03 November 2003 – Senate Legal and Constitutional Legislation Committee – Budget Supplementary Hearing
- 02 December 2003 – Senate Foreign Affairs, Defence and Trade References Committee Inquiry into the Assessment of Threats to the Security of Australians in South-East Asia
- 16 February – Senate Legal and Constitutional Legislation Committee – Additional Budget Estimates Hearing
- 25 May 2004 – Senate Legal and Constitutional Legislation Committee – Budget Estimates Hearing
- 28 May 2004 – Senate Foreign Affairs, Defence and Trade References Committee Inquiry into the Assessment of Threats to the Security of Australians in South-East Asia.

## Interaction with the public

Terrorism and other security issues have had a much higher public profile since the 11 September 2001 attacks in the United States and the 12 October 2002 attack in Bali.

ASIO publishes brochures and pamphlets about its work, in addition to its *Report to Parliament*. Members of the public can call ASIO's public telephone number (see Appendix B) and request information about the Organisation.

### ASIO interviews

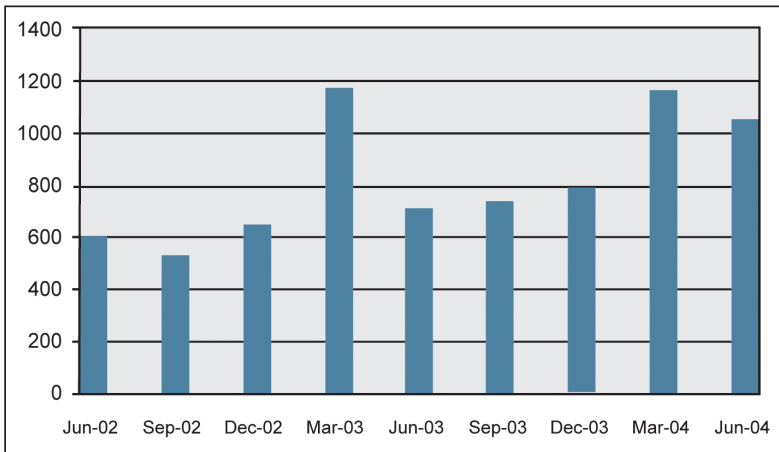
Investigations often require officers to ask questions of members of the public. These interviews are conducted under a code of conduct which requires ASIO officers to show proof of identity and to behave in an appropriate manner. Any concerns an interviewee may have about an ASIO officer's bona fides or actions can be reported to ASIO or to the IGIS.

### ASIO website ([www.asio.gov.au](http://www.asio.gov.au))

Interest in the ASIO website remained high. In 2003–04 the site recorded an average of 37 915 hits and 931 visitor sessions per day, increases of 34% and 18% respectively on 2002–03. Employment pages remained the most popular. Information on the website is regularly updated.

The *ASIO Now* brochure will be updated and translated into several community languages and be available on the website and in hard copy.

**Figure 7. Website interest – average visits per day**



## Media policy

ASIO does not normally comment on matters of national security, but in some circumstances the Attorney-General (or the Director-General, with the Attorney's agreement) will provide public comment where this may help to promote public confidence in the legality, propriety and effectiveness of ASIO's conduct.

Interest in security issues and ASIO activities has of course increased over recent years, as reflected in a substantial increase in the frequency of media requests for information, briefings and interviews throughout the reporting period.

Advertisements for employment with ASIO continued to generate media interest. We provided information on ASIO employment in response to media requests, with the resulting articles raising interest in our recruitment campaign.

## **Our people**

ASIO's success depends on recruiting, developing and retaining the right people with the right capabilities. Recruitment and staff development remain a focus for ASIO.

As of 30 June 2004, ASIO had 805 staff – this will increase over the next two years to about 1000.

## **Workplace relations and reforms**

The ASIO Consultative Council (ACC) – consisting of management and Staff Association representatives – deals with people management policies and practices and workplace issues. The ACC meets monthly, and is chaired (on rotation) by the head of the Corporate Management and Liaison Division and the President of the Staff Association.

Under ASIO's Sixth Workplace Agreement, which covers all non-Senior Executive Service (SES) staff, salaries increased by 4% in April 2004 and will increase by a further 4% in April 2005.

During the reporting period work commenced or continued on a range of reforms and initiatives that are expected to be completed during 2004–05 including:

- consolidating terms and conditions of employment into a single 'plain English' document
- introducing a health and well-being program that includes initiatives designed to highlight or address issues relevant to ASIO staff
- reviewing staff dispute/grievance mechanisms including access to external independent bodies
- refining the performance management framework introduced during the previous reporting period.

Work is underway to conduct a staff survey in 2004–05. The survey had been planned for 2003–04 but operational pressures prevented it.

### **Performance pay**

Performance pay is available to SES officers, with the amount paid based on a percentage of gross salary. In 2003–04, 18 officers received performance pay. Payments ranged from \$2852 to \$22 332. The average payment was \$9118 and the total amount paid was \$164 128.

## **Recruitment and staffing**

Recruitment and staffing remained a challenge, both in terms of numbers and quality.



## Recruiting

Recruitment has been at levels in excess of the mid-1980s when ASIO Headquarters was relocated from Melbourne to Canberra. As ASIO continues to grow, the level of recruitment will remain high. ASIO staff recruitment remains a resource-intensive task because of the need for security clearances and other general suitability (including psychological) requirements.

During 2003–04 we recruited 195 staff compared to 101 in 2002–03. This was an exceptional effort and the most staff ever recruited into ASIO over a financial year.



An external review of recruitment and vetting practices was conducted to identify opportunities for improvement. Recommended changes were implemented and the timeframes for various processes reduced without affecting quality. The average time from the advertised closing date to the date of job offer is now 20 weeks – a reduction of 5 weeks since the previous year.

Early in the reporting period recruitment efforts focused on technical and surveillance staff to bolster intelligence collection capabilities. Later in the period the focus shifted to recruitment for the NTAC.

Throughout the period ASIO's graduate entry program remained a recruitment priority, with activity starting in February 2003 and finishing in January 2004. To maintain the quality of our graduate intake we ran a major graduate advertising campaign in February 2003 followed by a supplementary campaign in September 2003. Despite this,

and receiving a total of nearly 2000 applications (1614 from the first and 325 from the supplementary campaign), only 26 graduate trainees commenced in January 2004. This compares to 28 in 2002–03.

At the end of the reporting period, recruitment of a further 30–35 graduates to commence in January 2005 was well underway. There were 1651 applications – around the same as for the equivalent campaign in 2003.

## Staffing profile

While employment of permanent staff remained a feature of our recruitment effort in 2003–04, we continue to make use of contract employees to meet short-term needs and to provide additional flexibility to satisfy our staffing requirements.

At 30 June 2004, 20% of staff were temporary employees compared to 16.5% at 30 June 2003. See Appendix C for staffing statistics.

## Staff retention

The attrition rate was 6.2%, which was down from 7% in 2002–03.

In separation interviews with our personnel and security areas, staff cited reasons similar to past years for leaving: better promotional opportunities, increased remuneration, greater job satisfaction and greater rewards and recognition.

## Advertising

We revamped our graduate recruitment campaign to update the look of our advertisements and website. We employed national recruitment companies to assist in our larger campaigns.

Advertising costs, mainly in the print media, were \$753 836 compared to \$226 206 in 2002–03. The increase was due to a larger volume of advertising, the updated graduate campaign and more use of colour advertising.

## Developing our people

Training and development remain a very high priority at all times but particularly in this period of growth. Our commitment to training and development is demonstrated through our investment of \$2 567 118 (about 2.7% of budget) in 2003–04. This includes corporately funded training and job-specific courses funded by individual work groups. Expenditure on training and development increased by \$752 027 (41%) over 2002–03. The corporate training program focused on developing intelligence, management and administrative competencies across the Organisation.

### Leadership and management development

Leadership development continued to be a priority, including for all SES and Senior Officers (SO). The broad range of training activities included 'time-outs', formal in-house and external courses, and support for tertiary education:

- three SES time-outs focused on managing growth, performance improvement, ethics and accountability, budget issues, and the security intelligence environment
- a total of 150 SOs attended focus groups generating ideas for improvement in a wide range of areas including accommodation, accountability, delegation, training and information management
- all SO and SES staff attended two combined SES/SO time-outs
- all SOs attended *Leader as Coach* training to support the introduction of the upgraded performance management process in 2003.

### Analytical and operational skills

A comprehensive intelligence training program was delivered to develop the intelligence gathering, analytical, operational and reporting skills of ASIO officers. Some of this training was conducted in cooperation with international liaison partners. Included in the training delivered in 2003–04 were:

- courses on *Terrorism: International Perspectives* and *Introduction to Islam*
- courses in critical thinking to enhance analytical and conceptual skills
- in-house training courses on agent recruitment, source management and operational tradecraft
- training in surveillance and counter-surveillance.

### Technical capabilities

Our technical officers maintained and improved their skills through internal and external courses.

### **Other training**

- The *Ethics and Accountability in ASIO* program was reviewed and updated with 132 staff completing the course this year. We have plans for around another 130 staff to undertake this training in 2004–05. Two SES officers lead each one-day program, underpinning the importance ASIO attaches to this training.
- A full program of administrative training was delivered including contract management, selection panel skills, presentation skills, trainer training, interviewing, effective reading and writing, finance and budgeting, and project management.
- Training in our administrative and intelligence computer systems and applications was given to 187 staff.
- Five *Introduction to ASIO* programs were run during the year for 109 new staff. Other new staff received similar information in job-specific training courses (for example, graduate entry training and NTAC training).
- Forty-two people were provided with support for tertiary studies.

### **Graduate traineeship**

A review of our graduate traineeship was undertaken during 2003 with recommendations implemented for the traineeship commencing in January 2004. Changes to the program included:

- redesigned analysis and collection courses
- redesigned work-place rotations to better reinforce new skills
- changing from two 15-person traineeships a year (commencing in October and April) to one 30-person traineeship commencing in January
- designing a series of development opportunities to follow the traineeship
- refining the assessment of course outcomes.

### **Secondments**

Secondments and personnel exchanges with other agencies in Australia and overseas continued. ASIO officers were seconded to the AFP, ASIS, DIGO, DOTARS, ONA, and PM&C.

The number of secondments into ASIO expanded – with officers from the AFP, ASIS, DFAT, DIGO, DIO, DOTARS, DSD, DSTO and ONA now working in ASIO in a variety of areas reflecting the changed approach to counter-terrorism over the past three years.

### **HRD oversight**

The Human Resource Development Committee met six times in 2003–04 providing guidance on such issues as updating of the Study Assistance policy, delivery of the HRD investment program, reviewing our strategy on leadership development and developing a more effective training program for ASIO officers levels 1–3.

## Workplace diversity

Statistical data on staff numbers, workforce profile, representation of designated work groups and salary structure are contained in Appendices C, D and E.

During the year a new *Workplace Diversity Program* was developed for the period 2004 to 2008, in line with our obligations under clause 4 of Chapter 3 of the *Public Service Commissioner's Directions 1999*. This program will be introduced in 2004–05.

The program supports our commitment to providing a workplace that is free from harassment and discrimination and promotes diversity and equal employment opportunities. It incorporates both ongoing initiatives and introduces some new ones, including:

- better collection of recruitment and employment statistics
- raising awareness of diversity issues among managers and staff
- better targeted recruitment publicity.

## Harassment Contact Officers

Five new Harassment Contact Officers (HCO) were trained during the year, and one HCO attended refresher training. A HCO networking group was introduced, enabling HCOs to attend or teleconference a quarterly meeting and providing better informal support opportunities. Our recording/reporting and staff support processes have been improved as a result.

An Intranet site was created, in line with our *Workplace Diversity Program*, incorporating a range of information for both managers and staff. It includes:

- relevant policies
- management information
- press and publication items of general interest
- list of HCOs by work group
- information from internal training courses.

## Seminar series

The ASIO Women's Network was replaced by a seminar series dealing with a variety of topics of interest more broadly across ASIO, including:

- general organisational knowledge
- new work areas in ASIO (for example, the NTAC)
- personal/professional career development
- management and workplace issues.

Seminars are open to all staff and information generated from them is circulated to State offices by means of video recording and our in-house newsletter. It is proving a useful way for new staff to become familiar with other areas and functions in ASIO.

### ***Diversity statistics***

The percentage of female staff overall is 41% and the percentage of female staff at senior officer level or above has risen slightly to 24%.

In early 2004–05 we will evaluate our graduate recruitment strategy to identify any changes that might increase the number of staff from non-English-speaking backgrounds.

### ***Disability strategy***

A new program was drafted and there has been undergoing consultation with staff.

## **Occupational Health and Safety (OH&S)**

### ***OH&S initiatives***

ASIO's Occupational Health and Safety sub-committee oversaw the continued implementation of the OH&S Agreement, which included 12 OH&S audits. Significant health and safety initiatives included:

- continuation of a phased approach to Health Week resulting in activities and health checks conducted over two separate weeks. These activities aimed to improve health, manage stress and educate staff on health and safety issues
- introduction of a regular *Health and Well-Being Program* with speakers and activities every two months. This was part of the Sixth Workplace Agreement
- offering free influenza vaccinations to promote health in the workplace and reduce absenteeism (this was also part of the Sixth Workplace Agreement)
- selecting and training first aid and health and safety representatives.

There were no accidents causing death or serious personal injury recorded during the reporting period. There were no incidents involving incapacity of 30 days or more as a result of accident, incident or disease arising out of an employee's work. No dangerous occurrences were reported.

### ***Compensation claims***

In 2003–04 there were 14 claims for compensation, compared to 11 in 2002–03. Liability was admitted for all. Our premium for 2004–05 has yet to be advised as COMCARE is still working through the objection we raised to our 2003–04 premium.

## **Information management**

### ***Strategic outlook***

Over the year ASIO updated its (classified) *Information Management Strategic Plan* for 2004 through to 2008. In the coming year we will use this information to continue to address issues of information management and the delivery of an enhanced and robust information processing environment.

### ***Communications Centre services***

To support the 24-hour operations of the NTAC we recruited and trained additional communications staff to move from on-call arrangements to 24-hour on-site services in the Communications Centre. The new arrangements started in April 2004.

### **Records management**

The upgrade of ASIO's records management software continued throughout the year. The upgrade will provide a stable and supportable facility for the management of paper records within a need-to-know security framework. This upgrade will support ASIO's improvements to the management of electronic documents and records. Work on the next stage will commence in 2004–05.

### **Assuring value for money in IT purchasing**

ASIO continues to identify suppliers of hardware and services in line with the principle of market testing. A request for tender was released during the year seeking vendor solutions for upgrading our core intelligence hardware and applications.

## **Security of ASIO**

We focused on developing and maintaining a robust security culture which builds on the security enhancements implemented following the *Cook Inquiry* of 1994 and the *Inquiry into Security Issues* in 2000. ASIO's growth over the past three years has presented some challenges in ensuring that security remains a priority. However, these challenges have been met by the implementation and regular review of security policies, practices and procedures, and an ongoing focus on security awareness training for staff.

### **Security Management Plan**

Objectives and strategies to maintain security within ASIO are set out in ASIO's (classified) *Security Management Plan*. The current plan, covering the period 2001–04, sits above ASIO's internal security policies and underpins ASIO's goals through security risk management. Work commenced on a new plan to come into effect in 2004–05.

### **Security clearance re-evaluations**

The security clearance is revalidated every 30 months and fully re-evaluated at least every five years. There were 58 full re-evaluations completed in the reporting period.

### **Supporting our staff**

ASIO's growth over recent years has placed increased demand on Employee Assistance Program resources. ASIO continues its active approach of providing assistance to staff with personal and professional matters to reduce the risk of such problems becoming security issues over time.

### **Physical security**

In early 2004 a review of all ASIO's State offices resulted in upgrades to physical and electronic security. A review will be conducted annually following the scheduled maintenance of each office. An integral part of the process is the provision of security awareness update briefings to all staff.

ASIO is involved in the Russell Passive Defence project, which will result in increased security measures in and around the Russell precinct, including ASIO Central Office.

### **Security audits**

Results of ASIO's routine security audits indicate that processes and systems in place conform to relevant policies and procedures. Audits completed during the reporting period examined the security of our information holdings, the management of accountable documents and the physical security of ASIO's assets.

### **Security policies**

During the reporting period ASIO continued to ensure its security policies and procedures remained current, effective and consistent with IASF-endorsed guidelines and practices. Improvements and additions were made to a number of policies, including those relating to ASIO security passes, visitor entry and the *ASIO House Security Instructions*.

## **Building management**

A number of refurbishment activities occurred in ASIO's Central Office over 2003–04, including:

- completing building extensions into part of the internal courtyards to provide an additional 500 square metres of office space
- further refurbishment to accommodate additional staff and functions as a consequence of recent Budget decisions and a corporate restructure
- refurbishment of space for the NTAC
- replacement of furniture in our Sydney Office.

Planning commenced for:

- additional space to temporarily accommodate additional staff in ASIO's Central Office
- a feasibility study for an extension to ASIO's Central Office building to house increases in both ASIO and ONA staff numbers. This study will be completed during 2004–05.

### **Ecologically sustainable development and environmental performance**

ASIO engaged Asset Services Australia to conduct an energy audit on the plant and utilities within ASIO Central Office. The final report made recommendations to optimise the use of electricity and gas consumption; funds have been set aside in 2004–05 to implement more of these changes.

Energy demand in ACO increased markedly during the period with the move to 24-hour operations.

Our building energy management system provided the flexibility to meet these additional energy requirements, while keeping waste to a minimum.



### **Environmental initiatives**

A range of recycling, waste and water management initiatives were introduced and/or maintained to minimise the impact on the environment within the limitations of a security organisation, including:

- balancing the air conditioning systems
- connecting supplementary fan coil units to the building automation system
- recycling paper and cardboard (where security requirements permit)
- using electronic forms to reduce paper usage.

### **Purchasing**

All purchasing activity in ASIO is conducted in accordance with the *Chief Executive's Instructions*, which require officers to follow the *Commonwealth Procurement Guidelines*, subject to authorised exemptions for the protection of national security. ASIO adheres to the Commonwealth's core procurement policy framework as set out in the *Procurement Guidelines*, and ensures that value for money is achieved through competitive procurement processes wherever practicable.

We are updating our *Chief Executive's Instructions* and developing new guidance on purchasing and contracting for goods and services; this will be accessible to all staff via the Intranet.

In 2003–04 ASIO's annual investment program continued. Purchasing objectives focused on investment in key business areas, including technical capabilities, information technology infrastructure and protective security measures.

### **Consultants**

During 2003–04, ASIO let 19 consultancy contracts, which was up from 13 in 2002–03. Total expenditure on consultancy contracts during the year (including contracts let during the previous year) came to \$0.412m, down from \$0.704m in 2002–03. The decrease resulted from a greater use of in-house expertise to inform agency decision-making and changes to the way consultancy contracts are classified under the *Requirements for Annual Reports* and the Department of Finance and Administration's *Guidance on Identifying Consultancies for Annual Reporting Purposes*.

Subject to authorised exemptions for the protection of national security, a list of consultancy contracts let to the value of \$10 000 or more (inclusive of GST), and the total value of each of those contracts over the life of each contract, may be made available to Members of Parliament as a confidential briefing, or to the Parliamentary Joint Committee on ASIO, ASIS and DSD on request.

### **Competitive tendering and contracting**

ASIO did not undertake any competitive tendering and contracting (CTC) activities in 2003–04. CTC activity in this context only relates to the contracting out of government activities, previously performed by a Commonwealth agency, to another organisation, and only includes the provision of goods and services. The scope for CTC activity by ASIO continues to be limited by national security considerations.



### ***Exempt contracts***

The Director-General of Security has directed that details of ASIO agreements, contracts and standing offers must not be notified in the *Purchasing and Disposals Gazette* on the basis that these are exempt documents under the *Freedom of Information Act 1982* for the reason that disclosure of such documents would, or could reasonably be expected to, cause damage to the security of the Commonwealth.

Details of ASIO agreements, contracts and standing offers may be made available to Members of Parliament as a confidential briefing, or to the Parliamentary Joint Committee on ASIO, ASIS and DSD on request.

ASIO considers that information about its individual contracts should be protected because the disclosure of this material could reasonably be expected to cause damage to national security.

### ***Contracts audit***

The Australian National Audit Office (ANAO) examined ASIO's contracting processes as part of its annual audit of agency compliance with the Senate Order for Departmental and Agency Contracts. The audit began in the 2003–04 financial year and was completed in 2004–05 with a report of the audit tabled in Parliament. ASIO will implement the ANAO recommendations in 2004–05.

Parts of the performance report have been excluded from this unclassified *Report to Parliament* because of security sensitivity.





Part 4

# Financial Statements



## Audit Report on the Financial Statements of the Australian Security Intelligence Organisation



**INDEPENDENT AUDIT REPORT**

**To the Attorney-General**

**Scope**

The financial statements comprise:

- Statement by the Director-General of Security;
- Statements of Financial Performance, Financial Position and Cash Flows;
- Schedules of Commitments and Contingencies;
- Schedule of Administered Items; and
- Notes to and forming part of the Financial Statements

of the Australian Security Intelligence Organisation for the year ended 30 June 2004.

The Australian Security Intelligence Organisation's Director-General is responsible for the preparation and true and fair presentation of the financial statements in accordance with the Finance Minister's Orders. This includes responsibility 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 Australian Security Intelligence Organisation's financial position, and of its performance as represented by the statements of financial performance and cash flows.

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

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 Director-General.

#### **Independence**

In conducting the audit, I have followed the independence requirements of the Australian National Audit Office, which incorporate Australian professional ethical pronouncements.

#### **Audit Opinion**

In my opinion, the financial statements:

- (i) have been prepared in accordance with the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997* and applicable Accounting Standards; and
- (ii) give a true and fair view, of the matters required by applicable Accounting Standards and other mandatory professional reporting requirements in Australia, and the Finance Minister's Orders, of the financial position of the Australian Security Intelligence Organisation as at 30 June 2004, and of its financial performance and cash flows for the year then ended.

Australian National Audit Office



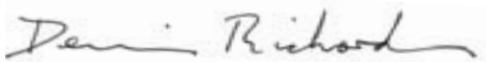
Brandon Jarrett  
Executive Director

Delegate of the Auditor-General

Canberra  
7 September 2004

## Statement by the Director-General of Security

In my opinion, the attached financial statements for the year ended 30 June 2004 are based on properly maintained financial records and give a true and fair view of the matters required by the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*.

A handwritten signature in black ink, reading "Dennis Richardson". The signature is written in a cursive style with a long horizontal line extending from the end.

Dennis Richardson  
Director-General of Security

7 September 2004

## Statement of Financial Performance for the year ended 30 June 2004

	Notes	2004 \$ '000	2003 \$ '000
<b>Revenues from ordinary activities</b>			
Revenues from Government	4A	99,047	86,237
Goods and services	4B	1,993	1,113
Interest	4C	–	13
Revenue from sale of assets	4D	976	859
Other revenues	4E	1,009	723
<i>Revenues from ordinary activities</i>		<b>103,023</b>	<b>88,945</b>
<b>Expenses from ordinary activities (excluding borrowing costs expense)</b>			
Employees	5A	61,068	48,660
Suppliers	5B	33,211	33,271
Depreciation and amortisation	5C	7,739	8,075
Write-down of assets	5D	700	41
Value of assets sold	4D	959	898
<i>Expenses from ordinary activities (excluding borrowing costs expense)</i>		<b>103,678</b>	<b>90,945</b>
<i>Borrowing costs expense</i>	6	<b>24</b>	<b>38</b>
<b>Net surplus / (deficit) from ordinary activities before income tax</b>		<b>(679)</b>	<b>(2,038)</b>
Net credit to asset revaluation reserve	12	3,217	–
<i>Total revenues, expenses and valuation adjustments recognised directly in equity</i>		<b>3,217</b>	<b>–</b>
<b>Total changes in equity other than those resulting from transactions with the Australian Government as owner</b>		<b>2,539</b>	<b>(2,038)</b>

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



## Statement of Financial Position as at 30 June 2004

	Notes	2004 \$ '000	2003 \$ '000
<b>ASSETS</b>			
<b>Financial assets</b>			
Cash	7A	7,216	5,350
Receivables	7B	1,846	2,031
<i>Total financial assets</i>		<u>9,062</u>	<u>7,381</u>
<b>Non-financial assets</b>			
Land and buildings	8A, 8D	16,550	12,781
Infrastructure, plant and equipment	8B, 8D	28,344	20,020
Intangibles	8C, 8D	3,071	2,631
Other non-financial assets	8E	2,398	628
<i>Total non-financial assets</i>		<u>50,362</u>	<u>36,060</u>
<b>Total Assets</b>		<u><u>59,424</u></u>	<u><u>43,441</u></u>
<b>LIABILITIES</b>			
<b>Interest bearing liabilities</b>			
Leases	9	115	331
<i>Total interest bearing liabilities</i>		<u>115</u>	<u>331</u>
<b>Provisions</b>			
Accommodation leases - make good	10A	1,487	1,032
Employees	10B	17,019	13,781
<i>Total provisions</i>		<u>18,506</u>	<u>14,813</u>
<b>Payables</b>			
Suppliers	11A	3,854	4,523
<i>Total payables</i>		<u>3,854</u>	<u>4,523</u>
<b>Total Liabilities</b>		<u><u>22,475</u></u>	<u><u>19,667</u></u>
<b>NET ASSETS</b>		<u><u>36,949</u></u>	<u><u>23,774</u></u>
<b>EQUITY</b>			
Contributed equity	12	32,781	22,144
Reserves	12	9,496	6,279
Retained surpluses or (accumulated deficits)	12	(5,328)	(4,649)
<b>TOTAL EQUITY</b>		<u><u>36,949</u></u>	<u><u>23,774</u></u>
<b>Current assets</b>		<b>11,460</b>	<b>8,009</b>
<b>Non-current assets</b>		<b>47,964</b>	<b>35,432</b>
<b>Current liabilities</b>		<b>12,754</b>	<b>11,484</b>
<b>Non-current liabilities</b>		<b>9,721</b>	<b>8,183</b>

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

## Statement of Cash Flows for the year ended 30 June 2004

	Notes	2004 \$ '000	2003 \$ '000
<b>OPERATING ACTIVITIES</b>			
Cash received			
Goods and services		3,847	1,207
Appropriations		98,210	85,675
Interest		–	13
Net GST received from ATO		4,521	2,921
<i>Total cash received</i>		<u>106,578</u>	<u>89,816</u>
Cash used			
Employees		57,830	47,947
Suppliers		39,567	34,780
Borrowing costs		24	38
<i>Total cash used</i>		<u>97,421</u>	<u>82,765</u>
Net cash from / (used by) operating activities	13	<u>9,157</u>	<u>7,051</u>
<b>INVESTING ACTIVITIES</b>			
Cash received			
Proceeds from sales of property, plant and equipment		976	859
<i>Total cash received</i>		<u>976</u>	<u>859</u>
Cash used			
Purchase of intangibles		1,300	–
Purchase of property, plant and equipment		17,386	10,783
<i>Total cash used</i>		<u>18,687</u>	<u>10,783</u>
Net cash from / (used by) investing activities		<u>(17,711)</u>	<u>(9,924)</u>
<b>FINANCING ACTIVITIES</b>			
Cash received			
Appropriations - contributed equity		10,637	4,692
<i>Total cash received</i>		<u>10,637</u>	<u>4,692</u>
Cash used			
Repayment of debt		216	202
Capital use charge paid		–	2,899
<i>Total cash used</i>		<u>216</u>	<u>3,101</u>
Net cash from / (used by) financing activities		<u>10,420</u>	<u>1,591</u>
<i>Net increase / (decrease) in cash held</i>		<u>1,867</u>	<u>(1,281)</u>
Cash at the beginning of the reporting period		5,350	6,631
<i>Cash at the end of the reporting period</i>	7A	<u>7,216</u>	<u>5,350</u>

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

## Schedule of Commitments as at 30 June 2004

	Notes	2004 \$ '000	2003 \$ '000
<b>BY TYPE</b>			
<b>Capital commitments</b>			
Land and buildings	A	–	1,582
Infrastructure, plant and equipment	B	847	553
<b>Total capital commitments</b>		<b>847</b>	<b>2,135</b>
<b>Other commitments</b>			
Operating leases	C	48,984	53,581
Other commitments		2,176	3,050
<b>Total other commitments</b>		<b>51,160</b>	<b>56,631</b>
<b>Commitments receivable</b>		<b>6,508</b>	<b>9,287</b>
<b>Net commitments</b>		<b>45,499</b>	<b>49,479</b>
<b>BY MATURITY</b>			
<b>Capital commitments</b>			
One year or less		847	2,135
From one to five years		–	–
Over five years		–	–
<b>Total capital commitments by maturity</b>		<b>847</b>	<b>2,135</b>
<b>Operating lease commitments</b>			
One year or less		6,046	5,265
From one to five years		24,112	26,459
Over five years		18,826	21,857
<b>Total operating lease commitments by maturity</b>		<b>48,984</b>	<b>53,581</b>
<b>Other commitments</b>			
One year or less		2,176	3,050
From one to five years		–	–
Over five years		–	–
<b>Other commitments by maturity</b>		<b>2,176</b>	<b>3,050</b>
<b>Commitments receivable</b>		<b>6,508</b>	<b>9,287</b>
<b>Net commitments by maturity</b>		<b>45,499</b>	<b>49,479</b>

Commitments are GST inclusive where relevant

A Outstanding contractual payments for building extension under construction.

B Plant and equipment commitments are contracts for purchase of equipment for various projects

C Operating leases included are effectively non-cancellable and comprise:

<i>Nature of lease</i>	<i>General description of leasing arrangement</i>
Leases for office accommodation	Various arrangements apply to the review of lease - annual review based on upwards movement in the Consumer Price Index (CPI) - biennial review based on CPI - biennial review based on market appraisal
Agreements for the provision of motor vehicles to senior executive and other officers	No contingent rentals exist. There are no renewal or purchase options available to ASIO.

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

## Schedule of Contingencies as at 30 June 2004

	Notes	2004 \$ '000	2003 \$ '000
Contingent liabilities		40	—
Contingent assets		—	—
Net contingencies		<u>40</u>	<u>—</u>

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

## Notes to and forming part of the Financial Statements for the year ended 30 June 2004

### Note 1: Summary of significant accounting policies

#### A. Objective

To provide advice, in accordance with the ASIO Act to Ministers and appropriate agencies and authorities, to protect Australia and its people from threats to national security.

ASIO is structured to meet the following Outcome:

A secure Australia for people and property, for Government business and national infrastructure, and for special events of national and international significance.

#### B. Basis of accounting

The financial statements are required by *section 49* of the *Financial Management and Accountability Act 1997* and are a general purpose financial report. The financial statements have been prepared in accordance with the agreement between the Finance Minister and the Attorney-General. This agreement states that ASIO's financial statements must be prepared in accordance with the *Financial Management and Accountability Orders (Financial Statements for reporting periods on or after 30 June 2004)* except where the disclosure of information in the notes to the financial statements would, or could reasonably be expected to be operationally sensitive. Subject to the requirements of the agreement, the financial statements are prepared in accordance with:

- Finance Minister's Orders (or FMOs, being the *Financial Management and Accountability Orders (Financial Statements for reporting periods ending on or after 30 June 2004)*);
- 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, except for certain assets which, as noted, are at valuation. Except where stated, 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. 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.

The continued existence of ASIO in its present form, and with its current programs, depends on Government policy and on continuing appropriations by Parliament for the Agency's administration and programs.

#### C. Revenue

The revenues described in this Note are revenues relating to the core operating activities of the Agency. Details of revenue amounts are given in Note 4.

*Revenues from Government*

Amounts appropriated for Departmental outputs appropriations for the year (less any current year savings and reductions) are recognised as revenue, except for certain amounts that relate to activities that are reciprocal in nature, in which case revenue is only recognised when it is earned. Savings are amounts offered up in Portfolio Additional Estimates Statements. Reductions are amounts by which appropriations have been legally reduced by the Finance Minister under Appropriation Act No.3 of 2003-04.

Appropriations receivable are recognised at their nominal amounts.

*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.

*Other revenue*

Revenue from the sale of goods is recognised upon the delivery of goods to customers.

Revenue from the rendering of a service is recognised by reference to the stage of completion of contracts or other agreements to provide services. The stage of completion is determined according to the proportion that costs incurred to date bear to the estimated total costs of the transaction.

Receivables for goods and services are recognised at the nominal amounts due less any provision for bad and doubtful debts. Collectability of debts is reviewed at balance date. Provisions are made when collectability of the debt is judged to be less rather than more likely.

Interest revenue is recognised on a proportional basis taking into account the interest rates applicable to the financial assets.

Revenue from disposal of non-current assets is recognised when control of the asset has passed to the buyer.

**D. Transactions with the Government as Owner**

Amounts appropriated which are designated as "equity injections" for a year (less any savings offered up in Portfolio Additional Estimates Statements) are recognised directly in Contributed Equity for that year.

**E. Leases**

A distinction is made between finance leases and operating leases. Finance leases effectively transfer from the lessor to the lessee substantially all the risks and benefits incidental to ownership of leased non-current assets. In operating leases, the lessor effectively retains substantially all such risks and benefits.

Where a non-current asset is acquired by means of a finance lease, the asset is capitalised at the present value of minimum lease payments at the beginning of the lease and a liability recognised for the same amount. The discount rate used is the interest rate implicit in the lease. Leased assets are amortised over the period of the lease. Lease payments are allocated between the principal component and the interest expense.

Operating lease payments are expensed on a basis which is representative of the pattern of benefits derived from the leased assets.

Lease incentives taking the form of "free" leasehold improvements and rent holidays are recognised as liabilities. These liabilities are reduced by allocating lease payments between rental expense and the reduction of the liability.

#### *Accommodation leases - make good*

Properties occupied by ASIO are subject to make good costs when vacated at the termination of the lease. A provision for make good is recognised at the commencement of a lease. The provision is calculated as the present value of the expected future make good payment. Make good expenses include initial recognition of the liability, movement in the liability as the time of payment of the make good advances one period and any adjustments resulting from changes in the basis of estimation. The provisions and expenses for make good costs are reviewed and adjusted annually.

#### **F. 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.

#### **G. Other Financial Instruments**

Interest is expensed as it accrues unless it is directly attributable to a qualifying asset.

#### *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).

#### *Contingent Liabilities and Contingent Assets*

Contingent liabilities (assets) are not recognised in the Statement of Financial Position but are discussed in the relevant schedules and notes. They may arise from uncertainty as to the existence of a liability (asset), or represent an existing liability (asset) in respect of which settlement is not probable or the amount cannot be reliably measured. Remote contingencies are part of this disclosure. Where settlement becomes probable, a liability (asset) is recognised. A liability (asset) is recognised when its existence is confirmed by a future event, settlement becomes probable or reliable measurement becomes possible.

#### **H. Acquisition of Assets**

Assets are recorded at cost on acquisition. The cost of acquisition includes the fair value of assets transferred in exchange and liabilities undertaken.

#### **I. Property, Plant and Equipment (PP&E)**

##### *Asset recognition threshold*

Purchases of property, plant and equipment are recognised initially at cost in the Statement of Financial Position, except for purchases costing less than \$2000, 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*

Land, buildings, infrastructure, plant and equipment are carried at valuation. Revaluations undertaken up to 30 June 2002 were done on a deprival basis; revaluations since that date are at fair value. This change in accounting policy is required by Australian Accounting Standard AASB 1041 *Revaluation of Non-Current Assets*. Valuations undertaken in any year are as at 30 June.

Fair values for each class of asset are determined as shown below.

<i>Asset Class</i>	<i>Fair value measured at:</i>
Land	Market selling price
Buildings	Market selling price
Leasehold improvements	Market selling price
Plant & equipment	Market selling price

Assets which are surplus to requirements are measured at their net realisable value. At 30 June 2004 ASIO had no assets in this situation.

The financial effect of this change in policy relates to those assets recognised at fair value for the first time in the current period where the measurement basis for fair value is different to that previously used for deprival value. The financial effect of the change is given by the difference between the fair values obtained for these assets in the current period and the deprival-based values recognised at the end of the previous period. The financial effect by class is as follows:

<i>Asset class</i>	<i>Increment / (decrement) to asset class</i>	<i>Contra account</i>
Land	2004: \$396,000 2003: Nil	Revaluation Reserve
Buildings	2004: \$1,236,107 2003: Nil	Revaluation Reserve
Leasehold improvements	2004: \$1,212,546 2003: Nil	Revaluation Reserve
Plant & equipment	2004: \$373,043 2003: Nil	Revaluation Reserve

The total financial effect was to increase the carrying amount of property, plant & equipment by \$3,217,696 (2003: nil) and increase revaluation reserves by \$3,217,696 (2003: nil).

### *Frequency*

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. All ASIO's assets have been revalued at 30 June 2004 to fair value. Revaluations will be performed when the fair value of an asset class differs materially from its carrying amount.

### *Conduct*

All valuations are conducted by an independent qualified valuer except where specifically noted otherwise.

### *Depreciation*

Depreciable property, plant and equipment assets are written-off to their estimated residual values over their estimated useful lives to ASIO using, in all cases, the straight line method of depreciation. Leasehold improvements are depreciated on a straight line basis over the lesser of the estimated useful life of the improvements or the unexpired period of the lease.

Depreciation/amortisation rates (useful lives) and methods are reviewed at each balance 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 applying to each class of depreciable asset are based on the following useful lives:

	2004	2003
Buildings on freehold land	25-40 years	25-40 years
Leasehold improvements	Lease term	Lease term
Plant and equipment	3-15 years	3-15 years

The aggregate amount of depreciation allocated for each class of asset during the reporting period is disclosed in Note 5C.

#### J. 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.

#### K. Intangibles

ASIO's intangibles comprise purchased software. The asset is carried at cost.

All software assets were assessed for indications of impairment as at 30 June 2004. No impairment write-down was booked.

Intangible assets are amortised on a straight-line basis over their anticipated useful lives.

Useful lives of ASIO's software is 3 to 4 years (2002-03: 3 to 4 years).

#### L. 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 entitlements 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 is estimated to be less than the annual entitlement for sick leave.

The leave liabilities are calculated on the basis of employees' remuneration, including ASIO's employer superannuation contribution rates to the extent that the leave is likely to be taken during service rather than paid out on termination.

The liability for annual leave reflects the value of total annual leave entitlements of all employees at 30 June 2004 and is recognised at the nominal amount.

The liability for long service leave has been determined by reference to Finance Brief 13 issued by Department of Finance and Administration. In determining the present value of the liability, ASIO has taken into account attrition rates and pay increases through promotion and inflation.

### *Superannuation*

Staff of ASIO contribute to 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.

ASIO 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 ASIO's employees.

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

### **M. Taxation**

ASIO is exempt from all forms of taxation except fringe benefits tax and the goods and services tax (GST). Revenues, expenses and assets are recognised net of GST:

- except where the amount of GST incurred is not recoverable from the Australian Taxation Office; and
- except for receivables and payables.

### **N. Foreign currency**

Transactions denominated in a foreign currency are converted at the exchange rate at the date of the transaction. Foreign currency receivables and payables are translated at the exchange rates current as at balance date.

Associated currency gains and losses are not material.

### **O. Insurance**

In accordance with the agreement with the Commonwealth, assets are not insured and losses are expensed as they are incurred. Workers Compensation is insured through Comcare Australia.

### **P. Bad and doubtful debts**

Bad debts are written off during the year in which they are identified.

Where necessary, provision is raised for any doubtful debts based on a review of all outstanding accounts as at year end.

### **Q. Comparative figures**

Where necessary, comparative figures have been adjusted to conform with changes in presentation in these financial statements.

### **R. Rounding**

Amounts have been rounded to the nearest \$1,000 except in relation to the following items:

- appropriations;
- act of grace payments and waivers;
- remuneration of executives; and
- remuneration of auditor.

#### S. Administered items

ASIO does not have any administered items.

#### T. Changes in accounting policy

The accounting policies used in the preparation of these financial statements are consistent with those used in 2002-03, except in respect of:

- the imposition of an impairment test for non-current assets carried at cost (refer note 1J).

#### U. Borrowing costs

Borrowing costs appearing in the Statement of Financial Performance relate to interest charges on leased communications equipment. Refer Note 1E.

### **Note 2: Adoption of AASB Equivalents to International Financial Reporting Standards from 2005-2006.**

The Australian Accounting Standards Board has issued replacement Australian Accounting Standards to apply from 2005-06. The new standards are the AASB Equivalents to International Financial Reporting Standards (IFRSs) which 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.

The purpose of issuing AASB Equivalents to IFRSs is to enable Australian 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.

For-profit entities complying fully with the AASB Equivalents will be able to make an explicit and unreserved statement of compliance with IFRSs as well as with the AASB Equivalents.

It is expected that the Finance Minister will continue to require compliance with the Accounting Standards issued by the AASB, including the AASB Equivalents to IFRSs, in his Orders for the Preparation of Agency financial statements for 2005-06 and beyond.

The AASB Equivalents contain certain additional provisions which will apply to not-for-profit entities, including Australian Government agencies. Some of these provisions are in conflict with the IFRSs and therefore ASIO will only be able to assert compliance with the AASB Equivalents to the IFRSs.

Existing AASB standards that have no IFRS equivalent will continue to apply, including in particular AAS 29 Financial Reporting by Government Departments.

Accounting Standard AASB 1047 *Disclosing the impact of Adopting Australian Equivalents to IFRSs* requires that the financial statements for 2003-04 disclose:

- An explanation of how the transition to the AASB Equivalents is being managed, and
- A narrative explanation of the key differences in accounting policies arising from the transition.

The purpose of this Note is to make these disclosures.

### *Management of the transition to AASB Equivalents to IFRSs*

ASIO has taken the following steps for the preparation towards the implementation of AASB Equivalents:

- The ASIO Audit and Evaluation Committee will oversight the transition to and implementation of AASB Equivalents to IFRSs. The Chief Finance Officer is formally responsible for the project and will report regularly to the Committee on progress against a formal plan that will be approved by the Committee.
- To date a consultant has been engaged and has prepared an impact analysis and has recommended an implementation plan for the adoption of the standards.
- The plan requires the following steps to be undertaken:
  - Quantification of all major accounting policy differences between current AASB standards and the AASB Equivalents to IFRSs as at 30 June 2004 by 31 October 2004.
  - Identification of processes to be able to report under the AASB Equivalents, including those necessary to enable capture of data under both sets of rules for 2004-05, and the testing and implementation of those changes.
  - Identification of processes to be able to report under the AASB Equivalents, including those necessary to enable capture of data under both sets of rules for 2004-05, and the testing and implementation of those changes.
  - Preparation of a transitional balance sheet as at 1 July 2004, under AASB Equivalents, by 31 October 2004.
  - Preparation of an AASB Equivalent balance sheet at the same time as the 30 June 2005 statements are prepared.
  - Meeting reporting deadlines set by the Department of Finance and Administration for the 2005-06 balance sheet under AASB Equivalent Standards.
  - The plan will also address the risks to successful achievement of the above objectives and include strategies to keep implementation on track to meet all deadlines.

### *Major changes in accounting policy*

Changes in accounting policies under AASB Equivalents are applied retrospectively i.e. as if the new policy had always applied. This rule means that a balance sheet prepared under the AASB Equivalents must be prepared as at 1 July 2004, except as permitted in particular circumstances by AASB 1 First-time Adoption of Australian Equivalents to International Financial Reporting Standards. This will enable the 2005-06 statements to report comparatives under the AASB Equivalents also.

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

### *Property, plant and equipment*

Under the new AASB 116 *Property, Plant and Equipment* the cost of an item of property, plant and equipment includes the initial estimate of the costs of dismantling and removing the item and restoring the site on which it is located. A corresponding provision for these costs is also recognised as a liability under the new AASB 137 Provisions, Contingent Liabilities and Contingent Assets.

While ASIO currently recognises a provision for 'make good' on leased premises it does not capitalise this cost in the value of the asset.

### *Sales of non current assets*

Proceeds from the disposal of non-current assets are currently recognised as revenue and the carrying amounts of the asset disposed of are recognised as an expense. Under Australian equivalents to IFRSs, the net of these amounts will be recognised as a gain or loss in the Income Statement.

*Employee benefits*

Currently ASIO measures the liability for annual leave at its nominal amount.

Under the new AASB 119 Employee Benefits, employee liabilities due more than 12 months from reporting date must be discounted to their present value.

**Note 3: Events occurring after reporting date**

There were no events occurring after reporting date which had an effect on the 2004 financial statements.

	2004 \$ '000	2003 \$ '000
<b>Note 4: Operating revenues</b>		
<i>Note 4A: Revenues from Government</i>		
Appropriations for outputs	98,210	85,675
Resources received free of charge	836	562
<b>Total revenues from Government</b>	<b>99,047</b>	<b>86,237</b>
<i>Note 4B: Goods and services</i>		
Provision of goods and services to:		
Related entities	1,763	922
External Entities	230	191
<b>Total sales of goods and services</b>	<b>1,993</b>	<b>1,113</b>
<i>Note 4C: Interest revenue</i>		
Interest on deposits	–	13
<i>Note 4D: Net gains from sale of assets</i>		
Infrastructure, plant and equipment:		
Proceeds from disposal	976	859
Net book value of assets disposed	(959)	(898)
<b>Net gain/(loss) from disposal of infrastructure, plant and equipment</b>	<b>17</b>	<b>(39)</b>
TOTAL proceeds from disposals	976	859
TOTAL value of assets disposed	(959)	(898)
<b>TOTAL net gain from disposal of assets</b>	<b>17</b>	<b>(39)</b>
<i>Note 4E: Other revenues</i>		
Rent	604	475
Miscellaneous	404	248
<b>Total other revenue</b>	<b>1,009</b>	<b>723</b>

**Note 5: Operating expenses***Note 5A: Employee expenses*

	2004 \$ '000	2003 \$ '000
Wages and salary	44,615	35,816
Superannuation	7,086	5,566
Leave and other entitlements	2,308	1,993
Separation and redundancies	498	142
Other employee expenses	6,129	5,005
<b>Total employee benefits expense</b>	<b>60,636</b>	<b>48,522</b>
Workers compensation premiums	432	138
<b>Total employee expenses</b>	<b>61,068</b>	<b>48,660</b>

*Note 5B: Suppliers' expenses*

Goods and services from related entities	8,077	9,213
Goods and services from external entities	19,487	18,048
Operating lease rentals *	5,647	6,010
<b>Total supplier expenses</b>	<b>33,211</b>	<b>33,271</b>

\* These comprise minimum lease payments only.

*Note 5C: Depreciation and amortisation**Depreciation*

Other infrastructure, plant and equipment	6,788	6,876
Buildings	93	54
<b>Total Depreciation</b>	<b>6,881</b>	<b>6,930</b>

*Amortisation*

Intangibles	859	1,145
<b>Total Depreciation and amortisation</b>	<b>7,739</b>	<b>8,075</b>

Depreciation expenses are \$773,900 lower than they would have been as a result of the extension of useful lives of plant and equipment assets and the re-assessment of residual values for assets which have been revalued (2003: nil).

The aggregate amount of depreciation or amortisation expensed during the reporting period for each class of depreciable assets are as follows:

Buildings	93	54
Leasehold improvements	1,480	1,363
Plant and equipment	5,308	5,513
Intangibles	859	1,145
<b>Total</b>	<b>7,739</b>	<b>8,075</b>

	2004 \$ '000	2003 \$ '000
<i>Note 5D: Write down of assets</i>		
<i>Financial assets</i>		
- Bad and doubtful debts expense	13	–
- Foreign exchange variations	12	5
<i>Non-financial assets</i>		
- Plant and equipment written off at stocktake	526	21
- Plant and equipment - other	150	–
- Intangibles written off at stocktake	–	15
<i>Total</i>	<u>700</u>	<u>41</u>

## Note 6: Borrowing costs expense

Leases	<u>24</u>	<u>38</u>
--------	-----------	-----------

## Note 7: Financial assets

### Note 7A: Cash

Cash at bank and on hand	<u>7,216</u>	<u>5,350</u>
All cash is recognised as a current asset		

### Note 7B: Receivables

Goods and services	1,165	1,240
Less provision for doubtful debts	–	–
	<u>1,165</u>	<u>1,240</u>
GST receivable from the Australian Taxation Office	681	791
<i>Total receivables (net)</i>	<u>1,846</u>	<u>2,031</u>

All receivables are current assets

Receivables (gross) are aged as follows:

Not overdue	1,489	1,628
Overdue:		
– less than 30 days	275	194
– 30 to 60 days	36	35
– 60 to 90 days	3	146
– more than 90 days	43	28
	<u>1,846</u>	<u>2,031</u>



<b>2004</b>	<b>2003</b>
<b>\$ '000</b>	<b>\$ '000</b>

## Note 8: Non-financial assets

### Note 8A: Land and buildings

Freehold land - at 2003-04 valuation (fair value)	1,340	944
Buildings on freehold land - at cost	121	-
Accumulated depreciation	-	-
	<u>121</u>	<u>-</u>
Buildings on freehold land - at 2003-04 valuation (fair value)	2,009	1,441
Accumulated depreciation	-	(576)
	<u>2,009</u>	<u>865</u>
Leasehold improvements - at cost	3,578	4,200
Accumulated amortisation	(340)	(396)
	<u>3,239</u>	<u>3,804</u>
Leasehold improvements - at 2003-04 valuation (fair value)	9,841	15,917
Accumulated amortisation	-	(8,749)
	<u>9,841</u>	<u>7,168</u>
<b>Total</b>	<u><u>16,550</u></u>	<u><u>12,781</u></u>

### Note 8B: Infrastructure, plant and equipment

Plant and equipment - at cost	8,930	16,947
Accumulated depreciation	(317)	(3,298)
	<u>8,613</u>	<u>13,649</u>
Plant and equipment - at 2003-04 valuation (fair value)	19,731	26,369
Accumulated depreciation	-	(19,998)
	<u>19,731</u>	<u>6,371</u>
<b>Total</b>	<u><u>28,344</u></u>	<u><u>20,020</u></u>

### Note 8C: Intangibles

Purchased computer software - at cost	9,012	7,714
Accumulated amortisation	(5,941)	(5,083)
<b>Total</b>	<u><u>3,071</u></u>	<u><u>2,631</u></u>

## Note 8D: Analysis of property, plant and equipment and intangibles

Table A - Reconciliation of the opening and closing balances of property, plant and equipment and intangibles

<i>Item</i>	<i>Land</i>	<i>Buildings</i>	<i>Buildings- Leasehold Improvements</i>	<i>Total Buildings</i>	<i>Plant and equipment</i>	<i>Intangibles</i>	<i>Total</i>
	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000
As at 1 July 2003							
Gross book value	944	1,441	20,117	21,558	43,316	7,714	73,532
Accumulated depreciation / amortisation	–	(576)	(9,145)	(9,721)	(23,296)	(5,083)	(38,099)
Net book value	944	865	10,972	11,837	20,020	2,631	35,433
Additions							
by purchase	–	121	2,369	2,490	14,896	1,300	18,685
from acquisition of operations	–	–	–	–	–	–	–
Net revaluation increment/(decrement)	396	1,236	1,213	2,449	373	–	3,217
Depreciation/ amortisation expense	–	(93)	(1,480)	(1,572)	(5,308)	(859)	(7,739)
Recoverable amount write-downs	–	–	–	–	–	–	–
Disposals							
from disposal of operations	–	–	–	–	–	–	–
other disposals	–	–	–	–	(1,634)	–	(1,634)
As at 30 June 2004							
Gross book value	1,340	2,130	13,419	15,549	28,661	9,012	54,562
Accumulated depreciation / amortisation	–	–	(340)	(340)	(317)	(5,941)	(6,598)
<b>Net book value</b>	<b>1,340</b>	<b>2,130</b>	<b>13,080</b>	<b>15,210</b>	<b>28,344</b>	<b>3,071</b>	<b>47,964</b>

Table B — Assets at valuation

<i>Item</i>	<i>Land</i>	<i>Buildings</i>	<i>Buildings- Leasehold Improve- ments</i>	<i>Total Buildings</i>	<i>Plant and equipment</i>	<i>Intangibles</i>	<i>Total</i>
	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000
<b>As at 30 June 2004</b>							
Gross value	1,340	2,009	9,841	11,850	19,731	–	32,921
Accumulated depreciation / amortisation	–	–	–	–	–	–	–
<b>Net book value</b>	<b>1,340</b>	<b>2,009</b>	<b>9,841</b>	<b>11,850</b>	<b>19,731</b>	<b>–</b>	<b>32,921</b>
<b>As at 30 June 2003</b>							
Gross value	944	1,441	15,917	17,358	26,369	–	44,670
Accumulated depreciation / amortisation	–	(576)	(8,749)	(9,324)	(19,998)	–	(29,322)
<b>Net book value</b>	<b>944</b>	<b>865</b>	<b>7,168</b>	<b>8,033</b>	<b>6,371</b>	<b>–</b>	<b>15,348</b>

Table C — Assets held under finance lease

<i>Item</i>	<i>Land</i>	<i>Buildings</i>	<i>Buildings- Leasehold Improve- ments</i>	<i>Total Buildings</i>	<i>Plant and equipment</i>	<i>Intangibles</i>	<i>Total</i>
	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000
<b>As at 30 June 2004</b>							
Gross value	–	–	–	–	326	–	326
Accumulated depreciation/ amortisation	–	–	–	–	–	–	–
<b>Net book value</b>	<b>–</b>	<b>–</b>	<b>–</b>	<b>–</b>	<b>326</b>	<b>–</b>	<b>326</b>
<b>As at 30 June 2003</b>							
Gross value	–	–	–	–	841	–	841
Accumulated depreciation/ amortisation	–	–	–	–	(410)	–	(410)
<b>Net book value</b>	<b>–</b>	<b>–</b>	<b>–</b>	<b>–</b>	<b>431</b>	<b>–</b>	<b>431</b>

Table D - Assets under construction

<i>Item</i>	<i>Buildings</i>	<i>Buildings- Leasehold Improve- ments</i>	<i>Total Buildings</i>	<i>Plant and equipment</i>	<i>Intangibles</i>	<i>Total</i>
	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000
<b>Gross value at 30 June 2004</b>	<b>–</b>	<b>–</b>	<b>–</b>	<b>1,446</b>	<b>–</b>	<b>1,446</b>
<b>Gross value at 30 June 2003</b>	<b>–</b>	<b>–</b>	<b>–</b>	<b>1,219</b>	<b>–</b>	<b>1,219</b>

	2004 \$ '000	2003 \$ '000
<b>Note 8E: Other non-financial assets</b>		
Prepayments	2,398	628
All other non-financial assets are current assets		

## Note 9: Interest bearing liabilities

Finance lease commitments		
Payable:		
within one year	121	242
in one to five years	–	121
Minimum lease payments	121	363
Deduct: future finance charges	(6)	(32)
<b>Net Lease liability</b>	<b>115</b>	<b>331</b>
Lease liability is represented by:		
Current	115	216
Non-current	–	115
<b>Net lease liability</b>	<b>115</b>	<b>331</b>

A finance lease exists in relation to certain communications equipment. The lease is non-cancellable and for a fixed term of five years. ASIO guarantees the residual values. There are no contingent rentals.

## Note 10: Provisions

### Note 10A: Accommodation Leases - make good provision

Accommodation leases - make good	1,487	1,032
----------------------------------	-------	-------

### Note 10B: Employee provisions

Salaries and wages	1,792	1,210
Leave	14,789	12,316
Superannuation	278	191
Other	160	64
<b>Aggregate employee benefit liability and related on-costs</b>	<b>17,019</b>	<b>13,781</b>
Current	8,733	6,706
Non-current	8,286	7,075

**Note 11: Payables****Note 11A: Supplier Payables**

Trade creditors

*Total supplier payables*

Supplier payables are represented by:

Current

Non-Current

*Total supplier payables***2004**  
**\$ '000**2003  
\$ '000

3,854

3,854

3,854

—

3,854

4,523

4,523

4,523

—

4,523

Settlement is usually made net 30 days.

## Note 12: Equity

### Note 12A: Analysis of Equity

Item	Accumulated results		Asset revaluation reserves		Contributed equity		Total equity	
	2004 \$'000	2003 \$'000	2004 \$'000	2003 \$'000	2004 \$'000	2003 \$'000	2004 \$'000	2003 \$'000
Opening balance as at 1 July	(4,649)	270	6,279	6,279	22,144	17,452	23,774	24,001
Net surplus/(deficit)	(679)	(2,038)	–	–	–	–	(679)	(2,038)
Net revaluation increments/ (decrements)	–	–	3,217	–	–	–	3,217	–
Decrease in retained surpluses on application of transitional provisions in accounting standard AASB 1041 Revaluation of Non-current Assets	–	–	–	–	–	–	–	–
Transactions with owner:								
Distributions to owner:								
Returns on Capital								
Capital use charge	–	(2,431)	–	–	–	–	–	(2,431)
Repayment of interest	–	(450)	–	–	–	–	–	(450)
Contributions by owner:								
Appropriations (equity injection)	–	–	–	–	10,637	4,692	10,637	4,692
Closing balance as at 30 June	(5,328)	(4,649)	9,496	6,279	32,781	22,144	36,949	23,774

	<b>2004</b>	2003
	<b>\$ '000</b>	\$ '000

### Note 13: Cash Flow Reconciliation

#### Reconciliation of Cash per Statement of Financial Position to Statement of Cash Flows:

Cash at year end per Statement of Cash Flows	7,216	5,350
Statement of Financial Position items comprising above cash: 'Financial Asset - Cash'	7,216	5,350

#### Reconciliation of net surplus (deficit) to net cash from operating activities:

Net surplus (deficit)	(679)	(2,038)
Depreciation/amortisation	7,739	8,075
Net write down of non-financial assets	676	36
Net loss on disposal of assets	(17)	39
(Increase)/Decrease in receivables	185	(1,290)
(Increase)/Decrease in prepayments	(1,770)	(251)
Increase/(Decrease) in provisions	455	1,032
Increase/(Decrease) in employee provisions	3,237	713
Increase/(Decrease) in supplier payables	(670)	1,184
Provision for interest	-	(450)
<b>Net cash from/(used by) operating activities</b>	<b>9,157</b>	<b>7,051</b>

### Note 14: Executive Remuneration

	2004	2003
The number of executive officers who received or were due to receive a total remuneration of \$100,000 or more:		
\$100 000 to \$109 999	1	-
\$140 000 to \$149 999	-	2
\$150 000 to \$159 999	1	1
\$160 000 to \$169 999	2	3
\$170 000 to \$179 999	1	3
\$180 000 to \$189 999	2	1
\$190 000 to \$199 999	3	2
\$200 000 to \$209 999	-	1
\$210 000 to \$219 999	2	1
\$220 000 to \$229 999	3	-
\$230 000 to \$239 999	1	-
\$260 000 to \$269 999	-	1
\$280 000 to \$289 999	1	-
\$360 000 to \$369 999	1	-
\$370 000 to \$379 999	-	1
\$390 000 to \$399 999	1	-

	2004	2003
The aggregate amount of total remuneration of executive officers shown above.	\$4,328,270	\$3,089,974
The aggregate amount of separation and redundancy/termination benefit payments during the year to executive officers shown above.	\$415,878	Nil

#### Note 15: Remuneration of Auditors

Financial statement audit services are provided free of charge to ASIO.

The fair value of audit services provided was:	<u>\$54,500</u>	<u>\$54,500</u>
No other services were provided by the Auditor-General.		

#### Note 16: Specific payment disclosures

No act of grace payments were made during the reporting period, and there were no amounts owing at year end.

No waivers of amounts owing to the Commonwealth were made pursuant to subsection 34(1) of the *Financial Management and Accountability Act 1997*.

During the reporting period there were 2 payments totalling \$182,600 (2003: nil payments) made under the Defective Administration Scheme.

#### Note 17: Average Staffing Levels

	2004	2003
Full time staff equivalent (FSE) at the end of the year	<u>770</u>	<u>637</u>



## Note 18: Appropriations

Note 18A: Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund (Appropriations) from Acts 1 and 3

Particulars	Total
<b>Year Ended 30 June 2004</b>	<b>\$</b>
Balance carried from previous year	5,350,305
Appropriation Act (No.1) 2003-2004 - basic appropriation	95,236,000
Appropriation Act (No.3) 2003-2004 - basic appropriation	2,974,000
GST refunds (FMA s30A)	4,521,011
Annotations to 'net appropriations' (FMAA s31)	4,823,000
Total appropriations available for payments	112,904,316
Payments made (GST inclusive)	105,688,590
<i>Balance carried to next year</i>	<i>7,215,726</i>

<i>Represented by:</i>	
Cash at bank and on hand	7,215,726
<i>Add: Appropriations not drawn from the OPA</i>	<i>-</i>
<i>Add: Receivables - Goods and Services - GST receivable from customers</i>	<i>69,472</i>
<i>Add: Return of contributed equity</i>	<i>-</i>
<i>Add: Other receivables - Net GST receivable from ATO</i>	<i>680,773</i>
<i>Less: Payable - Suppliers - GST Portion</i>	<i>(750,245)</i>
<b>Total</b>	<b>7,215,726</b>
<i>Reconciliation for Appropriation Acts (Nos. 1 and 3)</i>	
Paid to the entity from the OPA	98,210,000
<i>Add: Finance Minister reduction of Appropriations in current year</i>	<i>-</i>
<i>Add: Administered Appropriation lapsed in current year</i>	<i>-</i>
Not Drawn from the OPA	-
<b>Total Appropriations Acts</b>	<b>98,210,000</b>

Particulars	Total
<b>Year ended 30 June 2003</b>	<b>\$</b>
Balance carried from previous year	6,631,308
Total annual appropriation - basic appropriations	81,087,000
Adjustments and annotations to appropriations	10,380,108
Available for payments	98,098,416
<i>Payments made during the year</i>	<i>91,956,660</i>
<i>Balance carried to the next year</i>	<i>6,141,756</i>
<i>Represented by:</i>	
Cash	5,350,305
GST receivable	791,451
<i>Add: Appropriations receivable</i>	<i>-</i>
<b>Total</b>	<b>6,141,756</b>

FMA = Financial Management and Accountability Act 1997

Act 1 = Appropriations Act (No 1) 2003-2004

Act 3 = Appropriations Act (No 3) 2003-2004

There were no savings offered-up during the year and there have been no savings offered-up in previous years that were still on-going.

**Note 18B: Acquittal of authority to draw cash from the Consolidated Revenue Fund (Appropriations) from Acts 2 and 4**

Particulars	Departmental Capital			Total
	Equity	Loans	Previous years' outputs	
	\$	\$	\$	\$
<b>Year ended 30 June 2004</b>				
Balance carried from previous year	–	–	–	–
Appropriation Act (No.2) 2003-2004	9,129,000	–	–	9,129,000
Appropriation Act (No.4) 2003-2004	1,508,000	–	–	1,508,000
Available for payments	10,637,000	–	–	10,637,000
Payments made (GST inclusive)	10,637,000	–	–	10,637,000
<i>Balance carried to next year</i>	–	–	–	–
<i>Represented by:</i>				
Cash	–	–	–	–
Appropriations not drawn from OPA	–	–	–	–
<b>Year ended 30 June 2003</b>				
Available for payments 2003	4,692,000	–	–	4,692,000
Payments made 2003	4,692,000	–	–	4,692,000
Balance carried to the next year	–	–	–	–
<i>Represented by:</i>				
Cash	–	–	–	–
Appropriations not drawn from the OPA	–	–	–	–

## Note 19: Reporting of Outcomes

### Note 19A: Total Cost/Contribution of Outcomes (Whole of Government)

	Total	
	2004 \$'000	2003 \$'000
Total expenses	103,702	90,983
Costs recovered from provision of goods and services to the non-government sector	230	191
Other external revenues		
Interest on cash deposits	–	13
Revenue from disposal of assets	976	859
Other	1,009	723
Goods and services revenue from related entities	2,600	1,484
<b>Net cost / (contribution) of outcome</b>	<b>98,888</b>	<b>87,713</b>

### Note 19B: Major Revenues and Expenses by Output Group

	Total	
	2004 \$'000	2003 \$'000
<b>Operation Revenues</b>		
Revenues from government	99,046	86,237
Sale of goods and services	1,992	1,113
Other non-taxation revenues	1,984	1,596
<b>Total operating revenues</b>	<b>103,023</b>	<b>88,945</b>
<b>Operating expenses</b>		
Employees	61,068	48,660
Suppliers	33,211	33,271
Depreciation and amortisation	7,739	8,075
Other	1,659	940
<b>Total operating expenses</b>	<b>103,678</b>	<b>90,945</b>

**Note 20A: Interest rate risk**

Financial Instrument	Notes	Floating Interest Rate		Fixed Interest Rate Maturing In				Non-Interest Bearing	Total		Weighted Average Effective Interest Rate		
				1 year or less	1 to 5 years		> 5 years						
		2004 \$'000	2003 \$'000	2004 \$'000	2003 \$'000	2004 \$'000	2003 \$'000	2004 \$'000	2003 \$'000	2004 \$'000	2003 \$'000	2004 %	2003 %
Financial Assets													
Cash at bank	7A	7,216	5,350	-	-	-	-	-	-	7,216	5,350	-	2.0
Receivables for goods and services (gross)	7B	-	-	-	-	-	-	-	-	15	538	n/a	n/a
Total		7,216	5,350	-	-	-	-	-	-	15	538	7,230	5,888
Total Assets										59,424	43,441		

[illegible]

## Note 20B: Net fair values of financial assets and liabilities

		2004		2003	
		Total carrying amount	Aggregate net fair value	Total carrying amount	Aggregate net fair value
	Note	\$'000	\$'000	\$'000	\$'000
Departmental Financial Assets					
Cash at bank	7A	7,216	7,216	5,350	5,350
Receivables for goods and services (net)	7B	15	15	538	538
<i>Total Financial Assets</i>		<u>7,230</u>	<u>7,230</u>	<u>5,888</u>	<u>5,888</u>
Financial Liabilities (Recognised)					
Finance lease liabilities	9	115	115	331	331
Trade creditors	11A	3,702	3,702	2,470	2,470
<i>Total Financial Liabilities (Recognised)</i>		<u>3,817</u>	<u>3,817</u>	<u>2,801</u>	<u>2,801</u>

*Financial assets*

The net fair values of cash and non-interest bearing monetary financial assets approximate their carrying amounts.

*Financial liabilities*

The net fair value of the finance lease is based on discounted cash flows using current interest rates for liabilities with similar risk profiles.

The net fair values for trade creditors are short-term in nature and are approximated by their carrying amounts.

## Note 20D: Credit risk exposures

ASIO'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 Position.

ASIO has no significant exposures 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 21: Assets held in trust

### Special Accounts

ASIO has an *Other Trust Monies Special Account* and a *Services for Other Government & Non-Agency Bodies Account*. For the years ended 30 June 2004 and 30 June 2003, both special accounts had nil balances and there were no transactions debited or credited to them.

The purpose of the *Other Trust Monies Special Account* is for expenditure of moneys temporarily held on trust or otherwise for the benefit of a person other than the Commonwealth.

The purpose of the *Services for Other Government & Non-Agency Bodies Account* is for expenditure in connection with services performed on behalf of other governments and bodies that are not Agencies under the *Financial Management and Accountability Act 1997*.

### Comcare

During 2003-2004 compensation payments made by Comcare amounted to \$71,154 (2003: \$60,234). This represented reimbursement of expenses previously paid by ASIO to staff and health care professionals.

Part 5

# Appendices





## Appendix A

### Membership of the Parliamentary Joint Committee on ASIO, ASIS and DSD

---

Membership of the PJCAAD during the reporting year comprised:

Hon. David Jull, MP (Chair)	(LP, Fadden, QLD)
Senator Sandy Macdonald	(NP, NSW)
Senator the Hon. Robert Ray	(ALP, VIC)
Hon. Kim Beazley, MP	(ALP, Brand, WA)
Mr Stewart McArthur, MP	(LP, Mallee, VIC)
Hon. Leo McLeay, MP	(ALP, Watson, NSW)
Senator Alan Ferguson	(LP, SA)

## Appendix B

### Contact Information

---

#### Written inquiries

The Director-General of Security  
ASIO Central Office  
GPO Box 2176  
CANBERRA ACT 2601

#### General inquiries

Central Office switchboard	Tel: 02 6249 6299 1800 020 648 (toll free)
	Fax: 02 6257 4501

#### Media inquiries

Media Liaison Officer	Tel: 02 6249 8381
	Fax: 02 6262 9547

#### State and Territory Office telephone inquiries

Australian Capital Territory	02 6249 7415
Victoria	03 9654 8985
New South Wales	02 9281 0016
Queensland	07 3831 5980
South Australia	08 8223 2727
Western Australia	08 9221 5066
Northern Territory	08 8981 2374
Tasmanian residents may call	
ASIO Central Office toll free	1800 020 648

#### Website

[www.asio.gov.au](http://www.asio.gov.au)

## Appendix C

### Staffing Statistics

**Table A. Staffing levels and number at 30 June, 1999–00 to 2003–04**

	1999–2000	2000–01	2001–02	2002–03	2003–04
<b>Full-time staff equivalent (FSE) at end of each FY</b>	565	551	597	637	770
<b>Number of staff at the end of each FY</b>	605	584	618	668	805

**Table B. Composition of the workforce (number at 30 June each year)**

	1999–2000	2000–01	2001–02	2002–03	2003–04
<b>Permanent full-time</b>	469	453	497	536	603
<b>Temporary full-time</b>	77	63	58	51	103
<b>Permanent part-time</b>	20	26	25	28	38
<b>Temporary part-time</b>	10	14	18	23	28
<b>Casual</b>	22	25	19	30	33
<b>Non-operational (including unattached and on compensation)</b>	7	3	1	–	–
<b>Total</b>	<b>605</b>	<b>584</b>	<b>618</b>	<b>668</b>	<b>805</b>

**Table C. SES equivalent staff classification and gender (positions at level) at 30 June each year**

	1999–2000	2000–01	2001–02	2002–03	2003–04
<b>Band 1 Female</b>	1	1	2	2	2
<b>Male</b>	9	9	8	9	9
<b>Band 2 Female</b>	1	1	1	1	1
<b>Male</b>	2	2	2	4	4
<b>Band 3 Male</b>	1	1	1	1	1
<b>Total</b>	<b>14</b>	<b>14</b>	<b>14</b>	<b>17</b>	<b>17</b>

**Note** – Figures in Table C do not include the Director-General.

## Appendix D

# Workplace Diversity Statistics

**Table A. Representation of designated groups within ASIO at 30 June 2004**

Group	Total staff <sup>1</sup>	Women	Race/ Ethnicity <sup>2</sup>	ATSI <sup>3</sup>	PWD <sup>4</sup>	Available EEO data <sup>5</sup>
<b>SES (inc DG)</b>	18	3	0	0	0	18
<b>Senior Officers<sup>6</sup></b>	158	39	14	0	3	146
<b>AO5<sup>7</sup></b>	302	123	46	1	5	266
<b>AO1–4<sup>8</sup></b>	292	159	15	2	9	272
<b>ITO1–2<sup>9</sup></b>	33	7	3	0	0	31
<b>ENG1–2<sup>10</sup></b>	2	0	0	0	0	2
<b>Total</b>	<b>805</b>	<b>331</b>	<b>78</b>	<b>3</b>	<b>17</b>	<b>735</b>

1. Based on staff salary classifications recorded in ASIO's personnel system.
2. Previously NESB – Non-English-speaking background.
3. Aboriginal and Torres Strait Islander.
4. People with a disability.
5. Provision of EEO data by staff is voluntary.
6. The Senior Officer group is the equivalent to the APS EL1 and EL2 classifications and includes equivalent officers in the Engineer and Information Technology classifications.
7. The AO5 (ASIO Officer Grade 5) group is equivalent to APS Level 6 and includes ASIO Generalist Intelligence Officers.
8. The AO1–4 group spans the APS 1–5 salary range. Salaries for Generalist Intelligence Officer Trainees are included in this group (equivalent to APS grade 3).
9. Information Technology Officers grades 1 and 2.
10. Engineers grades 1 and 2.

**Table B. Percentage representation of designated groups in ASIO 2000–2004**

Group	June 2000	June 2001	June 2002	June 2003	June 2004
<b>Women<sup>1</sup></b>	40	40	40	42	41
<b>Race / Ethnicity<sup>2</sup></b>	8	6	11	12	11
<b>ATSI<sup>3</sup></b>	0.4	0.3	0.75	0.74	0.41
<b>PWD<sup>4</sup></b>	4	3	4	4	2

1. Percentages for women based on total staff; percentages for other groups based on staff for whom EEO data was available.
2. Previously NESB – Non-English-speaking background.
3. Aboriginal and Torres Strait Islander.
4. People with a disability.

## Appendix E

### ASIO Salary Classification Structure at 30 June 2004

#### ASIO MANAGERS

SES Band 3	\$153 652	minimum point	
SES Band 2	\$121 447	minimum point	
SES Band 1	\$101 860	minimum point	
AEO 3	\$90 277		
AEO 2	\$81 898	to	\$90 277
AEO 1	\$72 216	to	\$77 951

#### GENERALIST INTELLIGENCE OFFICERS

GIO	\$40 668	to	\$62 897
-----	----------	----	----------

#### ASIO OFFICERS

ASIO Officer 5	\$55 142	to	\$62 897
ASIO Officer 4	\$45 479	to	\$49 644
ASIO Officer 3	\$39 660	to	\$42 734
ASIO Officer 2	\$34 925	to	\$38 632
ASIO Officer 1	\$30 955	to	\$34 124

#### ASIO ITOs

SITOA	\$90 277		
SITOB	\$81 898	to	\$90 277
SITOC	\$72 216	to	\$77 951
ITO2	\$55 142	to	\$62 897
ITO1	\$42 734	to	\$49 644

#### ASIO ENGINEERS

SIO(E)5	\$91 711		
SIO(E)4	\$81 898	to	\$90 277
SIO(E)3	\$72 216	to	\$77 951
SIO(E)2	\$55 142	to	\$62 897
SIO(E)1	\$42 734	to	\$49 644

## Appendix F

### Assumed Identities

---

#### Commonwealth Legislation

During the period 1 July 2003 to 30 June 2004, 168 assumed identity approvals were granted to officers in accordance with the *Crimes Act 1914*. Of these, 21 approvals were varied and 4 were revoked.

The general nature of the duties undertaken by those officers under the assumed identities concerned:

- intelligence collection
- operational support
- intelligence training
- administrative support
- surveillance.

The most recent audit required in accordance with Section 15XU of the Act was conducted in July 2004 for the preceding financial year. The audit did not disclose any fraud or other unlawful activity.

#### New South Wales Legislation

During the year 46 assumed identity approvals were granted in accordance with the *NSW Law Enforcement and National Security (Assumed Identities) Act 1998*. Of these, 1 approval was varied and 2 were revoked.

The general nature of the duties undertaken by those officers under the assumed identities concerned:

- intelligence collection
- operational support
- surveillance.

The most recent audit required in accordance with Section 11 of the Act was completed in July 2004 for the preceding financial year. The audit did not disclose any fraudulent or other criminal behaviour.

## Glossary of Acronyms and Abbreviations

---

AAT	Administrative Appeals Tribunal
ACS	Australian Customs Service
AFP	Australian Federal Police
AIC	Australian Intelligence Community
ANSTO	Australian Nuclear Science and Technology Organisation
ASIC	Aviation Security Identity Card
ASIS	Australian Secret Intelligence Service
CBRN	Chemical, Biological, Radiological or Nuclear (weapons or terrorism)
C/CSP	Carrier/Carriage Service Provider
CIAC	Critical Infrastructure Advisory Council
CTORG	Counter-Terrorist Overseas Response Group
DFAT	Department of Foreign Affairs and Trade
DIGO	Defence Imagery and Geospatial Organisation
DIMIA	Department of Immigration and Multicultural and Indigenous Affairs
DIO	Defence Intelligence Organisation
DOTARS	Department of Transport and Regional Security
DSD	Defence Signals Directorate
IAAG	Industry Assurance Advisory Group
IASF	Inter-Agency Security Forum
JCTICU	Joint Counter-Terrorism Intelligence Coordination Unit
MAL	Movement Alert List
NATEX	National Anti-Terrorist Exercise
NCTC	National Counter-Terrorism Committee
NCTP	National Counter-Terrorist Plan
NIG	National Intelligence Group
ONA	Office of National Assessments
OPREX	Operational Response Exercise
PJCAAD	Parliamentary Joint Committee on ASIO, ASIS and DSD
PM&C	Department of the Prime Minister and Cabinet
PMV	Politically motivated violence
PSCC	Protective Security Coordination Centre
PSM	Protective Security Manual
PSPC	Protective Security Policy Committee
RMU	Research and Monitoring Unit
SCNS	Secretaries Committee on National Security
TSCM	Technical surveillance counter-measures
TSU	Technical Support Unit
WMD	Weapons of mass destruction

## Compliance Index

---

Annual Report requirement	Page
Assumed identities	108
Advertising and market research	56
Certified agreements and AWAs	54
Consultants and contractors	62–3
Contact details	104
Corporate governance	49
Disability strategy	59
Environmental performance	61–2
External scrutiny	51–2
Financial performance	13
Financial statements	65–100
Fraud control measures	50–1
Freedom of Information	26
Glossary	109
Index	111–16
Internet home page address and Internet address for report	104
Letter of transmittal	iii
Management of human resources	54–9
Occupational health and safety	59
Organisational structure	8
Outcome and Output structure	9–10
Overview of agency	8
Performance pay	54
Purchasing	62
Report on performance	11–45
Resource tables by outcomes	13
Review by Director-General	3–7
Roles and functions	8–10
Staffing statistics	105–6
Summary resource table	13
Table of contents	v
Warrants issued under section 34D of the <i>ASIO Act 1979</i>	39–40



## General Index

### A

Abu Sayyaf Group, 19  
 accountability, 50–2, 56, 57  
 Administrative Appeals Tribunal (AAT), 18, 28  
 advertising costs, 56  
 al-Qa'ida, 3, 14, 15, 16, 17–19  
 ammonium nitrate, 32  
 Ansar al-Islam, 19  
 ANZAC ceremony, 44  
 appeal mechanisms, 28, 30  
 archival records, access to, 26–8  
*Archives Act 1983*, 26, 51  
 Armed Islamic Group, 19  
 Asbat al-Ansar, 19  
 ASIO Act 1979, *See* legislation, Commonwealth  
*ASIO Now*, 53  
 ASIO staff, *See* staff  
 assumed identities, 50, 51, 108  
 Attorney-General, ix, 6, 8, 18, 22, 23, 29, 33, 36, 38, 39, 41, 43, 49, 51, 53  
 audit and evaluation, 32–4, 40, 49, 50–1, 59, 61, 63, 108  
 Auditor-General, 51  
 Australian Customs Service (ACS), 43  
 Australian Federal Police (AFP), 3, 6, 8, 15, 16, 17, 18, 38, 42, 43, 44, 57  
 Australian Government Counter-Terrorism Committee (AGCTC), 37  
 Australian National Audit Office, 33, 49  
 Australian Secret Intelligence Service (ASIS), 6, 8, 23, 31, 43, 44, 45, 57  
 Australian Transaction Reports and Analysis Centre (AUSTRAC), 51  
 aviation security, 21, 31–2  
 Aviation Security Identification Card (ASIC), 13, 31  
 Australian Taxation Office, 51  
 Ayub, Abdul Rahim, 16

### B

Bali bombing, 15, 16, 25, 53  
 Bashir, Abu Bakar, *See* Jemaah Islamiyah

biological warfare, *See* WMD  
 border control, *See* visa checking  
 Brigitte, Willy, 3, 7, 17, 42  
 budget, 6, 32, 49, 51, 56  
 budget oversight, 51  
 building management, 61  
 business continuity, 50

### C

capabilities, *See* investment in capabilities  
*Charter of the United Nations (Terrorism and Dealing with Assets) Regulations 2002*, 19  
 chemical, biological, radiological or nuclear (CBRN) threats, *See* WMD  
 client survey, 14  
 Commonwealth Heads of Government Meeting (CHOGM), 44  
 communications, *See* information management  
 compensation claims, 59  
 complaints about ASIO, 53  
 compliance index, 110  
 computer attack, *See* critical infrastructure  
 computer exploitation, *See* warrant operations  
   – computer access  
 consultants and contractors, 62–3  
   – exempt contracts 63  
 contact information, 104  
 Contact Reporting Scheme, 32  
 corporate committees, 49, 54, 57  
 corporate governance, 49  
*Corporate Plan 2002–2006*, ix, 49–50  
 cost recovery, 33  
 Council of Australian Governments, 32  
 counter-espionage, 6, 21  
 counter-intelligence, *See* security of ASIO  
 counter-proliferation, *See* WMD  
 counter-terrorism capability, 3, 6, 13, 36, 37–8  
 counter-terrorism exercises, 13, 38, 42  
 Counter-Terrorism Overseas Response Group (CTORG), 38  
 critical infrastructure, 3, 6, 14, 21–2, 33, 38, 42  
 Critical Infrastructure Advisory Council (CIAC), 21–2

## D

Defence Imagery and Geospatial Organisation (DIGO), 6, 23, 43, 57  
 Defence Intelligence Organisation (DIO), 6, 8, 23, 57  
 Defence Science and Technology Organisation (DSTO), 6, 44, 57  
 Defence Signals Directorate (DSD), 6, 23, 35, 43, 44, 45, 57  
 Department of Defence, 29, 30, 31  
 Department of Foreign Affairs and Trade (DFAT), 6, 8, 19, 23, 24–5, 29, 38, 43, 57  
 Department of Immigration and Multicultural and Indigenous Affairs (DIMIA), 5, 24–5, 26, 29, 31, 43  
 Department of Transport and Regional Services (DOTARS), 6, 21, 23, 57  
 diplomatic premises, threats to, 24  
 Direction de la Surveillance du Territoire (DST), 17  
 Director-General, 7, 8, 37, 39, 49, 51, 52, 53, 63  
 disability strategy, 59

## E

ecologically sustainable development, 61–2  
 EEO, *See* workplace diversity  
 Egyptian Islamic Jihad, 19  
 electronic and audio counter-measures, *See* technical surveillance counter-measures  
*Emerging Issues in Protective Security* paper, 29  
 engineering development, *See* technical capabilities and development  
 entry and search of premises, *See* warrant operations – entry and search  
 entry to Australia, controls on, *See* visa checking  
 environmental performance, 61–2  
 equal employment opportunity, *See* workplace diversity  
 equipment testing, *See* security equipment testing and standards  
 e-security, *See* critical infrastructure  
 espionage, *See* counter-espionage  
 evaluation, *See* audit and evaluation  
 external scrutiny, *See* accountability

## F

Fadilah, Lutfi, 15  
 financial investigations, 19  
 financial statements, 65–100  
 foreign intelligence collection, 6, 9, 45  
 foreign interference, 14, 21, 32  
 foreign liaison, *See* liaison with overseas agencies  
 fraud control, 50  
*Freedom of Information Act 1982*, 26

## G

‘Gatekeeper’ accreditation, 34  
 Greek Olympics Advisory Security Group (OAG), 43  
*Guidelines for the Collection of Intelligence*, 36, 51  
 Gunawan, Rusman, 15

## H

Habib, Mamdough, 18  
 Hambali, 15, 16  
 HAMAS, 19  
 Harakat-ul-Mujahideen, 19  
 Hicks, David, 18  
 Hizballah, 19  
 human resource management, *See* staff  
 human source intelligence, 36, 41  
 Husin, Azahari bin, 16

## I

Idris, 16  
 illegal arrivals, *See* visa checking  
 Indonesia, 3, 15, 26  
 industrial democracy, *See* staff – workplace relations  
 industry, engagement with, 21, 22, 32  
 Industry Assurance Advisory Group (IAAG), 22  
 information management, 10, 50, 59–60  
 – Communications Centre, 59  
*Information Management Strategic Plan 2004–2008*, 50, 59  
 infrastructure, *See* critical infrastructure  
*Inquiry into the Assessment of Threats to the Security of Australians in South-East Asia*, 52

*Inquiry into Security Issues*, 29, 31, 60  
 Inspector-General of Intelligence and Security (IGIS), 16, 27, 39, 40, 50, 51–2  
 – *Annual Report*, 52  
 Inter-Agency Security Forum (IASF), 29  
 – *Status of Security Report*, 29  
 Inter-departmental Emergency Task Force (IDETF), 38  
 internal security, *See* security of ASIO  
 Internet interception, *See* warrant operations – computer access  
 investigative priorities, 15, 17, 20  
 Iraq, 3, 4, 20, 25  
 Islamic Army of Aden, 19  
 Islamic community, attacks on, 20  
 Islamic Movement of Uzbekistan, 19  
 Islamist extremism, 15, 17

## J

Jaish-e-Mohammed, 19  
 Jakarta bombing, 3, 15  
 Jemaah Islamiyah, 3, 4, 15–16, 19  
 – Bali bombing, 15, 16, 25, 53  
 Jewish community, attacks on, 20  
 Joint Counter-Terrorism Intelligence Coordination Unit (JCTICU), 43

## K

Khazaal, Belal, 15, 18  
 Khazaal, Maher, 18

## L

Lashkar-e-Tayyiba (LeT), 19  
 Lashkar-I-Jhangvi, 19  
 Leader of the Opposition, ix, 49, 51  
 legislation (Commonwealth):  
 – *Archives Act 1983*, 26  
 – *Australian Security Intelligence Organisation Act 1979*, ix, 17, 36, 39  
 – *ASIO Legislation Amendment Act 2003*, 36  
 – *Communications Legislation Amendment Bill (No. 2) 2003*, 41  
 – *Crimes Act 1914*, 41, 50, 108  
 – *Crimes (Internationally Protected Persons) Act 1976*, 16  
 – *Criminal Code Act 1995*, 15, 18, 19

– *Freedom of Information Act 1982*, 26, 63  
 – *Telecommunications Act 1997*, 40  
 – *Telecommunications (Interception) Act 1979*, 37  
 – *Telecommunications (Interception) Amendment Act 2004*, 37  
 – *Telecommunications (Interception) Amendment Bill 2004*, 41  
 – *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004*, 41

legislation (NSW):

– *Law Enforcement and National Security (Assumed Identities) Act 1998*, 50, 108

liaison with Australian agencies, 42–3

liaison with overseas agencies, 43–4

Liberation Tigers of Tamil Eelam (LTTE), 19

locksmith accreditation, 34

Lohdi, Faheem Khalid, 15, 17

## M

Mallah, Zeky, 15  
 management and accountability, 49–63  
 management structure, 8  
 Marriott Hotel bombing, 15  
 media policy, 53  
 Mohammed, Omar Abdi, 18  
 Morocco, 3  
 Movement Alert List (MAL), *See* visa checking

## N

National Anti-Terrorism Exercise (NATEX),  
*See* counter-terrorism exercises  
 National Archives of Australia, 26–8  
 National Counter-Terrorism Committee (NCTC), 6, 13, 21, 37–8  
*National Counter-Terrorism Handbook*, 38  
 National Counter-Terrorism Plan (NCTP), 37–8  
 National Intelligence Group (NIG), 38  
 National Security Committee of Cabinet (NSC), ix, 5, 29, 49  
 National Security Hotline, 5, 42, 50  
 National Threat Assessment Centre (NTAC), 5, 8, 13, 22–3, 42, 52, 57, 58, 59, 61  
 nuclear proliferation, *See* WMD

## O

occupational health and safety, 59

- compensation claims, 59

Office of National Assessments (ONA), 6, 8, 23, 31, 57, 61

Olympic Games:

- Athens 2004 Games, 43
- Athens 2004 Paralympics, 43
- Beijing 2008 Games, 44

open source information, 4, 9, 36, 41–2

organisational structure, *See* management structure

Osama bin Laden, *See* al-Qa'ida

Outcome structure, 9–10

Outputs:

- enabling, 10
- executive, 10
- foreign intelligence, 9, 45
- price of, 13
- protective security advice, 3, 6, 9, 29–35, 36
- security intelligence analysis & advice, 9, 14–28
- security intelligence investigation & capability, 9, 36–44

Output performance, 13–45

## P

Palestinian Islamic Jihad, 19, 52

Parliamentary Committees, 7, 52

Parliamentary Joint Committee on ASIO, ASIS and DSD (PJCAAD), 51, 52, 62, 63, 103

passport cancellations, 3–4, 17–18

people management, *See* staff

performance pay, 54

performance reporting, 13–45

personnel security assessments, 5, 29–32

- adverse and qualified assessments, 5, 31
- appeals, 30
- Aviation Security Identification Cards (ASIC), 13, 31–2
- vetting for AIC, 31

physical security, 9, 29, 32–3, 60–1

- cost recovery, 33

police, State and Territory, liaison with, 3, 14, 17, 20, 22, 38, 39, 42

politically motivated violence (PMV):

- Bali, 15, 16, 25, 53
- foreign-influenced, 14–15, 19
- local, 14, 20
- 11 September, 6, 14, 17, 53

polygraph trial, 32

Prime Minister, ix, 23

proliferation, *See* WMD

proscribed organisations, 5, 15, 17, 18, 19, 52

protective security, 3, 6, 9, 29–35, 36

- Protective Security Coordination Centre (PSCC), 34
- safehand and overnight couriers, 34
- training, 50, 52–3

protest activity, *See* politically motivated violence – local

public, ASIO contact with, 7, 20, 53

purchasing, 62

## Q

Questioning and detention, *See* warrant operations – questioning and detention powers

## R

Rais, Muhammad, 15

recruitment, *See* staff – recruitment

Research and Monitoring Unit, 4, 42

risk management advice, *See* protective security

Roche, Jack, 4, 5, 16

Russell Passive Defence Project, 60

## S

safehand and overnight couriers, 34

Salafist Group for Call and Combat, 19

salary classification structure, 107

Saudi Arabia, 3

searches, *See* warrant operations – entry and search

Secretaries Committee on National Security (SCNS), 29, 32

security assessments, personnel, *See* personnel security assessments

security clearances, *See* personnel security assessments and staff – security clearances

Security Construction and Equipment Committee (SCEC), 34, 35

*Security Equipment Catalogue*, 32, 35

security equipment testing and standards, 35

security intelligence analysis & advice, 9, 14–28

security intelligence investigation & capability, 9, 36–44

*Security Management Plan 2001–2004*, 50

security of ASIO, 10, 13, 33, 60–1

Senate Estimates, 52

Senate Foreign Affairs, Defence and Trade References Committee, 52

Senate Legal and Constitutional Legislation Committee, 41, 51, 52

Shipping, threats to, 21

Siliwangi, Sardono, 15

Singapore, 16

Spain, 3

special powers, *See* warrant operations – questioning and detention powers

Staff:

- advertising costs, 56
- attrition rate, 55
- Employee Assistance Program, 60
- graduate traineeship, 57
- people management priorities, 54
- performance management, 54, 56
- performance pay, 54
- recruitment, 6, 54–6, 58
- retention, 55
- salary classification structure, 107
- secondments, 57
- security clearances, 9, 55, 60
- staffing profile, 55
- statistics, 6, 54, 105–6
- training and development, 6, 7, 56–8, 59
- workplace diversity, 58, 59, 106
- workplace relations, 7, 54

Staff Association, 49, 52, 54

Status of Security Report, 29

surveillance, 4, 9, 36, 41, 42, 55, 56, 108

sweeps, *See* technical surveillance counter-measures

## T

Tamil extremism, *See* LTTE

technical capabilities and development, 6, 9, 44, 56

technical surveillance counter-measures (TCSM), 9, 29, 35

telecommunications interception, *See* warrant operations – telecommunications interception

terrorism, *See* politically motivated violence

terrorist finances, *See* financial investigations

terrorist groups, proscription of, *See* proscribed organisations

Terrorist Threat Crisis Group (TTCG), 23

terrorist training, 4, 17

threat assessments, 5, 6, 9, 20–4, 42

threat levels, 3, 14, 22–4

Top, Noor Din, 16

Top Secret certification, 32, 34

training and development, *See* staff – training and development

travel advisories, 23–4

Trusted Information Sharing Network (TISN), 22

Turkey, 3, 44

## U

Ul-Haque, Izhar, 17

unauthorised arrivals, *See* visa checking

United Nations Security Council, 19

Usama bin Laden, *See* al-Qa'ida

## V

vetting, *See* personnel security assessment

violent protest activity, *See* politically motivated violence – local

visa checking, 5, 9, 14, 24–6

- Movement Alert List (MAL), 24
- recommendations against entry, 25–6
- unauthorised arrivals, 25, 26

## W

warrant operations, 36, 38–41

- approvals, 39, 51

- computer access, 36, 38
  - emergency warrants, 39
  - entry and search, 36, 38, 42
  - examination of postal and delivery service articles, 36, 38
  - external scrutiny, 40
  - listening devices, 36, 38
  - questioning and detention powers, 5, 36–7, 39–40
  - security intelligence warrants, 39
  - telecommunications interception, 5, 36, 37, 38, 40, 41
  - tracking devices, 36, 38
- weapons of mass destruction (WMD), 6, 19, 33
- website, ASIO, 36, 50, 53, 56
- women in ASIO, 58–9, 106
- Workplace Agreement, 54, 59
- workplace diversity, 58, 59, 106
- workplace relations, 54

## **Z**

Zawahiri, Ayman, 14, 17

Zulkarnaen, 16