

Australian Security
Intelligence Organisation

Report to Parliament
2002-2003

© Commonwealth of Australia

ISSN 0815-4562

ISBN 0-9751485-0-8

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: 9408/03

28 November 2003

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 2003.

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

A handwritten signature in black ink that reads "Dennis Richardson".

Dennis Richardson
Director-General of Security

FOI WARNING: Exempt document under *Freedom of Information Act 1982*. Refer related FOI requests to Attorney-General's Department, Canberra.

Contents

ASIO and its Annual Report	ix
PART 1: OVERVIEW	1
The Year in Review	3
Agency Overview	6
PART 2: OUTPUT PERFORMANCE	9
Output 1: Security Intelligence Analysis and Advice	12
Output 2: Protective Security Advice	28
Output 3: Security Intelligence Investigation and Capability	35
Output 4: Foreign Intelligence	43
PART 3: MANAGEMENT AND ACCOUNTABILITY	45
Governance	47
Accountability	48
Our People	52
Information Management	57
Security of ASIO	58
Building Management	60
Purchasing	61
Consultants and Contractors	62
PART 4: FINANCIAL STATEMENTS	63
PART 5: APPENDIXES	101
A. Membership of the Parliamentary Joint Committee on ASIO	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*

What ASIO does

The Australian Security Intelligence Organisation (ASIO) is Australia's national 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, attacks on Australia's defence system or acts of foreign interference. These are the 'heads of security' which provide the direction for ASIO's work.

ASIO provides Government with security intelligence advice 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 the *Corporate Plan* which is available on our website at www.asio.gov.au

ASIO reports to the Attorney-General. Oversight arrangements include the Inspector-General of Intelligence and Security, the Parliamentary Joint Committee on ASIO, ASIS and DSD, and the Auditor-General.

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, the Leader of the Opposition and members of the Secretaries' Committee on National Security.

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

Part 1

Overview



The Security Environment

ASIO's central challenge is the successful management of the twin demands of significant organisational growth and of a continued heightened operational tempo. The challenge will not ease over the next 2-3 years at least.

Counter-terrorism issues continue to dominate. The October 2002 Bali bombings by Jemaah Islamiyah demonstrated the presence of a highly capable terrorist group in our region. Statements by senior al-Qa'ida figures continued to underline the fact that Australia and our interests abroad are seen as legitimate targets. Bali and Iraq dominated the reporting period.

In general, the terrorist threat to Australian interests was higher overseas than at home. We assessed the overall threat level in Australia as *Medium*, but *High* for Australian interests in much of South East Asia, South Asia, the Middle East and parts of East Africa.

The dramatic increase in the volume of information being shared between countries and between agencies since 11 September has had implications for ASIO's information management systems and analytical processes. The need for sharp prioritisation and good, steady judgement under pressure, has never been greater.

Protecting people and property

Our focus has been on those Australian citizens and residents who have trained with terrorist groups overseas and on Jemaah Islamiyah.

We contributed to the post-Bali investigation, deploying officers to Bali on 12 October 2002 and forming a team in Canberra to support the Australian Federal Police (AFP).

Following on from the 2001-02 Jemaah Islamiyah investigations, we conducted enter and search operations which drew some public criticism. Each of the operations was approved within the legal framework and met the national security test in the relevant legislation. The intelligence dividend was significant.

We also continued to investigate Australians who have trained with al-Qa'ida and other terrorist groups. A number are known to have received terrorist training in Afghanistan and Pakistan. There are almost certainly others about whom we are not aware.

The overall threat level in Australia is unlikely to fall below *Medium* in the foreseeable future. Intelligence obtained in 2002-03 confirms Australia was viewed as a target by al-Qa'ida prior to 11 September and continues to be seen in this light.

Our work on counter-terrorism continued to increase:

- The National Security Hotline, established in December 2002, had referred 7 537 calls to ASIO by 30 June, of which 1 049 contained sufficient information to initiate investigations, and 141 are still being pursued.
- The number of Threat Assessments produced in 2002-03 rose 15% from 1786 to 2055.

We provided advice on the threat from local politically motivated violence.

There were reports of harassment, threats and some acts of violence against members of the Australian Islamic community. Anti-Jewish harassment also increased, although violent attacks were fewer than in the previous year.

We delivered training in risk analysis, protective security and the integration of intelligence and border control to a number of Pacific countries.

We also participated in the Greek Olympics Advisory Security Group, which provides advice in relation to the 2004 Olympics.

Protecting Government business and national infrastructure

ASIO received 14 272 requests for personnel security assessments in 2002-03 — a 16% increase on 2001-02. Two adverse and three qualified assessments were issued.

Temporary visa applications (96%), and permanent visa applications (85%), were assessed within agreed timeframes — effectively meeting our benchmarks.

On advice from ASIO, DFAT expelled an Iraqi diplomatic visa holder.

Five visa applicants were refused entry to Australia because of their assessed involvement in terrorist activities, and two because they were assessed as likely to engage in espionage activities.

Our protective security advice to clients increased by 20%, reflecting heightened awareness of the need to protect Commonwealth resources, staff and visitors. We conducted 94 technical surveillance counter-measure sweeps compared to 64 in 2001-02.

We are finalising a confidential report on the use of the polygraph for security vetting.

Seven Threat Assessments relating to national infrastructure protection were produced during the period.

Enhancing capabilities

ASIO was restructured in 2003 — expanding from three to five divisions, putting in place the management framework within which the Organisation can expand over the next few years.

We invested \$1.73 million (about 2.1% of budget) on training and developing our people in generic and job-specific skills, supplementing on-the-job training.

We conducted in-house training courses to improve terrorism-related expertise and agent recruitment skills.

Management and accountability

I briefed the Parliamentary Joint Committee on ASIO, ASIS and DSD on developments in the War against International Terrorism (including the response to the Bali attacks) and regarding security arrangements in ASIO, ASIS and DSD.

I also appeared before a number of other Parliamentary committees, including the Senate Committee on Foreign Affairs, Defence and Trade (Bali) and the Senate Legal and Constitutional Committee inquiry into the *ASIO Bill*.

In October 2002 the Prime Minister requested the Inspector-General of Intelligence and Security review all relevant intelligence and associated intelligence assessment processes, to establish whether there was any forewarning of the Bali bombings. In his report, presented in December 2002, the Inspector-General advised no such intelligence had been received by Australian agencies.

Our 6th Workplace Agreement came into effect on 10 April 2003. We also adopted a new Performance Management Framework, which will provide a better basis for managing performance in ASIO.

ASIO's attrition rate dropped over the last 12 months to 7%, with the downward trend continuing into 2003-04. The length of the recruitment process remains a problem, and an external review has been commissioned to identify opportunities for improving time lines.

The Outlook for 2003-2004

Counter-terrorism and the threat from Islamic extremism to Australia and Australian interests overseas will remain our key investigative priority.

Central to this will be our focus on deepening further our overseas liaison.

Our capacity to combat terrorism will be enhanced by the *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2002*, which authorises warrants to question (and in limited circumstances to detain) persons in order to investigate terrorism.

With the additional funding of \$24.5m over four years that we received in the 2003-04 Budget, we will be able to improve our response to counter-terrorism priorities.

Following a review of security arrangements after 11 September, we will undertake security assessments of Aviation Security Identity Card applicants in conjunction with the AFP, the Australian Protective Service and the Department of Transport and Regional Services.

On the technical side, we need to continue to develop our computer capabilities, responding to the challenge of disseminating and presenting large quantities of data in a timely and effective manner.

Dennis Richardson

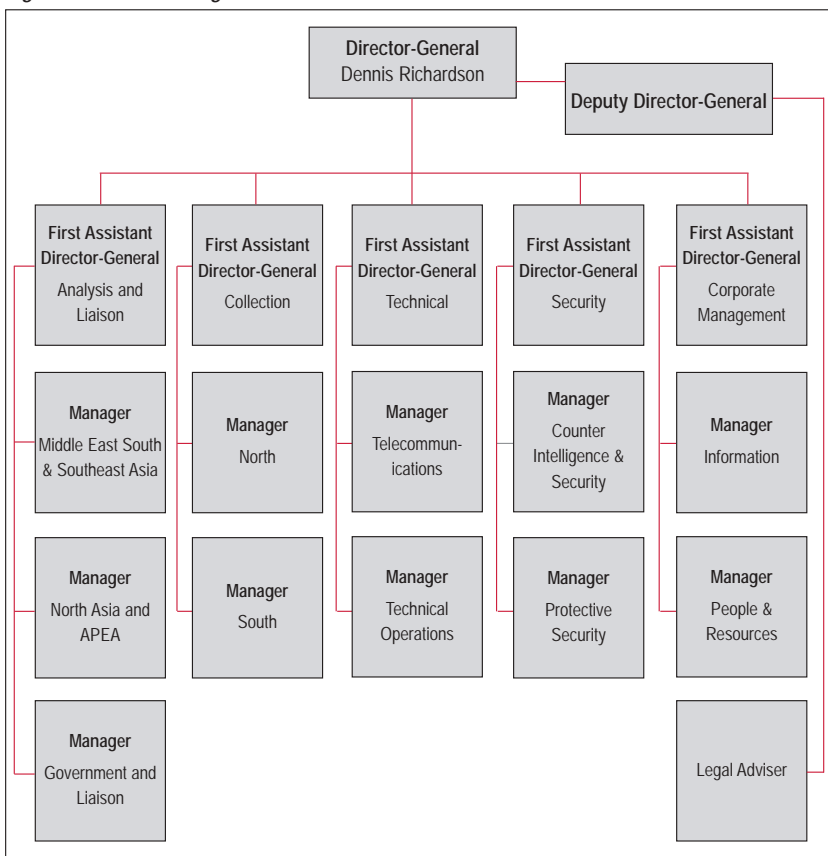
Director-General of Security

Organisational Structure

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

A review of ASIO's management structure, commenced in 2001-02, was completed in 2002-03 and resulted in a significant organisational restructure which took effect from 1 March 2003. The restructure — which expanded the number of divisions from three to five — takes account of new initiatives and increasing staff numbers flowing from additional counter-terrorism funding provided in the wake of the 11 September attacks and the Bali bombings. ASIO's current management structure is at Figure 1.

Figure 1. ASIO's management structure in 2002-03



The 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 / archives issues
- advice on deterrence action, and
- 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, and
- contributions to the external policy framework.

Output 1.3 Security Intelligence Investigation and Capability

This Output includes:

- information collection from human sources, open sources and by technical means
- surveillance capabilities
- counter-terrorism response capabilities
- technical research and development
- deterrence action
- national and international liaison, and
- 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 Outcome of 'A Secure Australia' is measured by:

- The contribution of ASIO's action and advice to the management and the reduction of risk to:
 - people and property
 - government business and national infrastructure, and
 - special events of national and international significance.
- The security of ASIO's activities

The overall price for our Output Group was \$88.945m (see Figure 2).

Figure 2. Price of ASIO's Outputs (\$m)

Output	Actual 2001-02	Estimated 2002-03	Actual 2002-03
Output Group 1: Security Intelligence	74.915	87.405	88.945

Counter-Terrorism capabilities

In the wake of 11 September the Government significantly strengthened Australia's counter-terrorism capability. ASIO received additional funding in the 2002-03 Budget of \$48.3m over four years, and \$14.9m per annum thereafter. A further \$28.5m over five years was provided following the Bali bombings. Of the initiatives for which this funding was provided:

- ASIO's 24-hour alert and monitoring capability is now operational.
- Overseas liaison has been significantly increased in the Middle East and Southeast Asia.
- Technical analysis capabilities have been expanded, and the introduction of new technical capabilities are in place or well advanced.
- Counter-terrorism cooperation with other Australian intelligence, law enforcement and border control agencies has been enhanced.
- Additional resources have been and are being recruited and trained to undertake investigations and analysis, and to expand ASIO's border control, threat assessment, critical infrastructure protection and security assessment capabilities.

In the 2003-04 Budget, the Government provided ASIO with a total of \$19.9m over four years to sustain and further enhance counter-terrorism analytical and liaison capabilities.

- The Government also provided \$3.6m over four years to assist in improving security at airports by providing security checking for Aviation Security Identification Card holders (see page 30).
- ASIO will also receive \$0.96m over four years to contribute to the expansion of the National Counter-Terrorism Committee counter-terrorist exercise program.

Output 1: Security Intelligence Analysis and Advice

ASIO contributes to the Outcome of ‘A secure Australia in a secure region’ 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 the National Information Infrastructure
- visa security checking, and
- 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 2002-03, 100% of clients surveyed rated ASIO product as almost always or generally useful (see figure 3).

- All customers expressed a high level of satisfaction with our reporting on Jemaah Islamiyah and the regional threat from Islamic extremism. Police clients rated ASIO Threat Assessments highly. However, they expressed a desire for Threat Assessments to reflect local circumstances rather than assign nation-wide threat levels.
- Commonwealth customers had a high level of satisfaction with the timeliness of our product. Police clients again commented that there was room for improvement in the timeliness of ASIO product, specifically in relation to Threat Assessments.

Figure 3a. Client feedback survey — usefulness of ASIO product

	Almost always useful (%)		Generally useful (%)		Sometimes useful (%)		Rarely useful (%)	
	2002	2003	2002	2003	2002	2003	2002	2003
Commonwealth	25	70	71	30	4	0	0	0
Police	27	71	73	29	0	0	0	0
Total	26	70.5	71	29.5	3	0	0	0

Figure 3b. Client feedback survey – timeliness of ASIO product

	Almost always timely (%)		Generally on time (%)		Sometimes timely (%)		Rarely timely (%)	
	2002	2003	2002	2003	2002	2003	2002	2003
Commonwealth	46	67	50	29	4	0	0	0
Police	50	29	50	71	0	0	0	0
Total	47	50	50	50	3	0	0	0

Threat from foreign influenced politically motivated violence

The Bali bombings by Jemaah Islamiyah in October 2002 demonstrated the presence of a highly capable terrorist group in our region. More generally, the terrorist threat from Islamic extremist groups with global reach — already at the forefront of security concerns since the 11 September attacks by al-Qa’ida — was highlighted by new information confirming that Australia was an al-Qa’ida target prior to 11 September 2001, and that Australian interests continue to be viewed as a legitimate target. We assess that Australian interests — especially in the Middle East, South Asia and Southeast Asia — will continue to be at heightened threat for the foreseeable future.

Foreign influenced politically motivated violence remained our key priority in 2002-03, with investigations into the Bali bombings and Jemaah Islamiyah, and Australian links with al-Qa’ida and Islamic extremism, absorbing the vast majority of operational and analytical resources.

All clients who responded to the client survey rated ASIO’s product on post-Bali investigations and Jemaah Islamiyah as usually or always useful.

Jemaah Islamiyah

In December 2001 authorities in Singapore uncovered a plot to attack Western targets in Singapore, including the Australian High Commission. These plans were linked to Jemaah Islamiyah (JI), a Southeast Asian Islamic extremist group with links to al-Qa’ida. International investigations also linked JI to other terrorist acts in the region.

ASIO and other Australian and regional intelligence and law enforcement agencies failed to identify JI’s transition in the 1990s from a fundamentalist Islamic group into a terrorist organisation. Following the arrests in Singapore, ASIO began investigating JI links to Australia and confirmed a JI presence as well as several Australian visits by key JI members.

JI leaders Abu Bakar Ba’asyir and Abdullah Sungkar (deceased) visited Australia 11 times between 1990 and 1999. Neither was then known to ASIO in a security context, but we believe the purpose of their visits was to establish a JI presence.

Investigative and analytical priority

PERFORMANCE

Early investigations

JI visits and visa applications

There is no record to indicate senior JI members Hambali or Wan Min bin Wan Mat, or any other suspects in the Bali bombings, ever travelled to Australia under their own names or any known aliases.

- ASIO has no record of any JI-linked applicants for residence being referred by the Department of Immigration and Multicultural and Indigenous Affairs (DIMIA) for security checking prior to December 2001.
- After the Bali bombings DIMIA, in consultation with ASIO, reviewed its file holdings to identify any applicants for protection visas and permanent residence with possible links to JI or other organisations of concern.

Bali bombings

On 12 October 2002, two explosive devices were detonated at Kuta in Bali. The first, inside Paddy's Bar, was detonated by a suicide bomber wearing a bomb vest and was apparently intended to move people out onto the street towards a second, larger device in a van outside the Sari Club. This device, also triggered by a suicide bomber, was detonated within a minute of the first explosion. Less than a minute later another device exploded harmlessly near the US Consulate in nearby Denpasar.

The official death toll for the Bali attacks was 202, including 88 Australians.

The team that conducted the Bali attack was co-ordinated by JI member Imam Samudra and consisted of logistics, bomb construction, support and deployment elements (which included the two suicide bombers).

While the Bali attack was a JI operation, we assess al-Qa'ida played a part, providing funding, advice and training. Al-Qa'ida and senior JI member Hambali (arrested in Thailand in August 2003) provided funds for the operation. In addition, JI leaders including Hambali, Samudra and Mukhlas received training in Afghanistan, which we assess was provided by al-Qa'ida.

Bali bombings — investigations

Australian Federal Police (AFP) and Indonesian police conducted a joint criminal investigation into the Bali bombings, which led to the identification and arrest of most of those who took part in planning or executing the attack. ASIO deployed officers to Bali after the attack to undertake analytical and investigative tasks as part of combined investigations into the bombings. Our deployment concluded on 20 December 2002. An ASIO team in our Central Office also provided analytical support to the investigation and we posted two officers to the AFP Joint Task Force in Canberra. We continue to support Bali-related investigations and have an officer posted to the AFP Transnational Crime Coordination Centre.

As of 30 June 2003, 34 people had been arrested for involvement in the Bali attack. Among the key arrests were the field commander Samudra, his deputy, Idris, and the brothers Amrozi (logistics), Ali Imron (bomb construction/deployment), and Mukhlas (*aka* Ali Ghufron, head of the JI group responsible for operations in Singapore and Malaysia). Other arrests included Umar Wayan and Sawad (bomb construction); and Yudi (*aka* Octavia), Amin (*aka* Junaedi), Abdul Rauf, and Agus (*aka* Hidayat), from the reconnaissance and support team.

Abu Bakar Ba'asyir was not charged over the Bali attack but faced trial on a number of other charges. In September 2003 he was convicted of treason and sentenced to four years gaol, but acquitted of involvement in a bombing in Indonesia in December 2000, the planned attack in Singapore in December 2001 and a plan to assassinate the then Vice-President Megawati Sukarnoputri in 2001.

Indonesian authorities continue their investigation into JI, focusing not only on those responsible for the Bali attack but also on the wider JI organisation. In addition to the 34 arrests directly related to Bali, there have been numerous arrests of people who provided assistance to the Bali bombers after the fact or who were involved in the broader JI network.

The pressure applied since the Bali attack by Indonesian authorities on both key JI members and those providing transport, finances and logistical support has damaged JI's organisational capability, making it difficult for JI fugitives to meet, plan and communicate. However, a number of key JI members, including some involved in planning the Bali attack — Zulkarnaen, Noor Din Top and Dr Azahari bin Husin — are still at large. JI retains the capacity to undertake further attacks.

Attacks on Western interests in Southeast Asia remain likely, as demonstrated by the bombing of the Marriott Hotel in Jakarta on 5 August 2002. The threat to Australian interests in Indonesia remains *High*.

In late October 2002 — following the listing of JI as a terrorist organisation by the Government — ASIO conducted enter and search operations on the residences of individuals with suspected links to JI.

- These operations were conducted in concert with the AFP and State Police. Police carried weapons as part of their standard operating procedures, and in some cases the weapons were drawn.

Five illegal immigrants were taken into DIMIA custody in the course of the searches and have since departed Australia. A person who was the subject of an unsuccessful visa application for Permanent Residency has also left Australia.

In addition to the searches ASIO also conducted a separate interview program.

A large volume of information was obtained during the searches. Key outcomes from the analysis of this material included:

- confirmation of links between JI members in Australia and senior JI figures in Southeast Asia
- evidence of past planning for attacks against Israeli interests in Australia
- confirmation the Australian group comprised Mantiqi IV in the JI regional structure
- confirmation of the size and distribution of JI in Australia, and
- information relating to recruitment, finance and training activities.

The search operations produced no evidence of current JI terrorist planning or operational cells in Australia, no explosives or illegal firearms and no direct links to the Bali bombings.

Jack Roche

The AFP arrested Australian Jack Roche in Perth in November 2002. Mr Roche has been committed for trial on charges of conspiracy to commit an offence under the *Crimes (Internationally Protected Persons) Act 1976*.

Outlook — JI in Australia

ASIO operations conducted since the Bali bombings have disrupted JI activity in Australia. We will continue to closely monitor JI activity and to investigate links between JI members in Australia and the JI network in Southeast Asia.

Usama bin Laden and al-Qa'ida

Al-Qa'ida and affiliated groups continue to pose the most significant security threat to Western interests, including Australia. Al-Qa'ida's leadership and capability have been reduced through the War on Terror; however, while many senior leaders have been killed or captured, intelligence suggests a new generation of leaders continues to plan operations. Al-Qa'ida retains the intent and capability to undertake acts of terrorism around the world, as demonstrated with attacks in Kenya in November 2002 and in Riyadh on 12 May 2003 (in which one Australian was killed).



Al-Qa'ida bombing in Riyadh, May 2003

In Australia there are groups with links to, and individuals who have been trained by, al-Qa'ida or its affiliates. In 2002-03 we continued to monitor the activity of these groups and identify Australians who have undertaken terrorist training overseas, or facilitated such training by others. We also contributed to counter-terrorism investigations by liaison partners.

Threat to Australia

New intelligence obtained in 2002-03 confirmed that Australia was viewed by al-Qa'ida as a target prior to 11 September 2001 and continues to be viewed as a legitimate target.

- On 12 November 2002, Arabic television network *al-Jazeera* broadcast an audio statement allegedly made by Usama bin Laden, saying: "We warned Australia before not to join in [the war] in Afghanistan, and [against] its despicable effort to separate East Timor. It ignored the warning until it woke up to the sounds of explosions in Bali. Its government falsely claimed that they were not targeted." This statement, giving more prominence to Australia than any other non-US Western country, reaffirmed Australia as a target.

- In an audiotape broadcast on *al-Jazeera* on 21 May 2003, Ayman al-Zawahari, second-in-command of al-Qa'ida and spiritual mentor of bin Laden, called for worldwide attacks on the diplomatic and commercial interests of Australia, the US, the UK and Norway, who he described as "crusaders and the murderers of your Iraqi brothers".

Terrorist training

ASIO is aware of a number of Australians who have received terrorist training since the late 1990s. The level of instruction received by these individuals ranges from basic military training to advanced terrorist tactics. Identifying other Australians who have undertaken terrorist training remains a priority.

Australians and al-Qa'ida – David Hicks

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.

Mr Hicks was interviewed by ASIO and the AFP in December 2001; ASIO conducted further interviews — one in conjunction with the AFP — at Guantanamo Bay in May 2002, August 2002, November 2002 and May 2003. Mr Hicks was also interviewed by US agencies.

ASIO continues to investigate Mr Hicks's involvement with al-Qa'ida.

Mamdouh Habib

Mamdouh Habib, an Egyptian-born Australian citizen from Sydney, was detained in Pakistan in October 2001 and transferred to Guantanamo Bay in May 2002.

Mr Habib was interviewed by ASIO and the AFP in Pakistan in late October 2001. ASIO conducted further interviews — one in conjunction with the AFP — at Guantanamo Bay in May, August and November 2002 and May 2003.

Mr Habib's activities overseas remain the subject of investigation.

Jack Thomas

Jack Thomas, a convert to Islam from Melbourne, was detained in Karachi on 4 January 2003 by Pakistani authorities in relation to possible offences under Pakistan's security/terrorism laws. Mr Thomas was interviewed by ASIO and the AFP in Pakistan.

Mr Thomas returned to Australia in June 2003. He has not been charged with any offences under Australian law.

Mohamad Sultan

Mohamad Ramez Sultan was arrested in Lebanon on 27 September 2002 for attempting to establish an al-Qa'ida cell in Lebanon. Mr Sultan holds Australian citizenship but left Australia in 1997 and has not returned under this name or any known aliases. Sultan and three associates were each sentenced on 6 May 2003 to three years imprisonment. Four others were sentenced in absentia to fifteen years imprisonment.

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 2002-03, ASIO provided advice to the Attorney-General on a number of organisations for this purpose.

As at 30 June 2003, the Government had made regulations listing fourteen organisations as terrorist organisations under the Act: Abu Sayyaf; Egyptian Islamic Jihad; al-Qa'ida; Ansar al-Islam; Armed Islamic Group (GIA); Asbat al-Ansar; Harakut-ul-Mujahideen; Islamic Army of Aden; Islamic Movement of Uzbekistan; Jaish-i-Mohammed; Jemaah Islamiyah; Lashkar I Jhangvi; Salafist Group for Call and Combat (GSPC); and Hizballah's terrorist apparatus, the External Security Organisation (ESO). Because the ESO has not been formally identified as a terrorist organisation by the UN Security Council, and therefore could not be proscribed under the Act, in June 2003 Parliament passed the *Criminal Code Amendment (Hizballah) Act 2003* to enable the Government to list the ESO as a terrorist organisation under Australian law.

Terrorist financial investigations

ASIO continued to undertake financial investigations as a key component of terrorism investigations.

ASIO has worked closely with other Commonwealth agencies to implement the *Charter of the United Nations (Anti-terrorism Measures) Regulations 2001* and its successor, 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*. ASIO is a member of the working group established by DFAT to implement the *Regulations*.

Entities gazetted to date include: al-Qa'ida and Taliban-associated persons and entities including Usama bin Laden; Jemaah Islamiyah; the Abu Sayyaf Group; Hamas; Hizballah; the Liberation Tigers of Tamil Eelam; and a number of Irish, European and South American terrorist entities.

AUSTRAC

On 1 May 2003 we signed a revised Memorandum of Understanding (MOU) with the Australian Transaction Reports and Analysis Centre (AUSTRAC). The new MOU provides ASIO with on-line access to the AUSTRAC database, and authorises us to communicate Financial Transaction Reports to foreign intelligence agencies (provided appropriate undertakings to protect the information are given by the foreign agency). On-line access to AUSTRAC will be available by the end of 2003.

Weapons of mass destruction

In 2002-03 ASIO focused on identifying attempts by nations and terrorist groups to acquire WMD-associated knowledge, technology and delivery systems.

CBRN Terrorism

Hoax anthrax letters containing white powder are now part of the Australian security environment.

We continued to engage with other Australian agencies, including Defence, Emergency Management Australia and Australia Post as well as the various Police, Fire, Ambulance and Water authorities to advise them of the threat of terrorist use of Chemical, Biological, Radiological or Nuclear (CBRN) weapons, and to contribute to the development of Australia's protective measures and response capability.

Aviation security

Aircraft and aviation infrastructure have been targets for terrorist attack for many years. At the request of the Department of Transport and Regional Services (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. Early in the reporting period DOTARS and ASIO agreed that a much more extensive and detailed assessment of this threat was required and work progressed on preparing this assessment over much of 2002-03. The new assessment was distributed in July 2003.

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

Threat from local politically motivated violence

Investigative and analytical priority

ASIO continued to give priority to investigating and reporting on Australian groups or individuals planning or inciting others to undertake violence to support their causes or ideological views.

We issued Security Intelligence Reports on the threat from local politically motivated violence.

PERFORMANCE

Our client survey found Police place high value on ASIO reporting as it plays a critical role in their decisions and their advice to State governments.

In contributing to reducing the threat from local politically motivated violence we produced accurate advice on a range of potential threats.

War on Iraq

We identified a number of groups planning acts of violence as part of protests opposing the war in Iraq, although these plans were not put into effect. We also provided threat advice for Australian High Office Holders, diplomatic representatives, community groups and visiting dignitaries during the conflict in Iraq.

ASIO accorded a high priority to reporting on threats to Defence before and during the war in Iraq. A major report issued on this subject prior to the start of the war was followed up by a series of Threat Assessments for Defence personnel, events, and facilities in Australia. Production of Threat Assessments also increased in response to more frequent US Navy ship visits to Australia.

Attacks on the Islamic Community

After the Bali bombings there were reports of harassment, threats and minor acts of violence against the Islamic community in Australia, including threatening phone calls and letters, vandalism against mosques in Sydney and Geelong and an arson attack on a mosque in Melbourne resulting in minor damage.

ASIO maintains regular contact with Islamic community leaders and continues to seek to develop a closer relationship with members of the Islamic community.

Attacks on the Jewish Community

We issued Threat Assessments relating to Israeli and Jewish interests in Australia, and threats to Australian interests in Israel.

There was a small increase in the number of reported incidents of anti-Jewish harassment, including hate mail and verbal abuse, but there were fewer and less severe violent attacks than in the previous year.

- There was an unsuccessful arson attack against a Sydney synagogue, the Jewish Museum in Melbourne sustained minor damage from vandals and two incidents of graffiti were reported in the context of the Iraq War.

Parts of this performance report are excluded from the 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 regarded as dissidents by foreign governments.

This performance report has been excluded from the unclassified *Report to Parliament* in its entirety.

Critical Infrastructure Protection

In 2002-03 the Government expanded its information infrastructure protection initiative to include critical physical infrastructure, following the Government/Business Task Force on Critical Infrastructure held in 2002.

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; communications; health; 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.

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

- In July 2002 we provided a classified briefing on the security environment to security executives of major CI companies. Other Commonwealth agencies such as the Protective Security Coordination Centre (PSCC), Emergency Management Australia (EMA), the AFP and DSD also gave presentations on their roles in infrastructure protection.
- As part of a broader engagement with industry, senior ASIO executives — including the Director-General — addressed a range of government and industry meetings and conferences, including meetings of the Australian Industry Group in Brisbane, Melbourne and Sydney in February 2003, the Australian National Trucking Convention in April 2003, the Port and Maritime Security Conference in May 2003 and the Australian Security Industry Association Conference in June 2003.

PERFORMANCE

A major assessment was made of the threat to Australia's oil and gas shipping and infrastructure. This assessment was distributed to Commonwealth and State and Territory governments and made available to relevant industry members.

Three Security Intelligence Reports were produced, compared to eight last year.

Outlook

The Government has approved ongoing funding for ASIO of \$1.351m per annum from 2002-03, and a further \$2m from 2003-04 for critical infrastructure protection. Priority will be given to:

- completing work commenced in 2002-03 to identify and record critical national infrastructure assets, and
- improving processes for disseminating relevant threat information to infrastructure owners in cooperation with other Commonwealth departments and State and Territory police services.

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

Threat levels in Australia and to Australian interests overseas

ASIO is responsible for preparing national assessments of the threat — from politically motivated violence and other activities prejudicial to security — in Australia and to Australians and Australian interests overseas. These include general assessments of threat, and assessments of threat directed against specific people, places and events, including:

- Australian dignitaries at home and abroad
- foreign dignitaries visiting Australia
- foreign interests in Australia
- Australian interests abroad
- national critical infrastructure
- sites of national significance, and
- ministerial residences, government buildings and defence establishments.

The arrangements for coordinating Threat Assessments were established under the former Standing Advisory Committee on Commonwealth/State Cooperation for Protection Against Violence (SAC-PAV), and have been continued under the National Counter-Terrorism Committee (see page 36).

Travel Advisories – which provide advice on a range of issues, including terrorism, for Australians travelling overseas — are the responsibility of DFAT. 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*. Threat levels for US, UK and Israeli interests in Australia remained *High* throughout the year.

- Statements by Usama bin Laden and his associates and intelligence on the intentions and capabilities of Islamic extremists clearly indicate the continuing interest of al-Qa'ida and affiliated groups in terrorist attacks against Australia and Australian interests.
- Intelligence suggesting Australia was a potential location for a major attack by al-Qa'ida led to the issue of a general terrorist alert by the Government on 19 November 2002; this alert remains in place.
- The threat to Australian interests overseas is also generally raised, with the threat to Australian interests in a number of countries in Southeast Asia, South Asia and the Middle-East assessed as *High*.
- As reported above (page 21), a major assessment of the threat to oil and gas production and transport infrastructure was produced.

Threat assessments and travel advisories

The threat environment

PERFORMANCE

Last year we reported an increase in the number of assessments and suggested a decrease this year. That did not happen — the number of assessments increased to 2055, up 15% from 1786 in 2001-02. The number of Threat Assessments produced annually has more than doubled in the past five years, due to:

- the fundamental change in the threat environment
- an increase in the flow of intelligence from overseas liaison services and Australian agencies, and
- a growing requirement to prepare regular update assessments of threats to Australian interests overseas.

Trends

The Bali bombing and the war in Iraq both led to significant spikes in Threat Assessment production. In the lead up to the war in Iraq, ASIO prepared assessments on threats to Australian interests overseas, Australian High Office Holders, foreign interests in Australia and the Australian Defence Force. From 20 March to 2 May 2003, ASIO produced 427 Threat Assessments related to the war.

Figure 4. Threat Assessments issued

Subject of assessment	1998-99	1999-00	2000-01	2001-02	2002-03
Visiting dignitaries	107	131	79	237	674
Australian dignitaries	347	552	503	834	739
Australian interests	—	—	122	176	375
Protective security	30	34	27	25	22
Demonstration notifications	63	48	100	193	149
Diplomatic premises	208	164	77	108	55
Other Threat Assessments	84	75	51	66	29
Olympic Games/CHOGM	46	342	383	147	—
WTO	—	—	—	—	12
Total	885	1 346	1 342	1 786	2 055

All Commonwealth and Police clients who responded to our client survey rated our Threat Assessments as almost always or generally useful. Commonwealth clients valued Threat Assessments as a basis of advice to Ministers on risk levels and resources. Threat Assessments also helped judgments about Ministerial travel within Australia and overseas, visiting dignitaries and special events. Police used Threat Assessments for similar purposes but looked for more detail and context.

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

Visa security checking

Australia's border control mechanisms are essential to minimising the risk of terrorists entering Australia. ASIO is the principal source of advice to DIMIA on the entry to Australia of people of security significance. We assess whether people applying for temporary entry or permanent residence have the potential to conduct terrorist activity, espionage or foreign interference, and provide a security assessment advising whether a person is a risk to national security.

ASIO does not conduct assessments of all visa applicants. We use a risk management approach to identify those people most likely to pose a risk. DIMIA and DFAT also refer applicants to ASIO if they suspect the applicant may be involved in activities prejudicial to Australia's national security.

PERFORMANCE

In 2002-03, 96% of temporary visa applications and 85% of permanent visa applications were assessed within agreed timeframes. Delays in assessments were largely caused by extra scrutiny of certain visa applications. The need to conduct checks with overseas authorities and to clarify incomplete visa applicant information also continued to create delays.

Trends

There was a slight downturn in security checking in relation to temporary travel. This can be attributed to reduced levels of travel flowing from the Bali bombing, the Iraq war and the SARS virus.

Figure 5. Visa security assessments 1998-99 to 2002-03

Type of entry	1998-99	1999-00	2000-01	2001-02	2002-03
Temporary	10 015	16 483	26 527	29 437	27 534
Permanent	8 107	8 371	7 392	9 584	12 355
Total	18 122	24 854	33 919	39 021	39 889

Note — These figures do not include security assessments of unauthorised arrivals held in detention

Visa refusals & cancellations

- On ASIO advice five visa applicants were refused entry to Australia because of their assessed involvement in terrorist activities.
- On ASIO advice two visa applicants were refused entry to Australia because they were assessed as likely to engage in espionage activities.
- On advice from ASIO, DFAT expelled one diplomatic visa holder (from Iraq) who was assessed as likely to engage in espionage activities.

Figure 6. Prejudicial security assessments for visa applicants 1998-99 to 2002-03

	1998-99	1999-00	2000-01	2001-02	2002-03
Prejudicial assessments	9	4	5	5	8 ⁽¹⁾

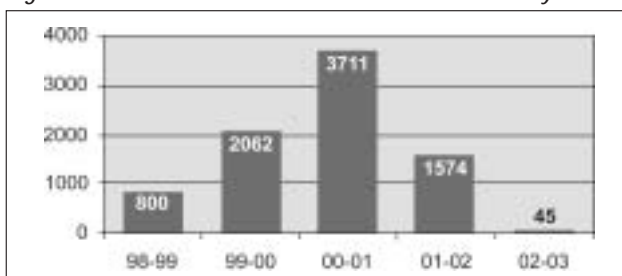
⁽¹⁾ 7 plus 1 diplomat expelled on advice from ASIO

There was a significant decline in unauthorised arrivals in 2002-03, with no unauthorised boat arrivals. There were 987 unauthorised air arrivals and 15 stowaways. As in previous years, the majority of unauthorised arrivals claimed to come from Iraq, Afghanistan and Iran.

During 2002-03, 83 unauthorised arrivals were referred to ASIO for security checking. ASIO issued 173 security assessments compared with 2281 the previous year. No prejudicial security assessments were issued. As of 30 June 2003, there were 32 cases awaiting resolution by ASIO.

Unauthorised arrivals who were granted three year Temporary Protection Visas are required to undergo a new security assessment prior to being granted a further Protection Visa. The assessment of such cases has commenced, with DIMIA and ASIO working together to ensure processing is completed in a timely and efficient manner. In 2002-03, 45 cases were referred to ASIO for a further security assessment.

Figure 7. Unauthorised arrivals referred to ASIO for security assessment.



Note — Figures for 98-99 are approximate only

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

Release of archival documents

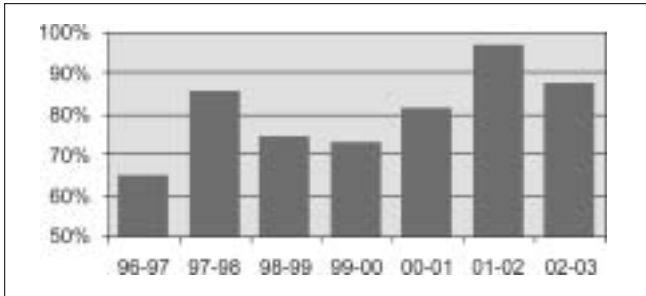
ASIO is an exempt agency under the *Freedom of Information Act 1982*, but is not exempt from the information access provisions of the *Archives Act 1983*.

Members of the public can apply to the National Archives of Australia for access to ASIO records that are at least 30 years old. When National Archives does not already hold records on the subject, it passes 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*. ASIO only recommends exemptions where disclosure of the information could damage national security or expose the existence or identity of a confidential source.

In 2002-03, 87.5% of applications due to be completed were finalised within the statutory timeframe of 90 days, against a benchmark of 80%.

This result was lower than the 97% last year, reflecting staff redeployments to other priorities, including the Bali and Iraq response teams. The lower rate also reflects the impact of several large requests lodged by a small number of researchers which, due to their size and complexity, could not be completed within the statutory period and in fact are expected to impact adversely on our ability to meet benchmarks for the first half of 2003-04.

Figure 8. Percentage of Archival requests satisfied within 90 days



Trends

We received applications for access to 244 separate items or subjects which were due to be completed in 2002-03, compared to 297 in the previous year 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. We received 92 requests in the last financial year (compared to 132 in 2001-02), of which 96.75% were completed within 90 days (compared to 99% in 2001-02).
- Nine per cent were for items that were either not recorded in our indexes or for which there were no ASIO records in the open access period.
- Many requests related to ASIO's records on war criminals; anti-apartheid and Vietnam demonstrations; ASIO's telecommunications interception policy; and Greek organisations, their members and related affiliations.
- Several large requests from individual/non-family researchers were also received. In some cases special arrangements were made to accommodate these requests.

The total number of folios (pages) examined was 19 382, compared to 30 550 in 2001-02 (which was an exceptional year). Figure 9 shows the distribution of exemption decisions made with respect to these folios.

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

Figure 9. Distribution of exemption claims across assessed folios

Subject of assessment	1999-00	2000-01	2001-02	2002-03
Folios released without exemption	21%	28%	31%	33%
Folios released with part of the text claimed as exempt	60%	58%	57%	56%
Folios claimed as totally exempt and not released	19%	14%	12%	11%
Total folios assessed	100%	100%	100%	100%

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 National Archives. Applicants still dissatisfied may then appeal to the Administrative Appeals Tribunal (AAT), which may uphold the original decision or grant access to all or part of a previously exempted record. One appeal to the AAT was lodged in the last days of the reporting period.

Five of the six applications for internal reconsideration in 2002-03 were completed. In all cases they resulted in minor changes or no change to the original exemption decisions. Some paperwork outside ASIO's control remains outstanding on the remaining application, which is also the subject of the AAT appeal.

No part of this performance report has been excluded from the unclassified *Report to Parliament*.

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 national security classified information or secure places) and administrative security practices, and
- providing advice on physical security (the security of government buildings and infrastructure) which includes electronic 'sweeping' of sensitive areas to protect against unauthorised monitoring of government meetings.

Security in Government

The Inter-Agency Security Forum (IASF), established following the Inspector-General of Intelligence and Security's *Inquiry into Security Issues*, is chaired by ASIO with senior-level representation from the Australian Intelligence Community (AIC) and related policy departments — PM&C, Treasury, Defence, DFAT, Attorney-General's and DIMIA. The IASF initially focused on implementation of the Government-endorsed recommendations of the Inquiry, but as these have been implemented the IASF has moved on to its long-term goal of establishing and maintaining best security practice for member departments and agencies. The IASF works closely with the Protective Security Policy Committee (PSPC) which is responsible for broader public sector protective security policy.

The Lappas Dowling case

Simon Lappas, a Defence Intelligence Organisation (DIO) employee, and Sherryll Dowling were prosecuted under the official secrets provisions of the *Crimes Act 1914*.

On 13 December 2002 Lappas was found guilty of one count of espionage contrary to section 76 of the *Crimes Act*. He was given a suspended 12-month sentence and released on a two-year good behaviour bond. Following an appeal by the Commonwealth Director of Public Prosecutions (DPP), the sentence was increased on 31 October 2003 to two years imprisonment with 18 months suspended.

Dowling pleaded guilty to two charges of receiving prescribed documents. She was placed on a five-year good behaviour bond on 9 May 2003.

ASIO worked with the Attorney-General's Department, the DPP, the AFP and DIO on aspects of the prosecution.

Personnel security

Before granting a security clearance for designated security assessment positions, Commonwealth agencies are required to assess the candidate's general suitability for access. ASIO then provides a security assessment advising whether anything in the candidate's background or activities is a cause for security concern. This advice is usually based on an assessment of material provided by the relevant agency, but ASIO may interview people to resolve security issues. Any psychological testing for security clearances is the responsibility of the agency, and does not involve ASIO.

ASIO will either advise the agency that it does not recommend against the candidate, or it 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 that ASIO considers may need to be considered 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 relevant agency.

Performance in 2002-03 was below last year's levels. While benchmarks were exceeded in the first half of the reporting period, performance decreased in the second as workloads increased and staff availability fell as a result of a diversion of resources to post-Bali investigations.

Figure 10. Personnel security assessments — performance against benchmarks

Performance measure	Target	Performance			
		1999-00	2000-01	2001-02	2002-03
Complete within 14 days	75%	33%	14.7%	74.7%	56.3%
Complete within 21 days	90%	43%	15.3%	86%	66.1%
Incomplete after 12 weeks	1%	8.8%	55.4%	1.3%	1.4%

Figure 11. Personnel security assessments — annual workloads

Level of access	1998-99	1999-00	2000-01	2001-02	2002-03
Confidential	1 038	1 163	969	1 431	1 542
Secret	5 909	6 658	5 803	6 595	7 618
Top Secret	4 453	4 650	4 335	4 329	5 112
Total	11 400	12 471	11 107	12 355	14 272

Appeals

Individuals have a right of appeal to the Administrative Appeals Tribunal (AAT) in respect of an adverse or qualified ASIO security assessment. One appeal was lodged during 2002-03 against an adverse assessment, while an appeal lodged in 2001-02 against a qualified assessment was withdrawn. No appeals were heard in 2002-03.

Trends

ASIO received 14 272 requests for security assessments, a 16% increase on 2001-02. The increase was spread across the levels of access but was greatest for the higher levels.

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

Adverse and qualified assessments

Two adverse and three qualified assessments were issued.

Figure 12. Adverse and qualified personnel security assessments

	1998-99	1999-00	2000-01	2001-02	2002-03
Qualified assessments	4	12	10	6	3
Adverse assessments	1	1	2	3	2
Total	5	13	12	9	5

Vetting for the AIC

Following the recommendations of the *Inquiry into Security Issues*, ASIO now undertakes Top Secret positive vetting for external agencies including ONA, ASIS, Defence, Treasury, Attorney-General's and DIMIA. In 2002-03, 14 full re-evaluations were completed for external agencies. The ASIO Legal Adviser was consulted to ensure that ASIO's advice in relation to these clearances is consistent with the provisions of the *ASIO Act*.

Aviation Security

In late 2002-03 we began recruiting for positions established to conduct security checks on Aviation Security Identity Card (ASIC) holders. Under requirements introduced by the Government following a review of security arrangements after 11 September, ASIO will undertake security assessments of ASIC applicants through a process now being established in conjunction with the AFP, the Australian Protective Service, and the Department of Transport and Regional Services.

Polygraph trial

A polygraph trial involving volunteers from ASIO was completed in January 2003. The trial, one of the Government-endorsed recommendations from the *Inquiry into Security Issues*, was conducted on behalf of the Australian Intelligence Community. ASIO is now finalising a confidential report — delayed by the diversion of resources to post-Bali investigations — which assesses the utility of the polygraph for security vetting. There will be no public reporting on the details of the trial.

Contact Reporting

The revised *Protective Security Manual* requires people working for, or on behalf of, the Commonwealth to report certain categories of contact with foreign nationals. Agencies pass this information to ASIO so that appropriate action can be taken and counter-measures put in place to lessen any possible risk to national security.

ASIO will maintain an ongoing focus on the contact reporting scheme.

Protective security advice

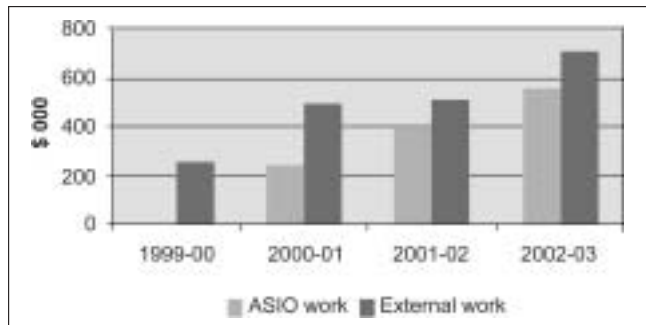
ASIO provides protective security policy advice to Government and specific advice to departments and agencies, including:

- Protective Security Risk Reviews and risk management advice
- physical security advice including access control systems, perimeter security, locks and alarms, CCTV systems and secure containers
- development of Security Plans
- certification of the overall security measures for Top Secret facilities
- security equipment assessment and testing
- specialist protective security training, and
- technical surveillance counter-measures (TSCM) testing (electronic sweeps).

Cost Recovery

ASIO's protective security advice and services are provided on a cost recovery basis. \$705 000 was recovered from clients in 2002-03, a 39% increase on the previous year. Increased demand reflected greater focus on protective security in the current heightened security environment. In addition, a number of major tasks were undertaken within ASIO for which notional charges of \$553 000 were attributed. This was mainly due to a review of the security of ASIO offices in the heightened security environment.

Figure 13. Protective security — value of external work and ASIO work



In September 2001 a review by consultants Ernst and Young recommended significant changes to the management of ASIO's protective security business. Implementation of the recommendations was finalised in 2002-03.

Protective security and risk management advice

In 2002-03 protective security advice to clients increased by 20%, reflecting heightened awareness of the need to protect Commonwealth resources, staff and visitors. Priority was given to AIC clients, key policy departments with significant holdings of classified material, Commonwealth and State parliaments, High Office Holders, and key government research and development organisations.

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

- Advice to the Australian Nuclear Science and Technology Organisation (ANSTO) to ensure security arrangements for the Replacement Research Reactor Project meet International Atomic Energy Agency and Australian Safeguards and Non-Proliferation Office standards.
- Risk Reviews for the Sydney Airport Corporation; Environment Australia; the South Australian Department of Finance and Treasury; DIMIA offices in Canberra and Sydney; and Department of Employment and Workplace Relations offices in Canberra, Sydney and Melbourne, which provided a benchmark for the Department to review security at their other offices.
- A physical security review of several Austrade offices and shop fronts, and an assessment of Comcar's security measures.
- Advice to the Department of Health and Ageing on storage and transport of smallpox vaccine stocks and to South Australia's Government House on their security arrangements.
- Advice to the AAT on the handling of information, which may include classified material, during appeals.
- Development of a Security Plan for the Department of Transport and Regional Services, and measures required to upgrade Department of Public Prosecutions offices to 'highly protected' facilities.

ASIO, on behalf of the interdepartmental Security Construction and Equipment Committee, accredits locksmiths to maintain manifoil combination locks and fit door locks on secure area doors. In 2002-03 we reconfirmed the accreditation of all endorsed locksmiths, accredited six new locksmiths, and arranged for TAFE colleges in Sydney and Melbourne to provide training in specific locks. No cases of compromised locks or suspicious lock outs were reported in 2002-03.

Gatekeeper/Public Key Infrastructure (PKI) accreditation permits private companies to undertake sensitive non-national security electronic data processing work on behalf of government departments and agencies.

Demand for accreditation fell in 2002-03, with only one information technology company PKI-accredited through a joint ASIO-DSD program in 2002-03, compared with eleven the previous year. ASIO provided protective security advice to two other companies seeking DSD Gatekeeper accreditation.

Fifty-one Top Secret (TS) facilities in Australia were inspected in 2002-03. Twenty-three facilities were certified, and the remainder provided with reports detailing the physical security improvements required to meet the minimum standards for TS certification. Re-certification of facilities is required every five years or following significant structural changes.

Most certifications were provided at the request of DSD, which requires ASIO's physical security certification of new TS-Signals Intelligence (TS-SI) sites as part of its accreditation process. ASIO also worked with the Joint Intelligence Support Systems (JISS) Project in relation to the physical security of new JISS TS-SI sites throughout Australia.

TS certification inspections were provided to commercial companies required to secure classified information acquired in their dealings with government agencies, and certifications of government agencies were conducted.

Training in government security standards was provided on a cost-recovery basis to security equipment manufacturers and security consultants, with emphasis on high-grade security systems. Completion of this training leads to endorsement by the Security Construction and Equipment Committee; this contributes to improved security across government agencies, which use endorsed consultants to develop and implement best practice protective security.

ASIO also provided lecturers on protective security, physical security and general security threat topics to PSCC training courses. Chubb Mk4 manifoil combination lock maintenance courses were provided to Defence Force personnel to enable them to service these locks in operational circumstances.

Security equipment standards

ASIO tests and evaluates a wide range of security products proposed for use in the security systems of government departments and agencies. The Security Construction and Equipment Committee, which reports to the Protective Security Policy Committee, is responsible for endorsement of security products.

Endorsed products are published in the *Security Equipment Catalogue* which is produced by ASIO. A new edition of the *Catalogue* was published in April 2003. 667 copies were sold to government departments and private sector companies.

Forty-six security products were tested by ASIO in 2002-03, compared to 32 the previous year. These included:

- blast mitigation equipment
- perimeter security systems, including security fencing and intruder detection systems
- biometric access control readers
- demountable B Class rooms, security doors and secure containers
- glazing products
- electronic and mechanical combination locks, and mortice locks
- stand-alone electronic access control locking systems, and
- secure pouches, safe-hand bags, wafer seals and document shredders.

Technical Surveillance Counter-Measures

ASIO undertakes physical and electronic surveys ('sweeps') and monitoring of government offices and meeting rooms to protect against unauthorised monitoring of sensitive or classified discussions.

Parts of this performance report are excluded from the 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 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
- human source intelligence collection
- surveillance
- collection of information from open sources
- liaison with other Australian stakeholders
- liaison with overseas security and intelligence partners, and
- 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 to the public 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), and
- maintaining and enhancing investigative capabilities.

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

Legislative amendments

ASIO Bill

The *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2002* was passed by the Parliament on 26 June 2003, and received Royal Assent on 22 July 2003.

The legislation, originally introduced in March 2002, was considered by three Parliamentary committees. The legislation is designed to enhance Australia's capacity to combat terrorism by authorising ASIO to seek warrants for the questioning of persons for the purpose of investigating terrorism. The warrants may authorise police officers to detain persons in limited circumstances.

ASIO is required to obtain the Attorney-General's consent before seeking a warrant from an independent issuing authority (a Federal Magistrate or Judge). Any questioning pursuant to 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.

The Act requires that details relating to such warrants be included in our *Annual Report*. ASIO is also required to prepare a written statement of procedures, which is to be presented to each House of Parliament and to the Parliamentary Joint Committee on ASIO, ASIS and DSD, before any warrants may be issued.

The Act also amends the definition of 'politically motivated violence' in the *ASIO Act* to include acts that are terrorism offences under the Criminal Code, and includes provisions to enhance ASIO's existing powers with respect to searches conducted on premises.

The *Criminal Code Amendment (Espionage and Related Offences) Act 2002* entered into force on 31 October 2002. The Act strengthened criminal provisions relating to the deliberate disclosure to a foreign power of national security information and increased the maximum penalty for espionage from seven years to 25 years imprisonment. The legislation was developed following a review of Australia's espionage laws after former DIO officer Jean-Philippe Wispelaere was arrested in the United States in 1999 for attempted espionage.

Counter-terrorism response capabilities

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

- the National Counter-Terrorism Committee (NCTC), formerly the Standing Advisory Committee on Commonwealth/State Cooperation for Protection Against Violence (SAC-PAV), and
- the Commonwealth Counter-Terrorism Committee (CCTC), formerly the Special Inter-Departmental Committee on Protection Against Violence (SIDC-PAV).

ASIO is involved at every level of Commonwealth counter-terrorism arrangements.

- We seek to help prevent terrorism through intelligence collection and reporting, and by participating in counter-terrorism training courses and exercises.
- We would actively respond to terrorist incidents through intelligence collection and reporting, managing the National Intelligence Group and providing intelligence support to States and Territories.
- And we contribute to counter-terrorism policy development and crisis contingency planning.

Support to the NCTP

In 2002-03 ASIO was one of a number of agencies involved in redrafting Australia's counter-terrorism arrangements and developing the new National Counter-Terrorism Plan (NCTP), to replace the National Anti-Terrorism Plan.

Under the NCTP, ASIO assists in management of terrorist incidents (providing intelligence support to the Commonwealth and State/Territory governments and police) and contributes to Commonwealth and State/Territory counter-terrorism policy. As part of its role, ASIO also hosts the National Intelligence Group (NIG), which coordinates intelligence collection and strategic assessments during a terrorist incident.

National anti-terrorist exercises

In 2002-03 ASIO participated in two State-based counter-terrorism exercises in Queensland and Victoria. Our engagement in the National Anti-Terrorism Exercise (NATEX) in Western Australia was reduced due to re-deployment of resources with the commencement of hostilities in Iraq. ASIO also participated in four nationally coordinated counter-terrorism training courses (one in Western Australia, one in Tasmania and two in the ACT).

Counter-Terrorism Overseas Response Group

ASIO is also a member of the Counter-Terrorism Overseas Response Group (CTORG), which is chaired by DFAT and includes Commonwealth agencies responsible for responding to overseas terrorist incidents posing a threat to Australians or Australia's interests, or leading to requests for assistance from a foreign government. ASIO coordinates security intelligence support to the CTORG.

Technical Support Unit

ASIO's Technical Support Unit (TSU) can be called upon to assist the State and Federal police manage a terrorist incident. Its role is to provide technical support to the police commander managing the incident and the police technical units in gathering intelligence at the scene. The TSU is continuously maintained in a high state of readiness and is regularly exercised.

The TSU was deployed to a NATEX in Perth in March 2003, but was recalled to Canberra following the outbreak of hostilities in Iraq. The TSU also attended an Operation Response Exercise (OPREX) in August 2002, a NATEX in Melbourne in June 2002 and an OPREX in Canberra in May 2003.

Warrant operations

Special powers

Under its legislation ASIO is permitted — subject to a warrant approved by the Attorney-General — to use intrusive methods of investigation, which may include telecommunications interception, listening devices, entry and search of premises, computer access, tracking devices and examination of postal and delivery service articles.

Warrant approvals

Only the Director-General can seek warrants, which are issued only for specified limited periods. Each warrant must be accompanied by a written statement specifying the grounds on which it is considered necessary to conduct an intrusive investigation. Applications for a warrant must go through a system of checks — including examination by the ASIO Legal Adviser and independent certification by a senior official of the Attorney-General's Department — before being presented to the Attorney-General for consideration.

At the expiry of each warrant ASIO reports 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.

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

Telecommunications interception

Telecommunications interception (TI) can only occur subject to a warrant approved by the Attorney-General.

Telecommunications interception capabilities include:

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

The *Telecommunications Act 1997* requires all C/CSPs, including Internet service providers (ISPs), to develop, install and maintain interception capabilities unless specifically exempted. It 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, and for these costs to be recovered.

The commercial environment

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

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 three to 115, of which 96 remain current. There are approximately 800 carriage service providers (including ISPs).

Growth in the technological diversity of services being offered to the public also continues, with accelerating rollouts of broadband Internet access services including digital subscriber line (DSL) technology, GPRS and 3G mobile networks and IEEE 802.11b (WiFi) networks.

Contribution to policy

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

Partnerships with industry

We develop technical specifications, negotiate and manage contracts with C/CSPs, and test and accept new capabilities on behalf of all Commonwealth and State intercepting agencies.

Funding

C/CSPs are responsible for the development costs of interception capabilities, with intercepting agencies required to pay for agency-specific delivery capabilities and ongoing delivery costs.

Human source intelligence collection

ASIO collects intelligence by recruiting and managing human sources — people who are willing to provide information about individuals, groups or foreign governments of security interest. We also conduct declared interviews of members of the public or targets to assist with our investigations.

A well-placed human source can provide ASIO with valuable information about security issues, but they can take a long time to recruit and develop. We invest significant resources to develop human source management skills in our intelligence officers.

Human source management

ASIO continually reviews its human source base to ensure maximum benefit is obtained from resource allocations. In 2002-03 the review process resulted in de-registration of several sources and provided the opportunity to redirect some sources to new, higher priority targets.

Surveillance

ASIO surveillance teams report on people of security interest. Surveillance operations provided valuable intelligence in support of investigations and operational planning in 2002-03.

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.

Funding was provided from 2002-03 to establish a 24-hour research, monitoring and alert capability. The Research and Monitoring Unit (RMU) became fully operational in September 2002.

The RMU provides Commonwealth and State clients with a daily compilation of relevant unclassified reporting. It also provides an open source research service drawing on unclassified publications and electronic sources. Provision of these services increased by 39% during the year, reflecting the growth in open source material relevant to counter-terrorism.

In December 2002 the Government established a National Security Hotline to allow the public to report information of possible security relevance. The Hotline received 19 707 calls by 30 June 2003, of which 7 537 were forwarded to ASIO. We assessed 1 049 of these contained sufficient information to initiate investigations; 141 are still being investigated. While few of the calls required major investigation, several contributed to our understanding of the security environment or related to existing investigations.

Liaison with Australian agencies

ASIO continued to rely on strong cooperative partnerships with Commonwealth and State agencies to advance investigations and provide access to information to identify and monitor individuals of security interest. The sharing of information between ASIO and other agencies is regulated by the *ASIO Act*, and monitored by the Inspector-General of Intelligence and Security.

Following 11 September, interaction between Australian agencies increased markedly as measures to predict and prevent terrorism were jointly developed and implemented. The importance of these measures was emphasised after the Bali attack, when inter-agency cooperation played a vital role in investigating the attacks and assessing the ongoing threat. Counter-terrorism investigations in 2002-03 saw extensive cooperation between agencies including ASIO, State police, the AFP, ASIS, DSD, Defence, DFAT, DIMIA and others.

Regular meetings between ASIO's senior management and managers from ASIS, DSD and the AFP slipped after Bali, as activity focused on supporting the Bali investigations. However, the meetings — which focus on strategic directions, cooperative arrangements, and identifying opportunities to share resources — have since resumed.

Following the 11 September attacks, the Government agreed to the formation of a new Joint Counter Terrorism Intelligence Coordination Unit (JCTICU) to enhance collaboration on counter-terrorism investigations and related operations.

The JCTICU commenced operation on 2 September 2002. Located in ASIO, it includes officers from ASIO, DSD, AFP, ASIS and DIGO. Day-to-day management is an ASIO responsibility, but the Director reports to an inter-agency Steering Committee each quarter.

Since commencing operation the JCTICU has:

- Provided analytical and management support and specialist advice to ASIO's Bali Investigation Team.
- Facilitated passage of information to provide leads and complement ASIO/AFP investigations.
- Facilitated dialogue on technical cooperation.

Police

The year was notable for increased interaction with Federal and State/Territory Police. Inter-agency exchanges have been ongoing since September 11, and were heightened following the Bali bombings. ASIO held regular meetings with law enforcement agencies in most States and Territories, including bi-monthly meetings on counter-terrorism issues between ASIO's Deputy Director-General and the Deputy Commissioners of State/Territory police services.

- The National Security Hotline (see page 40) required regular liaison between ASIO, the AFP and State/Territory Police to ensure leads were pursued.
- In October 2002 the AFP and relevant State police services assisted ASIO in the conduct of search and entry operations of suspected JI members (see page 15).

The AFP and NSW Police assisted in unrelated search and entry operations, as part of ASIO investigations of persons suspected of involvement or support for terrorism.

- State police services provided support more generally for ASIO operations, providing police escorts to ASIO officers and providing information on individuals of security interest to ASIO.

Other agencies

The Australian Customs Service (ACS) provided significant support to ASIO.

Other Federal and State agencies including DIMIA and DFAT provided significant support for our investigations. We acknowledge the particularly heavy load placed on telecommunications providers in responding to high demand.

Liaison with overseas partners

ASIO communicates with the security and intelligence authorities of a range of countries approved by the Attorney-General. These international relationships are central to our counter-terrorism effort. They provide access to security and intelligence information that cannot be otherwise obtained, particularly about threats to Australian interests overseas and threats to Australia which originate offshore.

As at 30 June 2003 we had liaison relationships with 238 organisations in 107 countries and territories. The Attorney-General approved liaison with four new agencies during 2002-03.

Strategic relationships

Cooperation on counter-terrorism with Southeast Asian and Middle Eastern liaison partners remained a high priority in 2002-03, reflecting the current security environment and the heightened threat to Australian interests in those areas.

Areas of engagement

In Southeast Asia we are increasing engagement on al-Qa'ida and Jemaah Islamiyah. We also continued to engage with regional counterpart agencies in the Pacific.

Maximising the benefit of our intelligence partnerships will remain a key business focus in coming years.

Significant visits

During 2002-03 we hosted visits by senior officers from government and intelligence partners.

Olympics support

ASIO is a member of the Greek Olympics Advisory Security Group (OAG) formed by the Greek government to provide security advice in relation to the Athens 2004 Olympics.

Technical capabilities

ASIO's engineering development group provides rapidly engineered devices, custom versions of existing devices and oversees acquisition of commercially available equipment and management of outsourced projects, with several projects successfully outsourced in 2002-03.

Cooperation with Australian agencies

We maintained productive relationships with agencies including DSD, the Defence Scientific and Technology Organisation, the AFP and a number of State law enforcement agencies. Inter-agency cooperation on technical development will continue to be a focus in 2003-04.

Parts of this performance report are excluded from the 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 Defence or the Minister for Foreign Affairs, and
- collecting foreign intelligence incidentally through ASIO's security intelligence investigations and liaison with overseas partners.

This performance report is excluded, in its entirety, from the 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 twice monthly and otherwise as required. 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, chaired by the Deputy Director-General and including an SES officer from the Australian National Audit Office. Figure 14 shows other corporate committees.

Figure 14. 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 an unclassified *Report to Parliament*. Financial activities are regularly audited and certain budgetary details published in the annual Budget Papers.

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.

The *Corporate Plan* is a public document, and is available on the ASIO Website at www.asio.gov.au

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

- The *2000-01 Information Management Strategy*, a review of which is under way and will be completed in late 2003.
- The *Security Management Plan 2001-04*, which will be reviewed in 2003.

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 and external reviews and evaluations, overseen by the Audit and Evaluation Committee, continued in 2002-03.

Fraud Control Plan

Our Fraud Control Plan has been assessed by the Interdepartmental Fraud Control Evaluation Committee and meets Commonwealth requirements. Two officers attended an AFP-accredited Fraud Investigations course in 2002-03.

No fraud investigations were undertaken in 2002-03.

Evaluations

One evaluation, of the Graduate Traineeship program, was completed in 2002-03; its recommendations will be implemented in 2003-04.

Audits

Five internal audits were completed, including:

- Compliance with the NSW *Law Enforcement and National Security (Assumed Identities) Act 1998*.
- Finance processing and controls.
- Payroll processing and controls.
- Two compliance audits to satisfy the requirements of State legislation and memoranda of understanding.

No loss of monies or assets was reported, and remedial action to redress any administrative or procedural shortcomings arising from these audits has been finalised or is continuing.

External Scrutiny

ASIO's activities are subject to external scrutiny through Ministerial oversight and by the Inspector-General of Intelligence and Security, the Auditor-General and the Parliamentary Joint Committee on ASIO, ASIS and DSD.

The Leader of the Opposition receives a copy of ASIO's classified *Annual Report*, and briefings by the Director-General as required under the *ASIO Act*.

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 2002-03 we provided the Attorney with 214 briefing papers and submissions on significant security and ASIO-related issues (compared with 158 in 2001-02).
- All operational activity by ASIO must comply with the Attorney-General's *Guidelines for the Collection of Intelligence*, which require ASIO to use methods of investigation which are appropriate to the perceived risk.
- The Attorney-General also receives reports from the Inspector-General on inquiries relating to ASIO, including complaints.

The Inspector-General

The Inspector-General's role is to ensure ASIO acts legally and with propriety, complies with Ministerial guidelines and shows due regard for human rights. He may inquire into matters on his own initiative, at the request of the Attorney-General or the Government, or in response to complaints. The Inspector-General undertakes regular reviews of ASIO activities, including:

- access to operational files
- 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
- access to and use of information obtained from the Australian Taxation Office, and
- compliance with the *Archives Act*.

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

In his 2002-03 report the Inspector-General noted that he inquired into 21 new complaints about ASIO in 2002-03 (compared with 16 in 2001-02). These included 19 preliminary inquiries into complaints specifically related to ASIO, and two inquiries into matters involving Australian intelligence agencies including ASIO. He also dealt with four matters carried over from 2001-02 and handled a further 32 complaints administratively.

Bali inquiry

On 23 October 2002 the Prime Minister asked the Inspector-General to review all relevant intelligence available to Australian intelligence agencies, and associated intelligence assessment processes, to establish whether there was any information that could have provided warning of the bombings in Bali in October 2002.

As part of this inquiry ASIO conducted an extensive search of electronic and hard copy records dating back to 11 September 2001.

In his report to the Prime Minister, presented in December 2002, the Inspector-General announced that the inquiry had concluded that there was no intelligence received by Australian agencies which provided warning of the attack.

The Inspector-General's *Annual Report* can be found at www.igis.gov.au

The PJC

The Parliamentary Joint Committee on ASIO, ASIS and DSD (the PJC) reviews aspects of ASIO activities referred to it by the Minister or by either Chamber. The PJC has a mandate to review ASIO administration and expenditure and presents an *annual report* to Parliament. PJC members are listed at Appendix A.

The PJC's functions do not include review of operationally sensitive matters, intelligence gathering priorities or individual complaints. The Committee must conduct reviews in private unless the Minister determines otherwise. The Minister may certify that certain evidence should not be provided to the PJC.

The PJC may request the heads of the relevant agencies and the Inspector-General to provide briefings for the purpose of performing its functions. In 2002-03, the Director-General briefed the PJC:

- on 23 October 2002, regarding developments in counter-terrorism (including Bali)
- on 2 December 2002, regarding security arrangements in ASIO, ASIS and DSD, and
- on 27 March 2003, regarding agency security arrangements.

Other Parliamentary Committees

In 2002-03 the Director-General appeared before other Parliamentary committees inquiring into intelligence and security matters, including:

- the Senate Committee on Foreign Affairs, Defence and Trade on 19 June 2003 at the *Inquiry into the performance of the Department of Foreign Affairs and Trade and other relevant agencies of the Commonwealth Government in the assessment and dissemination of threats to the security of Australians in Southeast Asia in the period 11 September 2001 to 12 October 2002*
- the Joint Standing Committee on Foreign Affairs, Defence and Trade, Human Rights Sub-Committee, on 22 August and 23 September 2002, and 18 June 2003
- the Joint Standing Committee on Foreign Affairs, Defence and Trade, Foreign Affairs Sub-committee, on 12 November 2002 in relation to Australia's relations with Indonesia
- the Senate Legal and Constitutional Legislation Committee on 27 May 2003 at the Senate Estimates hearings
- public hearings of the Senate Legal and Constitutional Committee's *Inquiry into the ASIO Bill* on 12-13 November, 18 November and 26 November 2002, and
- The House of Representatives Standing Committee on Communications, Information Technology and the Arts on 21 August 2002.

Interface with the Public

The current security environment has increased public awareness of terrorism and security issues in Australia. This has been reflected in a significant increase in the amount of information voluntarily reported by members of the public. All information received from the public is assessed and appropriate action taken.

ASIO interviews

ASIO officers may interview members of the public as part of investigations. ASIO officers operate under a strict code of conduct when undertaking such interviews. They must show proof of identity, and if the interviewee is concerned they can telephone the public ASIO line (see Appendix B) to confirm the officer's identity.

A person interviewed may complain to ASIO or to the Inspector-General if they have concerns about the behaviour of an ASIO officer. Complaints about ASIO are carefully evaluated. Some reflect misconceptions about ASIO's roles and powers, and discussion with an ASIO officer can often clarify issues or resolve concerns. In other cases, complainants are referred to the Inspector-General.

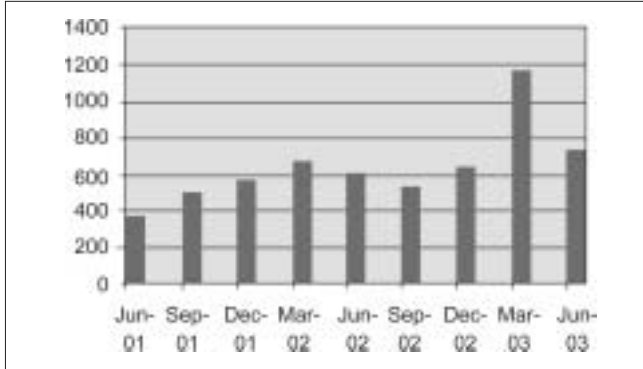
ASIO publishes brochures and pamphlets about its work, in addition to its *Annual Report*. Members of the public can call ASIO's public telephone number and request information about the Organisation.

www.asio.gov.au

Interest in the ASIO website remained high. In 2002-03 the site recorded an average of 24 945 hits and 762 visitor sessions per day, increases of 39% and 31% respectively on 2001-02. Employment pages remained the most popular.

- In 2001-02 an independent consultant reviewed the site, and we will begin implementing their recommendations in late 2003.
- Plans to translate our brochure *ASIO Now* into several community languages were delayed by the reallocation of resources after the Bali attack. Translation will now commence in late 2003 and an updated version of the brochure will be made available on the website and in hard copy.

Figure 15. 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 terrorism and security issues increased after the 11 September attacks and was raised further following Bali. Interest in ASIO activities and issues was 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 newspaper articles raising interest in our recruitment campaign.

Our People

ASIO's success depends on recruiting, developing and maintaining capable people to meet the new challenges the Organisation faces. Key drivers for our people management strategy are:

- the need to attract and retain highly skilled, motivated staff in a changing and competitive employment market with a growing demand for intelligence and security expertise, and
- the need to identify future staffing requirements, and structure our recruitment and development programs to meet these needs.

People management priorities for 2002-03 included:

- Ongoing recruitment and training of staff to manage increased workloads following the changes to the security environment.
- A further expanded and enhanced development program for existing staff.
- Negotiating our 6th Workplace Agreement with a continuing focus on retaining our skilled staff.
- Ensuring a smooth transition of staff into a new, expanded structure.

As of 30 June 2003, ASIO had around 668 staff; this will increase over the next two years to about 830, the highest level since the mid 1980s.

Workplace Relations and Reforms

In 2002 negotiations began on a 6th Workplace Agreement, with the 5th Agreement expiring on 30 March 2003. An initial proposal was voted on in December 2002, and was rejected by the majority of staff. Following further negotiations, a revised agreement was accepted following a ballot on 7-8 April 2003, and came into effect on 10 April 2003. 78% of all eligible staff participated in the second ballot, with 68% of those voting in favour of the Agreement.

Major initiatives in the 6th Agreement include:

- Salary increases of 4.5% on 10 April 2003, 4% on 1 April 2004 and 4% on 1 April 2005.
- Rationalisation of salary points.
- Increase in working hours from 7.35 hours to 7.5 hours per day.
- A stand-down between Christmas and New Year.
- Payment of excess hours at a rate of 1.35 times normal salary.

These changes reflected our need to negotiate a fiscally responsible outcome that also served to retain existing staff and to maintain our competitiveness with other public sector agencies.

As part of the 5th Workplace Agreement, in 2002-03 we adopted a new Performance Management Framework (PMF). The new PMF encourages staff and managers to jointly define, evaluate and recognise performance to ensure the goals of the Organisation and of individuals are met. We are seeking to improve performance, encourage success and facilitate the achievement of potential through constructive feedback to staff and active planning of staff learning.

*Workplace
initiatives*

*Performance
Management*

*Performance
Pay*

Performance pay is available to SES officers, with the amount paid based on a percentage of gross salary. In 2002-03 ten officers received performance pay. Payments ranged from \$6 686 to \$20 737. The average payment was \$11 269 and the total amount paid was \$112 689.

Recruitment and Staffing

Recruitment and staffing of ASIO remain a challenge, as we seek to expand the Organisation while maintaining the quality of staff.

Staffing profile

Employment of permanent staff was the primary aim of recruitment in 2002-03, although we continued to make use of contract employees to meet short term needs.

At 30 June 2003, 16.5% of staff were temporary employees compared to 16% at 30 June 2002. See Appendix C for staffing statistics.

Staff retention

ASIO's attrition rate dropped over the reporting period to 7%, and continues to fall. This probably reflects, in part, the growth which has created more opportunities within ASIO.

ASIO will conduct a Staff Survey in 2003-04 and use the information, together with other material, for workforce planning.

Recruiting

Recruitment for ASIO is a very resource intensive task, and the length of the recruitment process remains a problem. We had to pay close attention to recruitment targets and times in 2002-03, and this will need to continue into the next financial year. We have commissioned an external review to identify opportunities to further improve recruitment processes.

Early in 2002-03, recruiting focused on technical and surveillance staff to boost intelligence collection capabilities. The focus later shifted to recruiting analysts to support initiatives announced in the 2003-04 Budget.

ASIO recruited 28 graduate trainees in 2002-03, the same number as in 2001-02. At the end of the reporting period, recruitment of 30 graduates to commence in 2003-04 was in progress. Applications for the Graduate program increased slightly from last year, and the number of applications for all positions advertised in the media was also higher in 2002-03.

Advertising

We continued our advertising campaign to recruit the best people from the widest field. Our website continued to attract the interest of potential applicants, and we employed national recruitment companies to assist in our larger campaigns.

Advertising costs, mainly in the print media, were \$222 206 in 2002-03, compared to \$250 851 in 2001-02.

Developing our people

Training our new and existing staff remains a very high priority. It is especially important as we seek to expand our specialist groups and enhance our officers' capabilities. As a result we invested about 2.1% of

*Leadership and
management
development*

our budget (\$1.73 million, an increase of \$330 000 on 2001-02) on training and development in 2002-03, including corporately-funded training and job-specific courses funded by individual work groups. In addition, on-the-job training remained a significant element in developing corporate expertise. Training focused on both intelligence-specific competencies and leadership, management and administrative skills across the Organisation.

Four officers were added to our training team — an increase of 50% — to meet expanded training needs following growth in staff numbers.

Leadership development was a priority, including all SES and Senior Officers. Training activities included 'time-outs', formal in-house and external courses, and support for tertiary education.

- Three SES time-outs focused on planning and implementing changes arising from the management restructure and addressing continuing developments in the intelligence environment.
- In May 2003 a SES/Senior Officer time-out focused on restructure issues and national counter-terrorism response capabilities.
- We conducted a program of administrative training including contract management, interviewing, effective reading and writing, performance management and frontline management.
- Staff with direct responsibility for training people or managing teams attended 'Coaching and Team-building Skills for Managers and Supervisors'.
- We conducted specialised financial and contract management courses.
- 40 people were provided with support for tertiary studies.

*Analytical and
operational
skills*

The intelligence collection, analysis and reporting skills of our officers are developed through a comprehensive training program. Some of this training is conducted in cooperation with foreign intelligence partners. In 2002-03:

- As part of our continued focus on developing expertise on terrorism-related issues, ASIO-initiated courses were conducted on 'Terrorism: International Perspectives' and 'Introduction to Islam'.
- Computer training was provided for all staff in upgraded office applications, with additional training for staff using specific applications.

*Technical
capabilities*

Technical intelligence collection skills remained a key priority for ASIO. Our capabilities in these areas were enhanced through joint training with intelligence partners, in-house training and attendance at commercial courses.

*Counter-
terrorism*

Fifty ASIO officers participated in counter terrorism training, including National Anti-Terrorism Exercises (see page 37).

*Information
Management*

Training in the use of ASIO's computer system and applications — including upgrades associated with the Advanced Infrastructure Project Mark II (see page 58) — was provided to 357 staff.

Two ASIO Traineeship Programs commenced, and two were completed, with graduating trainees taking up positions across the Organisation.

- Traineeships run for twelve months and involve a mix of coursework and three 11-week placements in key areas of ASIO.

Intensive two-day Introduction to ASIO Programs, which are compulsory for all new starters, ensured people joining ASIO were integrated into the Organisation as quickly and seamlessly as possible.

Secondments and personnel exchanges with other agencies continued.

Workplace Diversity

Statistical data on ASIO's staff numbers, workforce profile, representation of designated workgroups and salary structure are contained in Appendixes C, D and E.

ASIO continued to offer staff a range of family-friendly initiatives, including:

- job sharing
- designing jobs (where possible) to allow officers to work outside normal office hours or in different geographic locations
- flexible leave provisions including the ability to purchase extra leave, and to access long service leave for a minimum period of one week, and
- personal leave arrangements that include provision for staff to care for sick family members and meet other unforeseen family commitments.

Our workplace diversity figures remained relatively unchanged in 2002-03. The percentage of ASIO employees with disabilities and from non-English speaking backgrounds remained low.

The percentage of female staff increased from 40% to 42%, with the percentage of female staff at senior officer level increasing from 18% to 23%.

Our workplace diversity and harassment officers completed a training program during the year which focussed on their roles and the assistance and advice that they could provide managers and staff.

Disability Strategy

Development of ASIO's Disability Strategy and associated action plan will be completed in the next reporting period. However, ASIO already has in place some of the elements outlined by the Office of Disability in its guide for agencies.

ASIO policies and initiatives to assist those with disabilities include:

- being an equal opportunity employer
- access for all staff to formal and informal complaints mechanisms, including through the ASIO Staff Association, the ASIO Ombudsman, and access to external review mechanisms
- considering the needs of those with disabilities in all internal policies, and
- raising awareness of workplace diversity through internal training courses and publications.

Occupational Health and Safety

ASIO's Occupational Health and Safety sub-committee oversaw the continued implementation of the OH&S Agreement, which included 19 OH&S audits. Significant health and safety initiatives included:

- A phased approach to Health Week, resulting in activities and health checks being conducted over two separate weeks.
- Offering influenza vaccinations to promote health in the workplace and reduce absenteeism.
- Selecting and training first aid and health and safety representatives.
- In response to a Management initiative in the 6th Workplace Agreement we are formulating an ongoing Health and Safety program, which when introduced will provide OH&S-related speakers and activities throughout the year.

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.

In 2002-03 there were 11 claims for compensation; liability was admitted for all 11, compared with seven in 2001-02. ASIO's Comcare premium increased significantly for 2003-04, against which we have lodged an objection.

Information Management

ASIO's capacity to access intelligence information and disseminate advice relies on efficient and secure information management. Information technology and information management remains a high priority.

A major revision of the *Information Management Strategic Plan* commenced in 2002-03, and a new Plan will be released by late 2003. The Plan documents the five-year strategic outlook of information management in ASIO, under the themes of:

- Maintenance of Capability.
- Enhanced Intelligence Information Capability.
- Enabling Organisational Growth.
- Information Centring.
- Security.
- Enhanced Corporate Information Capability.

The major information management initiatives scheduled for 2003-04 are:

- Implementing the records management system for paper records.
- Major upgrades to the data communications capability and local data processing capability of our Liaison Offices.
- Reviewing ASIO's business continuity plan.
- A major systems upgrade to support the Aviation Security Identity Card initiative (see page 30).
- Enhancing the security of ASIO's corporate intelligence database to permit incorporation of Restricted Circulation Material.
- Enhancing ASIO's information analysis capability, particularly in the areas of data mining, pattern matching and visualisation.

The Advanced Infrastructure Project Mark II was completed in 2002-03, replacing the computing infrastructure in all of ASIO's offices in Australia and overseas. As well as upgrading all PCs and servers, the project upgraded the operating system and office automation package, including word processing, spreadsheet and email capabilities.

In 2002-03 the secure telephone network was replaced with new generation Voice Over IP (VOIP) technology. The transition to VOIP technology delivered increased portability of extensions, teleconferencing facilities and improved visual display of caller information.

Information management improvements pursued in 2002-03 included replacement of the ASIO records management system. Following a competitive tender process, a commercial off-the-shelf software package for paper file management was selected and is being implemented. Business enhancements will be made where possible to take advantage of efficiencies offered by the new software.

Security of ASIO

ASIO's security culture is based on well-established and documented security policies, procedures and practices designed to protect classified information, ASIO sources, operational tradecraft, IT systems and ASIO staff. While appropriate and effective security policies and procedures are necessary and important they are not, of themselves, sufficient. To this end, ASIO continued to improve its integrated approach to security risk management and the development of a security culture.

*Infrastructure
development*

*Records
management*

ASIO has continued to benefit from the *Inquiry into Security Issues*, with the bulk of its recommendations applicable to ASIO now implemented.

ASIO's *Security Management Plan 2001-2004* sets out objectives and strategies to maintain security within ASIO. The Plan conforms with the principal themes of the *Inquiry into Security Issues* and fulfils the *Commonwealth Protective Security Manual* requirement for all departments and agencies to have a security plan that supports the agency's goals through security risk management. This Plan will be reviewed in early 2004 with special attention to reinforcing the security culture.

The plan is supported by a number of internal policies and procedures. These range from electronic pass checking and random bag searches to more complex practices, including the isolation of ASIO computer networks from outside contact and the security clearance and regular re-evaluation of all staff. Our strategy is to minimise risk from:

- foreign intelligence services attempting to penetrate ASIO or gain access to ASIO information
- targeting of ASIO by hostile groups or individuals, and
- unauthorised disclosure of information by ASIO staff.

All ASIO staff are cleared to Top Secret (Positive Vetting) level. This process involves detailed examination of an officer's background, including financial checks, police checks, psychological assessments, interviews of referees and interviews of the officers themselves. The process meets the standard set by the Inter-Agency Security Forum. Clearances are revalidated every 30 months and fully re-evaluated at least every five years. There were 90 revalidations and 59 full re-evaluations completed in 2002-03.

Although not a *Protective Security Manual* requirement, our process of reviewing security clearances includes an interview with all new staff members after 5-6 months with ASIO. The objective of these interviews is to review the officer's understanding of security processes and reinforce the importance of security. We conducted 97 of these interviews in 2002-03. In addition, ASIO managers are required to undertake an annual security assessment of all staff.

To ensure best practice in the security assessment process, ASIO is undertaking a review of the Assessing Officer's Handbook, which provides guidelines on vetting practice and areas to be covered during the re-evaluation process.

New employees are introduced to ASIO's in-house support staff, whose role is to provide assistance with personal and professional matters that may have security implications. We provide this support, as well as psychological counselling and other assistance, to ensure issues are properly managed so they do not become a matter of security concern.

IT security

In 2002-03 we developed a new IT security training facility to address the need to protect our information holdings. ASIO's access to and use of the Internet was given close attention, and programs were developed to improve understanding of external threats to the Internet and IT systems.

ASIO's Information Systems Security Policies were reviewed in 2002-03, and our telecommunications environment was reaccredited by DSD.

Physical security

In 2001-02, following the *Inquiry into Security Issues*, a Protective Security Risk Review of all ASIO offices was undertaken. Against the background of the changing security environment, a further review of security at ASIO's Central Office was undertaken in 2002-03, resulting in further upgrades to physical and electronic security and the establishment of the Russell Incident Group, which reports on security incidents relevant to the ASIO/Defence complex at Russell.

Security audits

ASIO continued its regular security audits of offices, persons with access and operational activity to ensure they conform to security policies and procedures, and to monitor any attempts to infiltrate the Organisation. These audits examine:

- the security of our information holdings, including the security of ASIO's information technology
- the distribution and handling of accountable documents
- the requirements involved in meeting security obligations to other countries
- the maintenance of security of ASIO operations, sources and officers
- the physical security of ASIO buildings and assets, and
- the security of ASIO staff.

Security policies

A range of policies to enhance our internal security and heighten awareness of security issues were developed or revised in 2002-03. These were circulated to all staff and made available on our Intranet.

- A number of internal processes were reviewed; these related to visitor entry, escort briefing and the authority to remove classified material.
- A Corporate Security Policy for IT systems was issued.
- Auditing of IT systems was upgraded to ensure appropriate access and use.

Building Management

The rental review on the ACO building was finalised in 2002-03 with a 34% increase in rent. We received budget supplementation to cover the additional cost. The next rent review is scheduled for 2003-04.

A number of refurbishment activities occurred in the ASIO Central Office over 2002-03. These included:

- Refurbishment of two floors.
- Refurbishment of the library and IT training rooms.
- Planning and commencing refurbishment to accommodate additional staff.
- ACO car park lighting was installed and drainage problems rectified.

Ecologically sustainable development and environmental performance

ASIO engaged Asset Services to conduct an energy audit on the plant and utilities within its Central Office. The final report makes recommendations to optimise the use of electricity and gas consumption for the building; funds have been set aside in 2003-04 to facilitate some of these changes.

Energy demand in Central Office increased markedly during the period following the Bali attack and ASIO search operations, when staff worked extended hours.

A range of recycling, waste and water management initiatives were introduced to minimise the impact of ASIO on the environment, including:

- sealing the building perimeter of Level 2 to allow proper balancing of the air conditioning system
- installing auto transformers on lighting circuits
- recycling paper and cardboard (where security requirements permit)
- increasing use of electronic forms to reduce paper usage, and
- raising staff awareness of ASIO's environmental responsibilities.

Purchasing

All purchasing activity in ASIO is conducted in accordance with the Chief Executive Instructions, which require that as far as security restrictions permit, all Commonwealth Procurement and Best Practice Guidelines are met. As far as possible, value for money is achieved through competitive quotations or restricted tenders, evaluated on a whole-of-life basis of the item being procured.

For security reasons, ASIO does not notify procurement information in the Purchasing and Disposal Gazette; however, contract details can be made available to Members of Parliament as a confidential briefing or to the Parliamentary Joint Committee on ASIO, ASIS and DSD.

In 2002-03 our annual investment program continued. Purchasing objectives focused on investment in key business areas, including information technology infrastructure and protective security measures.

Consultants and Contractors

Expenditure on consultancy contracts fell slightly to \$0.704m, compared to \$0.771m in 2001-02. The decrease resulted primarily from completion in 2001-02 of the development phase of computer infrastructure upgrades, which were implemented in 2002-03 using ASIO resources and contract support. The scope for outsourcing in ASIO continues to be limited due to national security considerations.

A list of the 13 consultancy contracts, excluding elements removed for security reasons, is available on request.

In 2002-03 we established a specialised position to manage contracts and the contracting process. We expect this position to be filled in late 2003.

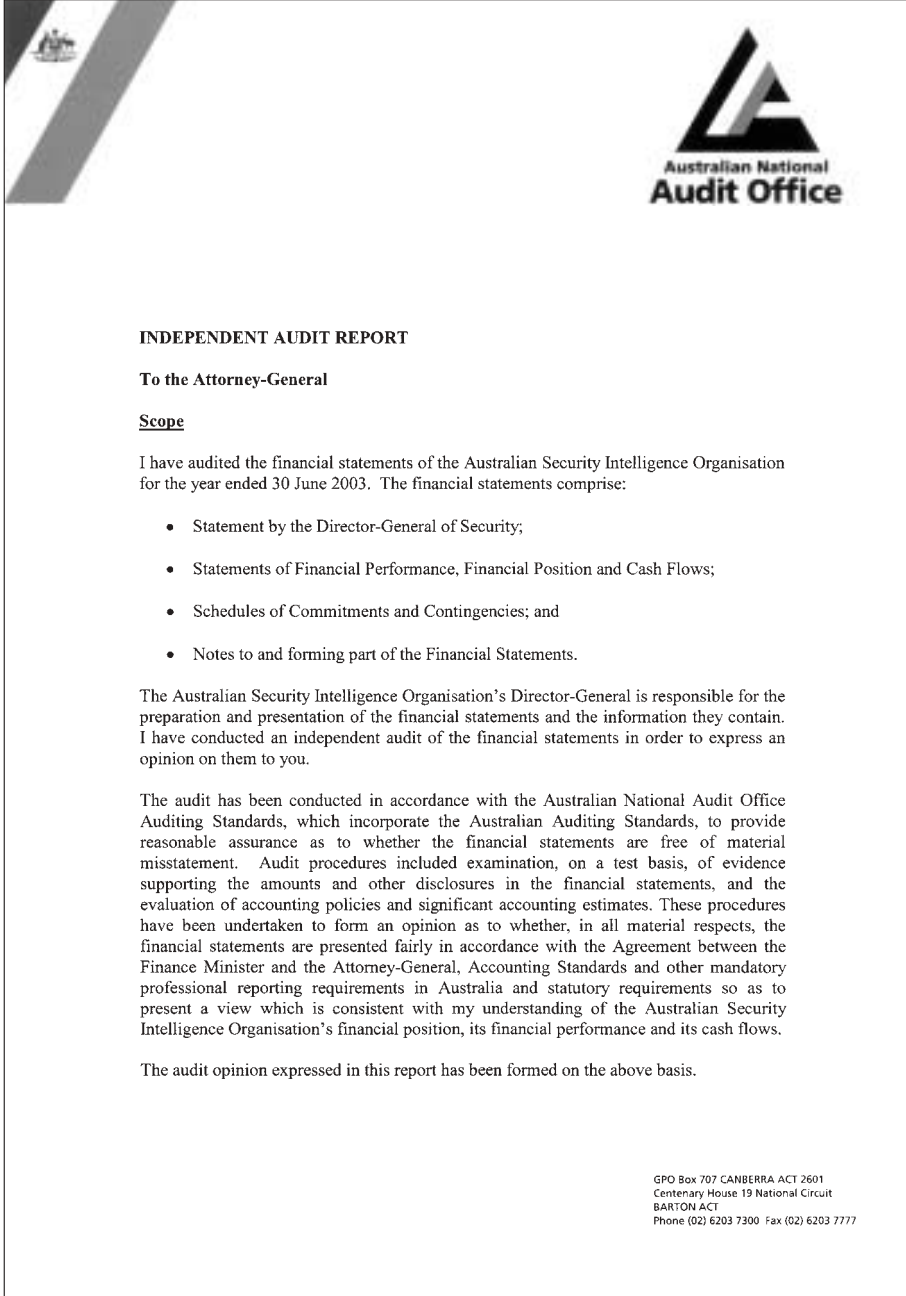
Parts of this performance report are excluded from the unclassified *Report to Parliament* because of security sensitivity.

Part 4

Financial Statements



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



Audit Opinion

In my opinion the financial statements:

- (i) have been prepared in accordance with the Agreement between the Finance Minister and the Attorney-General and the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*; and
- (ii) give a true and fair view, in accordance with the Agreement between the Finance Minister and the Attorney-General, 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 2003 and its financial performance and cash flows for the year then ended.

Australian National Audit Office



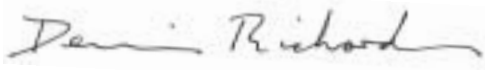
Brandon Jarrett
Acting Executive Director

Delegate of the Auditor-General

Canberra
16 September 2003

Statement by the Director-General of Security

In my opinion, the attached financial statements for the year ended 30 June 2003 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 that reads "Dennis Richardson". The signature is written in a cursive style with a long horizontal flourish at the end.

Dennis Richardson
Director-General of Security

15 September 2003

Statement of Financial Performance for the year ended 30 June 2003

	Notes	2003 \$ '000	2002 \$ '000
Revenues from ordinary activities			
Revenues from Government	3A	86 237	65 682
Sales of goods and services	3B	1 113	6 851
Interest	3C	13	210
Revenue from sale of assets	3D	859	1 088
Other	3E	723	1 084
<i>Revenues from ordinary activities</i>		<u>88 945</u>	<u>74 915</u>
Expenses from ordinary activities (excluding borrowing costs expense)			
Employees	4A	48 660	41 959
Suppliers	4B	33 271	24 786
Depreciation and amortisation	4C	8 075	6 606
Write-down of assets	4D	41	947
Value of assets sold	3D	898	1 241
<i>Expenses from ordinary activities (excluding borrowing costs expense)</i>		<u>90 945</u>	<u>75 539</u>
<i>Borrowing Costs Expense</i>		<u>38</u>	<u>58</u>
Net surplus / (deficit)		<u>(2 038)</u>	<u>(682)</u>
Net credit to asset revaluation reserve	11	<u>—</u>	<u>4 349</u>
<i>Total revenues, expenses and valuation adjustments attributable to the Commonwealth Government and recognised directly in equity</i>		<u>—</u>	<u>4 349</u>
<i>Total changes in equity other than those resulting from transactions with owners as owners</i>		<u>(2 038)</u>	<u>3 667</u>

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

Statement of Financial Position as at 30 June 2003

	Notes	2003 \$ '000	2002 \$ '000
ASSETS			
Financial assets			
Cash	5A	5 350	6 631
Receivables	5B	2 031	741
<i>Total Financial Assets</i>		<u>7 381</u>	<u>7 372</u>
Non-Financial Assets			
Land and buildings	6A, 6D	12 781	11 981
Infrastructure, plant and equipment	6B, 6D	20 020	19 460
Intangibles	6C, 6D	2 631	2 219
Other	7	628	377
<i>Total Non-Financial Assets</i>		<u>36 060</u>	<u>34 037</u>
TOTAL ASSETS		<u><u>43 441</u></u>	<u><u>41 409</u></u>
LIABILITIES			
Interest Bearing Liabilities			
Leases	8	331	533
<i>Total Interest Bearing Liabilities</i>		<u>331</u>	<u>533</u>
Provisions			
Capital use charge	9A	—	468
Accommodation leases - make good	9B	1 032	—
Employees	9C	13 781	13 068
<i>Total Provisions</i>		<u>14 813</u>	<u>13 536</u>
Payables			
Suppliers	10A	4 523	3 339
<i>Total Payables</i>		<u>4 523</u>	<u>3 339</u>
TOTAL LIABILITIES		<u><u>19 667</u></u>	<u><u>17 408</u></u>
NET ASSETS		<u><u>23 774</u></u>	<u><u>24 001</u></u>
EQUITY			
Contributed equity	11	22 144	17 452
Reserves	11	6 279	6 279
Retained surpluses or (accumulated deficits)	11	(4 649)	270
TOTAL EQUITY		<u><u>23 774</u></u>	<u><u>24 001</u></u>
Current assets		8 009	7 749
Non-current assets		35 432	33 660
Current liabilities		11 484	9 672
Non-current liabilities		8 183	7 736

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

Statement of Cash Flows for the year ended 30 June 2003

	Notes	2003 \$ '000	2002 \$ '000
OPERATING ACTIVITIES			
Cash Received			
Goods and services		1 207	9 210
Appropriations		85 675	64 996
Interest		13	210
GST received from ATO		2 921	2 163
<i>Total cash received</i>		<u>89 816</u>	<u>76 579</u>
Cash used			
Employees		47 947	41 599
Suppliers		34 780	24 362
Borrowing costs		38	58
<i>Total cash used</i>		<u>82 765</u>	<u>66 019</u>
Net cash from / (used by) operating activities	12	<u>7 051</u>	<u>10 560</u>
INVESTING ACTIVITIES			
Cash Received			
Proceeds from sales of property, plant and equipment		859	225
<i>Total cash received</i>		<u>859</u>	<u>225</u>
Cash used			
Purchase of property, plant and equipment		10 783	10 458
<i>Total cash used</i>		<u>10 783</u>	<u>10 458</u>
Net cash from / (used by) investing activities		<u>(9 924)</u>	<u>(10 233)</u>
FINANCING ACTIVITIES			
Cash received			
Appropriations - contributed equity		4 692	4 284
<i>Total cash received</i>		<u>4 692</u>	<u>4 284</u>
Cash used			
Repayment of debt		202	178
Capital use charge paid		2 899	746
<i>Total cash used</i>		<u>3 101</u>	<u>924</u>
Net cash from / (used by) financing activities		<u>1 591</u>	<u>3 360</u>
<i>Net increase/(decrease) in cash held</i>		<u>(1,281)</u>	<u>3 687</u>
Cash at the beginning of the reporting period		<u>6 631</u>	<u>2 944</u>
<i>Cash at the end of the reporting period</i>	5A	<u>5 350</u>	<u>6 631</u>

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

Schedule of Commitments as at 30 June 2003

	Notes	2003 \$ '000	2002 \$ '000
BY TYPE			
Capital commitments			
Land and buildings	A	1 582	—
Infrastructure, plant and equipment	B	553	520
<i>Total capital commitments</i>		<u>2 135</u>	<u>520</u>
Other commitments			
Operating leases	C	53 581	41 728
Other commitments		3 050	2 383
<i>Total other commitments</i>		<u>56 631</u>	<u>44 111</u>
Commitments receivable		<u>9 287</u>	<u>7 776</u>
Net commitments		<u><u>49 479</u></u>	<u><u>36 855</u></u>
BY MATURITY			
Capital commitments			
One year or less		2 135	520
From one to five years		—	—
Over five years		—	—
Operating lease commitments			
One year or less		4 730	3 577
From one to five years		19 300	13 457
Over five years		26 788	20 914
Other commitments			
One year or less		655	1 797
From one to five years		(1 708)	(1 440)
Over five years		(2 421)	(1 970)
<i>Net commitments by maturity</i>		<u><u>49 479</u></u>	<u><u>36 855</u></u>

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 2003

	Notes	2003 \$ '000	2002 \$ '000
Contingent liabilities		—	—
Contingent assets		—	—
Net contingencies		<u>—</u>	<u>—</u>

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

Notes to the Financial Statements for the year ended 30 June 2003

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 (Financial Statements 2002-2003) Orders* 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 (Financial Statements for reporting periods ending on or after 30 June 2003) Orders*);
- 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. Assets and liabilities arising under agreements equally proportionately unperformed are however not recognised unless required by an Accounting Standard. Liabilities and assets which 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 3.

Revenues from Government

Departmental outputs appropriations for the year (less any savings offered up in Additional Estimates Statements) is recognised as revenue.

Resources Received Free of Charge

Services received free of charge are recognised as revenue when and only when a fair value can be reliably determined and the services would have been purchased if they had not been donated. Use of those resources is recognised as an expense.

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 to other government bodies. The stage of completion is determined according to the proportion that costs incurred to date bear to the estimated total costs of the transaction.

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 by the Government as Owner

From 1 July 2002, the FMOs require that amounts of appropriations designated as 'equity injections' (less any savings offered up in Portfolio Additional Estimates Statements) are recognised directly in Contributed Equity as at 1 July or later date of effect of the appropriation.

This is a change of accounting policy from 2001-02 to the extent any part of an equity injection that was dependent on future events occurring was not recognised until the appropriation was drawn down.

The change in policy has no financial effect in 2002-03 because the full amounts of the equity injections for 2001-02 were recognised in that year.

A Capital Usage Charge of 11% (2002: 11%) is imposed by the Government on the departmental net assets of the Agency at year end. The net assets figure is adjusted to take account of asset gifts and revaluation increments during the financial year. The Charge is accounted for as a dividend to Government.

In accordance with the recommendations of a review of Budget Estimates and Framework, the Government has decided that the Charge will not operate after 30 June 2003.

E. Leases

A distinction is made between finance leases which effectively transfer from the lessor to the lessee substantially all the risks and benefits incidental to ownership of leased non-current assets and operating leases under which 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 inception of the lease and a liability recognised for the same amount. Leased assets are amortised over the estimated useful life of the asset. 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.

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.

G. Financial Instruments

Accounting policies for financial instruments are stated at Note 19.

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.

Asset recognition threshold

Purchases of property, plant and equipment with a historical cost equal to or in excess of \$2000 are capitalised in the year of acquisition and included in the financial statements. Assets with a historical cost under \$2000 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 revalued progressively in accordance with the 'deprival' method of valuation in successive three-year cycles so that no asset has a value greater than three years old.

ASIO has implemented its revaluations program as follows:

- Land and buildings, including leasehold improvements at State offices, were revalued as at 30 June 2002.
- Infrastructure, plant and equipment comprises computing and communications equipment, technical and operational equipment, office furniture, office equipment and motor vehicles. Computing and communications equipment was revalued during 2000-2001 and all other equipment items were revalued at 30 June 2002. Motor vehicles are changed over every two years and their value is disclosed at cost of acquisition.

Assets in each class acquired after the commencement of the progressive revaluation cycle will be reported at cost until the next progressive revaluation.

The financial effect of the move to progressive revaluations is that carrying amounts of assets will reflect current values and that depreciation charges will reflect the current cost of the service potential consumed in each period.

With the application of the deprival method, ASIO values its land at its current market buying price and its other assets at their depreciated replacement cost. Any assets which would not be replaced or are surplus to requirements are valued at net realisable value. At 30 June 2003, ASIO had no assets in this situation.

All valuations are independent except where specifically noted otherwise.

Recoverable amount test

From 1 July 2002, Schedule 1 no longer requires the application of the recoverable amount test in Australian Accounting Standard AAS 10 *Recoverable Amount of Non-Current Assets* to the assets of agencies when the primary purpose of the asset is not the generation of net cash inflows.

No property plant and equipment assets have been written down to recoverable amount per AAS 10. Accordingly, the change in policy has had no financial effect.

I. Depreciation of non-financial assets

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 amortised 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:

	2003	2002
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 4C.

J. Intangibles

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

From 1 July 2002, Schedule 1 no longer requires the application of the recoverable amount test in Australian Accounting Standard AAS 10 *Recoverable*

Amount of Non-Current Assets to the assets of agencies when the primary purpose of the asset is not the generation of net cash inflows.

However, Schedule 1 now requires such assets, if carried on the cost basis, to be assessed for indications of impairment. The carrying amount of impaired assets must be written down to the higher of its net market selling price or depreciated replacement cost.

All software assets were assessed for impairment as at 1 July 2002. None were found to be impaired.

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 (2001-02: 3 to 4 years).

K. 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. This is a change in accounting policy from last year required on initial application of a new Accounting Standard AASB 1028 from 1 July 2002.

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 2003 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 Commonwealth and is settled by the Commonwealth in due course.

ASIO makes contributions to the Commonwealth at rates determined by an actuary to be sufficient to meet the cost to the Commonwealth of the superannuation entitlements of the ASIO's employees.

The liability for superannuation recognised as at 30 June 2003 represents outstanding contributions for the final 8 days of the year.

L. Taxation

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

M. 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 considered material to the Organisation's operations.

N. 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.

O. 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.

P. Comparative figures

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

Q. 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.

R. Administered items

ASIO does not have any administered items.

S. Changes in accounting policy

The accounting policies used in the preparation of these financial statements are consistent with those used in 2001-02, except in respect of:

- measurement of certain employee benefits at nominal rates (refer note 1K)
- the imposition of an impairment test for non-current assets carried at cost (refer note 1J)

T. Borrowing costs

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

Note 2: Events occurring after reporting date

There were no events occurring after reporting date which had an effect on the 2003 financial statements.

	2003 \$ '000	2002 \$ '000
Note 3: Operating revenues		
Note 3A: Revenues from Government		
Appropriations for outputs	85 675	64 996
Resources received free of charge	562	686
<i>Total revenues from Government</i>	<u>86 237</u>	<u>65 682</u>
Note 3B: Sales of goods and services		
Provision of goods and services to:		
Related entities	922	6 802
External entities	191	50
<i>Total sales of goods and services</i>	<u>1 113</u>	<u>6 851</u>
Note 3C: Interest revenue		
Interest on deposits	<u>13</u>	<u>210</u>
Note 3D: Net gains from sale of assets		
Infrastructure, plant and equipment:		
Proceeds from disposal	859	1 088
Net book value of assets disposed	(898)	(1 241)
<i>Net gain/(loss) from disposal of infrastructure, plant and equipment</i>	<u>(39)</u>	<u>(153)</u>
TOTAL Proceeds from disposals	859	1 088
TOTAL value of assets disposed	(898)	(1 241)
<i>TOTAL net gain from disposal of assets</i>	<u>(39)</u>	<u>(153)</u>
Note 3E: Other revenues		
Rent	475	520
Miscellaneous	248	564
<i>Total other revenue</i>	<u>723</u>	<u>1 084</u>

2003	2002
\$ '000	\$ '000

Note 4: Operating expenses

Note 4A: Employee expenses

Wages and salary	35 816	33 480
Superannuation	5 566	4 603
Leave and other entitlements	1 993	859
Separation and redundancies	142	407
Other employee expenses	5 005	2 248
<i>Total employee benefits expense</i>	<u>48 522</u>	<u>41 597</u>
Workers compensation premiums	138	362
<i>Total employee expenses</i>	<u><u>48 660</u></u>	<u><u>41 959</u></u>

Note 4B: Suppliers' expenses

Goods and services from related entities	9 213	5 282
Goods and services from external entities	18 048	13 652
Operating lease rentals*	6 010	5 852
<i>Total supplier expenses</i>	<u>33 271</u>	<u>24 786</u>

* These comprise minimum lease payments only.

Note 4C: Depreciation and amortisation

Depreciation

Other infrastructure, plant and equipment	6 876	5 522
Buildings	54	43
<i>Total Depreciation</i>	<u>6 930</u>	<u>5 564</u>

Amortisation

Intangibles	1 145	1 042
<i>Total Depreciation and amortisation</i>	<u>8 075</u>	<u>6 606</u>

	2003	2002
	\$ '000	\$ '000
The aggregate amount of depreciation or amortisation expensed during the reporting period for each class of depreciable asset are as follows:		
Buildings	54	43
Leasehold improvements	1 363	1 018
Plant and equipment	5 513	4 503
Intangibles	1 145	1 042
Total	<u>8 075</u>	<u>6 606</u>

Note 4D: Write down of assets

Financial assets

- Foreign exchange variations	5	—
-------------------------------	---	---

Non-financial assets

- Plant and equipment written down due to change in capitalisation policy	—	729
- Plant and equipment written off at stocktake	21	210
- Plant and equipment — other	—	8
- Intangibles written off at stocktake	15	—
Total	<u>41</u>	<u>947</u>

Note 5: Financial assets

Note 5A: Cash

Cash at bank and on hand	<u>5 350</u>	<u>6 631</u>
All cash is recognised as a current asset		

Note 5B: Receivables

Goods and services	1 240	299
Less provision for doubtful debts	—	—
	<u>1 240</u>	<u>299</u>
GST receivable from the Australian Taxation Office	791	442
Total receivables (net)	<u>2 031</u>	<u>741</u>
All receivables are current assets		

	2003	2002
	\$ '000	\$ '000
Receivables (gross) are aged as follows:		
Not overdue	1 628	638
Overdue:		
– less than 30 days	194	84
– 30 to 60 days	35	3
– 60 to 90 days	146	1
– more than 90 days	28	15
	<u>2 031</u>	<u>741</u>

Note 6: Non-financial assets

Note 6A: Land and buildings

Freehold land—at 1999-2002 valuation	<u>944</u>	<u>944</u>
Buildings on freehold land—at 1999-02 valuation	1 441	1 441
Accumulated depreciation	<u>(576)</u>	<u>(521)</u>
	865	920
Leasehold improvements—at cost	4 200	1 982
Accumulated amortisation	<u>(396)</u>	<u>(86)</u>
	3 804	1 896
Leasehold improvements—at 1999-02 valuation	15 917	15 917
Accumulated amortisation	<u>(8 749)</u>	<u>(7 696)</u>
	<u>7 168</u>	<u>8 221</u>
<i>Total</i>	<u><u>12 781</u></u>	<u><u>11 981</u></u>

	2003 \$ '000	2002 \$ '000
Note 6B: Infrastructure, plant and equipment		
Plant and equipment—at cost	16 947	11 143
Accumulated depreciation	<u>(3 298)</u>	<u>(967)</u>
	13 649	10 176
Plant and equipment—at 1999-02 valuation	10 025	10 054
Accumulated depreciation	<u>(6 938)</u>	<u>(5 822)</u>
	3 087	4 232
Plant and equipment—at 2001-02 valuation	16 344	16 964
Accumulated depreciation	<u>(13 060)</u>	<u>(11 912)</u>
	3 284	5 052
<i>Total</i>	<u><u>20 020</u></u>	<u><u>19 460</u></u>
Note 6C: Intangibles		
Purchased computer software—at cost	7 714	6 639
Accumulated amortisation	<u>(5 083)</u>	<u>(4 420)</u>
	2 631	2 219
<i>Total</i>	<u><u>2 631</u></u>	<u><u>2 219</u></u>

Note 6D: 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 2002							
Gross book value	944	1 441	17 899	19 340	38 161	6 639	65 084
Accumulated depreciation/ amortisation	—	(521)	(7 782)	(8 303)	(18 702)	(4 419)	(31 424)
Net book value	944	920	10 117	11 037	19 460	2 219	33 660
Additions	—	—	2 218	2 218	6 993	1 572	10 783
Depreciation/ amortisation expense	—	(54)	(1 363)	(1 418)	(5 512)	(1 145)	(8 075)
Write-offs	—	—	—	—	(617)	(497)	(1 114)
Disposals	—	—	—	—	(1 221)	—	(1 221)
As at June 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

Table B — Assets at valuation

<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 30 June 2003							
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)
Net book value	944	865	7 168	8 033	6 371	—	15 348
As at 30 June 2002							
Gross value	944	1 441	15 917	17 358	27 019	—	45 320
Accumulated depreciation/ amortisation	—	(521)	(7 696)	(8 217)	(17 734)	—	(25 951)
Net book value	944	920	8 221	9 140	9 285	—	19 369

Table C — Assets held under finance lease

<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 30 June 2003							
Gross value	—	—	—	—	841	—	841
Accumulated depreciation/ amortisation	—	—	—	—	(410)	—	(410)
Net book value	—	—	—	—	431	—	431
As at 30 June 2002							
Gross value	—	—	—	—	841	—	841
Accumulated depreciation/ amortisation	—	—	—	—	(289)	—	(289)
Net book value	—	—	—	—	552	—	552

	2003 \$ '000	2002 \$ '000
--	-----------------	-----------------

Note 7: Other non-financial assets

Prepayments	628	377
	<hr/>	<hr/>

All other non-financial assets are current assets

Note 8: Interest bearing liabilities

Finance lease commitments		
Payable:		
within one year	242	240
in one to five years	121	364
	<hr/>	<hr/>
Minimum lease payments	363	604
Deduct: future finance charges	(32)	(71)
	<hr/>	<hr/>
<i>Lease liability</i>	<u>331</u>	<u>533</u>
	<hr/>	<hr/>
Lease liability is represented by:		
Current	216	202
Non-current	115	331
	<hr/>	<hr/>
<i>Net lease liability</i>	<u>331</u>	<u>533</u>
	<hr/>	<hr/>

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 9: Provisions

Note 9A: Capital Use Charge provision

Capital Use Charge	—	468
	<hr/>	<hr/>
Balance owing 1 July	468	—
Capital Use Charge provided for during the period	2 431	1 214
Capital Use Charge paid	(2 899)	(746)
	<hr/>	<hr/>
Balance owing 30 June	<u>—</u>	<u>468</u>
	<hr/>	<hr/>

The Capital Use Charge provision is a current liability

	2003	2002
	\$ '000	\$ '000
Note 9B: Accommodation Leases – make good provision		
Accommodation leases - make good	<u>1 032</u>	<u>—</u>
Note 9C: Employee provisions		
Salaries and wages	1 210	1 056
Leave	12 316	11 600
Superannuation	191	98
Other	64	314
<i>Aggregate employee benefit liability and related on-costs</i>	<u>13 781</u>	<u>13 068</u>
Current	6 706	5 663
Non-current	7 075	7 405

Note 10: Payables

Note 10A: Supplier payables

Trade creditors	<u>4 523</u>	<u>3 339</u>
All supplier payables are current liabilities		

Note 11: Equity

	<i>Accumulated results</i>		<i>Asset revaluation reserves</i>		<i>Contributed equity</i>		<i>Total equity</i>	
	2003 \$'000	2002 \$'000	2003 \$'000	2002 \$'000	2003 \$'000	2002 \$'000	2003 \$'000	2002 \$'000
Opening balance as at 1 July 2002	270	2 497	6 279	1 930	17 452	13 168	24 001	17 595
Net surplus/(deficit)	(2 038)	(682)			—	—	(2 038)	(682)
Net revaluation increments/decrements	—	—	—	4 349	—	—	—	4 349
Transaction with owner:								
Distributions to owner:								
Returns on Capital								
Capital use charge	(2 431)	(1 545)	—	—	—	—	(2 431)	(1 545)
Repayment of interest	(450)	—	—	—	—	—	(450)	—
Contributions by owner:								
Appropriations (equity injection)	—	—	—	—	4 692	4 284	4 692	4 284
Closing balance as at 30 June 2003	(4 649)	270	6 279	6 279	22 144	17 452	23 774	24 001

2003	2002
\$ '000	\$ '000

Note 12: 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	5 350	6 631
Statement of Financial Position items comprising above cash: 'Financial Asset — Cash'	5 350	6 631

Reconciliation of operating surplus (deficit) to net cash provided by operating activities:

Net surplus (deficit)	(2 038)	(682)
Depreciation/Amortisation	8 075	6 606
Net write down of non-financial assets	36	947
Net loss on disposal of assets	39	153
(Increase)/Decrease in receivables	(1 290)	1 296
(Increase)/Decrease in prepayments	(251)	442
Increase/(Decrease) in provisions	1 032	—
Increase/(Decrease) in employee provisions	713	339
Increase/(Decrease) in supplier payables	1 184	1 459
Provision for interest	(450)	—

<i>Net cash provided/(used) by operating activities</i>	<u>7 051</u>	<u>10 560</u>
---	--------------	---------------

Note 13: 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>\$ 51 000</u>
--	------------------	------------------

No other services were provided by the Auditor-General.

Note 14: Executive remuneration

The number of executive officers who received or were due to receive a total remuneration package of \$100 000 or more (including performance pay and separation and redundancy payments):

	2003 Number	2002 Number
\$100 000 to \$110 000	0	1
\$130 000 to \$140 000	0	3
\$140 000 to \$150 000	2	4
\$150 000 to \$160 000	1	1
\$160 000 to \$170 000	3	3
\$170 000 to \$180 000	3	0
\$180 000 to \$190 000	1	0
\$190 000 to \$200 000	2	0
\$200 000 to \$210 000	1	0
\$210 000 to \$220 000	1	1
\$260 000 to \$270 000	1	0
\$340 000 to \$350 000	0	1
\$370 000 to \$380 000	1	0

The remuneration referred to above is all remuneration received or receivable by executives and includes salaries, accrued annual and long service leave, performance pay, accrued superannuation, the cost of motor vehicles, allowances and applicable fringe benefits tax.

The aggregate amount of total remuneration of executive officers shown above.

<u>\$ 3 089 974</u>	<u>\$ 2 292 071</u>
---------------------	---------------------

Total remuneration includes:

The aggregate amount of performance pay paid during the year to executive officers shown above

<u>\$ 102 805</u>	<u>\$ 47 563</u>
-------------------	------------------

The aggregate amount of separation and redundancy payments made during the year to executive officers shown above

<u>\$ —</u>	<u>\$ —</u>
-------------	-------------

Note 15: Act of Grace payments, Waivers and Defective Administration Scheme payments

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*.

No payments were made during the reporting period under the Defective Administrative Scheme.

	2003 Number	2002 Number
Note 16: Average staffing levels		
Average staffing levels	<u>621</u>	<u>575</u>

Note 17: Appropriations

Note 17A: Appropriations Acts (No 1/3) 2002-2003

Particulars	Total
Year ended 30 June 2003	\$
Balance carried forward from previous year	6 631 308
Appropriation for reporting period (Act 1)	81 087 000
Appropriation for reporting period (Act 3)	4 588 000
GST refunds (FMA s30A)	3 712 425
Annotations to 'net appropriations' (FMA s37)	2 079 683
Available for payments	98 098 416
Payments made	91 956 660
<i>Balance carried to next year</i>	6 141 756
<i>Represented by:</i>	
Cash	5 350 305
GST receivable	791 451
Appropriations receivable	—
Total	6 141 756
Year ended 30 June 2002	
Total annual appropriations	64 996 000
Adjustments and annotations to appropriations	14 751 788
Available for payments 2002	79 747 788
Payments made 2002	73 116 480
<i>Balance carried forward to 1 July 2002</i>	6 631 308
<i>Represented by:</i>	
Cash	6 631 308
Appropriations receivable	—
Total	6 631 308

FMA = *Financial Management and Accountability Act 1997*

Act 1 = *Appropriations Act (No 1) 2002-2003*

Act 3 = *Appropriations Act (No 3) 2002-2003*

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 17B: Appropriations Acts (No 2/4) 2002-2003

Particulars	Departmental Capital			Total
	Equity \$	Loans \$	Carryovers \$	\$
Year ended 30 June 2003				
Balance carried from previous year	—	—	—	—
Current Appropriation (Act 2)	4 692 000	—	—	4 692 000
Available for payments	4 692 000	—	—	4 692 000
Payments made	4 692 000	—	—	4 692 000
<i>Balance carried to next year</i>	—	—	—	—
<i>Represented by:</i>				
Cash	—	—	—	—
Appropriations receivable	—	—	—	—
Year ended 30 June 2002				
Available for payments 2002	4 284 000	—	—	4 284 000
Payments made 2002	4 284 000	—	—	4 284 000
Balance carried forward to 1 July 2002	—	—	—	—
<i>Represented by:</i>				
Cash	—	—	—	—
Appropriations receivable	—	—	—	—

Note 18: Reporting of Outcomes

Note 18A: Total Cost/Contribution of Outcomes (Whole of Government)

	Total	
	2003 \$'000	2002 \$'000
Total expenses	90 983	75 597
Costs recovered from provision of good and services to the non-government sector	191	50
Other external revenues		
Interest on cash deposits	13	210
Revenue from disposal of assets	859	1 088
Other	723	1 084
Goods and services revenue from related entities	1 484	7 488
Net cost / (contribution) of outcome	87 713	65 678

Note 18B: Major Revenues and Expenses by Output Group

	Total	
	2003 \$'000	2002 \$'000
Operation revenues		
Revenues from government	86 237	65 682
Sale of goods and services	1 113	6 851
Other non-taxation revenues	1 596	1 294
Total operating revenues	88 945	73 827
Operating expenses		
Employees	48 660	41 959
Suppliers	33 271	24 844
Depreciation and amortisation	8 075	6 606
Other	940	1 100
Total operating expenses	90 945	74 509

Note 19: Financial Instruments

Note 19A: Terms, conditions and accounting policies

<i>Financial Instrument</i>	<i>Notes</i>	<i>Accounting policies and methods (including recognition criteria and measurement basis)</i>	<i>Nature of underlying instrument (including significant terms and conditions affecting the amount, timing and certainty of cash flows)</i>
Financial assets		Financial assets are recognised when control over future economic benefits is established and the amount of the benefit can be reliably measured.	
Cash	5A	Cash is recognised at nominal amounts. Interest is credited to revenue as it accrues	ASIO's investment funds are held within the Reserve Bank of Australia. Monies in ASIO's bank accounts are swept into the Official Public Account nightly and interest is earned on the daily balance at rates based on money market call rates. Rates have averaged 2.0% for the year. (2002: 3.0%)
Receivables for goods and services	5B	These receivables are recognised at the nominal amounts due less any provision for bad or doubtful debts. Collectability of debts is reviewed at balance date. Provisions are made when collection of the debt is judged to be less rather than more likely.	All receivables are with entities external to the Commonwealth. Credit terms are net 30 days (2001-02: 30 days)
Accrued revenue		Interest is credited to revenue as it accrues. Interest on ASIO's operating bank account is payable quarterly. Interest on fixed interest deposits is payable on maturity.	Interest: as for cash.
Financial liabilities		Financial liabilities are recognised when a present obligation to another party is entered into and the amount of the liability can be reliably measured.	
Trade creditors	10A	Creditors and accruals are recognised at their nominal amounts, at which the liabilities will be settled. Liabilities are recognised to the extent that the goods or services have been received (and irrespective of having been invoiced).	All creditors are entities that are not part of the Commonwealth legal entity. Settlement is usually made net 30 days.
Finance lease liabilities	8	Liabilities are recognised at the present value of the minimum lease payments at the beginning of the lease. The discount rates used are estimates of the interest rates implicit in the leases.	At reporting date, ASIO had one finance lease with a term of 5 years. The interest rate implicit in the lease is 7.08%. The lease assets secure the lease liabilities.

Note 19B: Interest rate risk

Financial Instrument	Notes	Floating Interest Rate		Fixed Interest Rate						Non-Interest Bearing		Total		Weighted Average Effective Interest Rate	
		2003 \$'000	2002 \$'000	1 year or less		1 to 5 years		> 5 years		2003 \$'000	2002 \$'000	2003 \$'000	2002 \$'000	2003 %	2002 %
Financial Assets															
Cash at bank	5A	5 350	6 631	—	—	—	—	—	—	—	—	5 350	6 631	2.0	3.0
Receivables for goods and services	5B	—	—	—	—	—	—	—	—	538	75	538	75	n/a	n/a
Total		5 350	6 631	—	—	—	—	—	—	538	75	5 888	6 706		
Total Assets												43 441	41 409		

Financial Liabilities	Notes	2003 \$'000	2002 \$'000	2003 \$'000	2002 \$'000	2003 \$'000	2002 \$'000	2003 \$'000	2002 \$'000	2003 \$'000	2002 \$'000	2003 %	2002 %		
Finance lease liabilities	8	—	—	216	202	115	331	—	—	—	—	7.08	7.08		
Trade creditors	10A	—	—	—	—	—	—	2 470	2 961	2 470	2 961	n/a	n/a		
Total		—	—	216	202	115	331	—	—	2 470	2 961				
Total liabilities												19 667	17 408		

Note 19C: Net fair values of financial assets and liabilities

	Note	2003		2002	
		Total carrying amount \$'000	Aggregate net fair value \$'000	Total carrying amount \$'000	Aggregate net fair value \$'000
Departmental Financial Assets					
Cash at bank	5A	5 350	5 350	6 631	6 631
Receivables for goods and services	5B	538	538	75	75
Total Financial Assets		<u>5 888</u>	<u>5 888</u>	<u>6 706</u>	<u>6 706</u>
Financial Liabilities (Recognised)					
Finance lease liabilities	8	331	331	533	533
Trade creditors	10A	2 470	2 470	2 961	2 961
Total Financial Liabilities (Recognised)		<u>2 801</u>	<u>2 801</u>	<u>3 494</u>	<u>3 494</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. (Where the liability is on a floating rate of interest, the method returns the principal amount).

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

Note 19D: 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 20: Assets held in trust

Comcare Trust Account

During 2002-2003 compensation payments made by Comcare amounted to \$60 234. This represented reimbursement of expenses previously paid by ASIO to staff and health care professionals.

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 2003 and 30 June 2002, 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*.

Part 5

Appendixes



Appendix A

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

Membership of the PJC 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 Paul Calvert (discharged on 29 August 2002)	(LP, TAS)
Senator Alan Ferguson (appointed on 29 August 2002)	(LP, SA)

Appendix C

Staffing statistics

Table A. Staffing levels and number at 30 June, 1998-99 to 2002-03

	98-99	99-00	00-01	01-02	02-03
Average staffing level (ASL) for each financial year (FY)	513	538	560	575	621
Full time staff equivalent (FSE) at end of each FY	525	565	551	597	637
Number of staff at the end of each FY	566	605	584	618	668

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

	98-99	99-00	00-01	01-02	02-03
Permanent full-time	473	469	453	497	536
Temporary full-time	30	77	63	58	51
Permanent part-time	22	20	26	25	28
Temporary part-time	6	10	14	18	23
Casual	21	22	25	19	30
Non-operational (including unattached and on compensation)	14	7	3	1	—
Total	566	604	584	618	668

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

		98-99	99-00	00-01	01-02	02-03
Band 1	Female	1	1	1	2	2
	Male	9	9	9	8	9
Band 2	Female	1	1	1	1	1
	Male	2	2	2	2	4
Band 3	Male	1	1	1	1	1
Total		14	14	14	14	17

Note — Figures do not include the Director General.

Appendix D

Workplace diversity statistics

Table A. Representation of designated groups within ASIO at 30 June 2003

Group	Total staff ¹	Women ²	Race/ Ethnicity	ATSI	PWD	Staff with EEO data ²
SES	18	3	0	0	0	14
Senior Officers ³	121	28	5	0	2	94
AO5 ⁴	280	111	33	1	5	182
AO1-4 ⁵	216	129	8	2	10	100
ITO1-2 ⁶	33	9	3	0	0	13
ENG1-2 ⁷	0	0	0	0	0	0
TOTAL	668	280	49	3	17	403

¹ Based on staff salary classifications recorded in CHRIS, ASIO's computerised personnel system.

² Provision of EEO data by staff is voluntary.

³ The Senior Officer group are the equivalent to the APS EO1 to EO2 classifications and includes equivalent officers in the Engineer and Information Technology classifications.

⁴ The AO5 (ASIO Officer Grade 5) group is equivalent to APS Level 6 and includes ASIO Generalist Intelligence Officers.

⁵ 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).

⁶ Information Technology Officers grades 1 and 2.

⁷ Engineers Grades 1 and 2.

Table B. Percentage representation of designated groups in ASIO 1999-2003

Group	June 1999	June 2000	June 2001	June 2002	June 2003
Women ¹	38	40	40	40	42
Race / Ethnicity ²	8	8	6	11	12
ATSI ³	0.4	0.4	0.3	0.75	0.74
PWD ⁴	4	4	3	4	4

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 2003

ASIO MANAGERS

SES Band 3	\$147 742		minimum point
SES Band 2	\$116 776		minimum point
SES Band 1	\$97 943		minimum point
AEO 3	\$86 805		
AEO 2	\$78 748	to	\$86 805
AEO 1	\$69 438	to	\$74 953

GENERALIST INTELLIGENCE OFFICERS

GIO	\$39 104	to	\$60 478
-----	----------	----	----------

ASIO OFFICERS

ASIO Officer 5	\$53 021	to	\$60 478
ASIO Officer 4	\$43 730	to	\$47 735
ASIO Officer 3	\$38 134	to	\$41 090
ASIO Officer 2	\$22 582	to	\$37 147
ASIO Officer 1	\$29 765	to	\$32 812

ASIO ITOs

SITOA	\$86 805		
SITOB	\$78 748	to	\$86 805
SITOC	\$69 438	to	\$74 953
ITO2	\$53 021	to	\$60 478
ITO1	\$41 090	to	\$47 735

ASIO ENGINEERS

SIO(E)5	\$88 184		
SIO(E)4	\$78 748	to	\$86 805
SIO(E)3	\$69 438	to	\$74 953
SIO(E)2	\$53 021	to	\$60 478
SIO(E)1	\$41 090	to	\$47 735

Appendix F

Assumed identities

Commonwealth Legislation

Part 1AC of the Commonwealth *Crimes Act 1914* entered into force on 12 October 2001. This legislation establishes a Commonwealth scheme for the acquisition and use of assumed identities by members of intelligence and law enforcement agencies. ASIO is a participating agency under the legislation. During 2002-03 ASIO issued 3 authorisations under the legislation, none of which were varied and none were revoked. The activities undertaken by approved officers and approved persons when using their assumed identities during the year concerned intelligence officer duties. The first authorisations under the Commonwealth scheme were issued in June 2003. Accordingly, there was no audit conducted of records of authorisations under the Commonwealth scheme during 2002-03.

New South Wales Legislation

During the year 40 assumed identity approvals were granted in accordance with the NSW *Law Enforcement and National Security (Assumed Identities) Act 1998*. No approvals were varied and none were revoked.

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

- surveillance duties
- intelligence officer duties, and
- support officer duties.

The most recent audit required in accordance with Section 11 of the Act was conducted in August 2002 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
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
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 & Indigenous Affairs
DIO	Defence Intelligence Organisation
DOTARS	Department of Transport and Regional Services
DSD	Defence Signals Directorate
EMA	Emergency Management Australia
IASF	Inter-Agency Security Forum
IGIS	Inspector-General of Intelligence and Security
JCTICU	Joint Counter-Terrorism Intelligence Coordination Unit
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	Operation Response Exercise
PJC	Parliamentary Joint Committee on ASIO, ASIS and DSD
PM&C	Department of 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
TSCM	Technical surveillance counter-measures
TSU	Technical Surveillance Unit
WMD	Weapons of mass destruction

Compliance index

Annual Report requirement	Page
Assumed identities	108
Advertising and market research	54
Certified agreements and AWAs	53
Consultants and contractors	62
Contact details	104
Corporate governance	47-48
Disability strategy	56-57
Environmental performance	61
External scrutiny	49-51
Financial performance	11, 65-100
Financial statements	65-100
Fraud Control measures	48
Freedom of Information	25
Glossary	109
Index	111
Internet home page address and Internet address for report	104
Letter of transmittal	iii
Management of human resources	52-56
Occupational health and safety	57
Organisational structure	6
Outcome and Output structure	7-8
Overview of agency	6
Performance pay	54
Purchasing	61
Report on performance	11-43
Resource tables by outcomes	11
Review by Director-General	3-5
Roles and functions	6-8
Staffing statistics	105-106
Summary resource table	11
Table of contents	v
Workplace agreements	53

General index

A

AAT (Administrative Appeals Tribunal), 27, 30, 32
Abu Sayyaf Group, 18
accountability, ix, 4-5, 27, 29, 35, 36, 38, 48-51
advertising costs, 54
al-Qaida, 3, 13, 14, 16-17, 18, 22, 42
Annual Report, ix, 47
anthrax, 19
archival records, access to, 25-27
Archives Act 1983, 25, 49
ASIO Act 1979, ix, 40, 49
ASIO Legislation Amendment (Terrorism) Act 2002, 5, 35-36
ASIO Now, 52
ASIO ombudsman, 57
ASIO staff. *See* staff
assumed identities, 48, 108
Attorney-General, accountability to, ix, 38, 47, 49
audio counter-measures. *See* technical surveillance counter-measures
audit and evaluation, 48, 60, 108
Auditor-General, ix
AUSTRAC, 18
Australian agencies, liaison with. *See* liaison with
Australian Federal Police, liaison with. *See* liaison with Australian agencies – Australian Federal Police
Australian National Audit Office, 47
aviation security, 19
Aviation Security Identification Card, 5, 11, 30, 58

B

Bali bombings and investigation, 3, 4, 13-15, 23, 24, 40, 41
Bali inquiry, 5
– Senate, 5, 51
– Inspector-General of Intelligence and Security, 5, 50
biological warfare. *See* WMD
border control. *See* visa checking

Budget,
– *2002-03*, 11, 21, 40
– *2003-04*, 11, 21
budget oversight, 49
building management, 60
business re-engineering, 32

C

capabilities. *See* investment in capabilities
CBRN (chemical, biological, radiological or nuclear) threats. *See* WMD
Charter of the United Nations (Anti-Terrorism Measures) Regulations 2001, 18
Charter of the United Nations (Terrorism and Dealing with Assets) Regulations 2002, 18
chemical, biological, radiological or nuclear threat. *See* WMD
client survey, 12, 13, 19, 23
Commonwealth Counter-Terrorism Committee, 36
communications. *See* information management
compensation claims, 57
complaints about ASIO, 49, 51
compliance index, 110
computer attack. *See* critical infrastructure protection
consultants and contractors, 62
contact information, 102
Contact Reporting Scheme, 31
controversial visitors. *See* visa checking - recommendations against entry
corporate governance, 47-48
Corporate Plan 2002-2006, ix, 47-48
cost recovery, 31
counter-espionage, 29-30
counter-intelligence. *See* security of ASIO
counter-proliferation. *See* CBRN
counter-terrorism capability, 5, 11, 35, 36-37
counter-terrorism exercises, 37, 55
Counter-Terrorist Overseas Response Group. *See* CTORG
Crimes Act 1914, 28, 108
Crimes (Internationally Protected Persons) Act 1976, 16

General index (continued)

Criminal Code Amendment (Espionage and Related Offences) Act 2002, 36

Criminal Code Amendment (Hizballah) Act 2003, 18

Critical Infrastructure Protection, 4, 21

CTORG, 37

D

Defence Signals Directorate (DSD), 21, 33, 41

Department of Defence, 19, 28

Department of Foreign Affairs & Trade, 18, 22, 28, 37

Department of Immigration & Multicultural and Indigenous Affairs, 14, 15, 24, 25, 28

Department of Prime Minister and Cabinet, 28

Department of Transport and Regional Services, 19

disability strategy, 56-57

Dowling, Sherryl, 28

E

ecologically sustainable development, 61

EEO. *See* workplace diversity

electronic and audio counter-measures. *See* technical surveillance counter-measures

Emergency Management Australia (EMA), 19, 21

engineering development. *See* technical development

entry and search of premises, 3, 15-16, 41

entry to Australia, controls on. *See* visa checking

environmental performance, 61

equal employment opportunity. *See* workplace diversity

equipment testing. *See* security equipment testing and standards

e-security. *See* critical infrastructure Protection

espionage, 20, 36

evaluation. *See* audit and evaluation

external scrutiny. *See* accountability

F

financial investigations, 18

financial performance, 65-100

financial statements, 65-100

foreign intelligence collection, ix, 8, 43

foreign interference, 20

foreign liaison. *See* liaison with overseas services

fraud control, 48

Freedom of Information Act 1982, 25

G

'Gatekeeper' accreditation, 32

glossary, 109

Government/Business Taskforce on Critical Infrastructure, 21

Guidelines for the Collection of Intelligence, 35, 49

H

Habib, Mamdouh, 17

Hamas, 18

Hicks, David, 17

Hizballah, 18

human resource management. *See* staff

human source intelligence, 35, 39

I

illegal arrivals. *See* visa checking – unauthorised arrivals

industrial democracy. *See* workplace relations

industry, engagement with, 21, 38-39

information management, 48, 55, 57-58, 60

infrastructure. *See* critical infrastructure protection

Inquiry into the performance of the Department of Foreign Affairs and other relevant agencies of the Commonwealth Government in the assessment and dissemination of threats to the security of Australians in Southeast Asia in the period 11 September 2001 to 12 October 2000. *See* Bali Inquiry - Senate

General index (continued)

Inquiry into Security Issues, 28, 30, 59, 60
Inspector-General of Intelligence and Security, 5, 26, 28, 38, 48, 49, 51
– Annual Report, 38, 50
– Bali inquiry, 5, 50
– See also Inquiry into Security Issues
Inter-Agency Security Forum, 28, 59
internal security. See security of ASIO
intrusive methods of investigation. See warrant operations
investigative priorities, 3, 13
investment in capability, 4, 5, 11
Iraq, war in, 3, 19, 13, 16-17
Islamic community, attacks on, 4, 20
Islamic extremism, 3, 5, 13, 13-17

J

Jemaah Islamiyah, 3, 13-16, 18, 41, 42
– Bali bombings, 3, 4, 13-15, 23, 24, 40, 41
– Search operations, 3, 15-15
Jewish community, attacks on, 4, 20
Joint Counter-Terrorism Intelligence Coordination Unit (JCTICU), 41
Joint Standing Committee on Foreign Affairs, Defence and Trade, 51

L

Lappas, Simon, 28
Leader of the Opposition, ix, 49
legislation (Commonwealth)
– *Archives Act 1983*, 25, 49
– *ASIO Act 1979*, 40, 49
– *ASIO Legislation Amendment (Terrorism) Act 2002*, 5, 35-36
– *Charter of the United Nations (Anti-Terrorism Measures) Regulations 2001*, 18
– *Charter of the United Nations (Terrorism and Dealing with Assests) Regulations 2002*, 18
– *Crimes Act 1914*, 28, 108
– *Crimes (Internationally Protected Persons) Act 1976*, 16
– *Criminal Code Amendment (Espionage and Related Offences) Act 2002*, 36
– *Criminal Code Amendment (Hizballah) Act 2003*, 18
– *Freedom of Information Act 1982*,

– *Telecommunications Act 1977*, 38
legislation (NSW)
– *Law Enforcement and National Security (Assumed Identities) Act 1998*, 48, 108
liaison with Australian agencies, 11, 35, 40-41
– Australian Federal Police, 3, 14, 15, 17, 40-41, 42
– Other Commonwealth agencies, 14, 19, 24, 25, 28, 40, 41, 42
– State/territory police, 15, 40-41
liaison with overseas agencies, 4, 5, 11, 16, 35, 42
– approved agencies, 42
Liberation Tigers of Tamil Eelam. See LTTE
locksmith accreditation, 32
LTTE, 18

M

management and accountability, 47-51
management restructure, 4, 6, 53
management structure chart, 6
media policy, 52

N

National Anti-Terrorist Plan (NATP), 37
National Archives of Australia, 25
National Counter-Terrorism Committee, 11, 22, 36
National Counter-Terrorist Plan, 21, 37
National Information Infrastructure Protection. See critical infrastructure protection.
National Intelligence Group (NIG), 37
National Security Committee of Cabinet, ix, 47
National Security Hotline, 3, 40, 41

O

occupational health and safety, 57
– compensation claims, 57
Olympic Games
– Athens 2004 Games, 4, 42
open source information, 35, 40

General index (continued)

organisational structure chart. *See*
management structure chart
Osama bin Laden. *See* al-Qaida
outcomes, 7, 12, 35
output performance, 11-44
outputs, 7, 8, 11, 28
– enabling, 8
– foreign intelligence, 8, 43
– protective security advice, 7, 28-34
– security intelligence analysis & advice, 7,
11-27
– security intelligence investigation &
capability, 7, 35-42

P

Parliamentary committees, 4-5, 50-51
Parliamentary Joint Committee on ASIO,
ASIS and DSD (*formerly Parliamentary
Joint Committee on ASIO*), ix, 4, 36, 50, 103
people management. *See* staff
performance pay, 54
performance reporting, 11-43
personnel security assessments, 4, 29-30,
59
– adverse and qualified assessments, 4, 30
– appeals, 29
– vetting for AIC, 30
physical security, 31-34, 60
– cost recovery, 31
PMV. *See* politically motivated violence
police, liaison with. *See* liaison with
Australian agencies
politically motivated violence
– foreign influenced, 13-19
– local, 19
– Bali attacks, 3, 4, 13-15, 23, 24, 40, 41
– 11 September, 13, 40
polygraph trial, 4, 30
proscribed organisations, 15, 18
proliferation. *See* CBRN
protective security advice, 4, 28-34
protective security training, 33
Protective Security Coordination Centre.
See PSCC
Protective Security Manual, 59
Protective Security Policy Committee, 28,
33
protective security risk reviews. *See*
physical security

protest activity, violent. *See* politically
motivated violence - local
PSCC, 21
public, ASIO contact with, 51-52
purchasing, 61

R

recruitment. *See* staff recruitment
Research and Monitoring Unit, 40
risk management advice, 32-33
Roche, Jack, 16

S

SAC-PAV, 22, 36
salary classification structure, 107
searches. *See* entry and search of premises
Secretaries' Committee on National Security,
ix
security of ASIO, 58-60
security assessments,
– illegal arrivals. *See* visa checking
– personnel. *See* personnel security
assessments
– visa checking. *See* visa checking
security clearances. *See* personnel security
assessments and staff security clearances
Security Construction and Equipment
Committee, 32, 33
Security Equipment Catalogue, 33
security equipment testing and standards,
34
security intelligence analysis and advice, 7,
11-27
security intelligence investigation and
capability, 7, 35-42
Security Intelligence Reports, 19, 21
security, internal. *See* security of ASIO
Security Management Plan 2001-2004, 59
Senate Legal and Constitutional Legislation
Committee, 5, 49, 51
separations. *See* staff separations
September 11 attacks. *See* politically
motivated violence - 11 September
SIDC-PAV, 36
special powers. *See* warrant operations
staff:
– people management, 5, 52-53
– Performance Management Framework, 53

General index (continued)

- performance pay, 54
 - salary classification structure, 107
 - Staff Association, 47, 50
 - staff recruitment, 5, 54
 - staff security clearances, 59
 - staff separations, 5, 54
 - staff training and development, 4, 53-56
 - staffing profile, 54, 105-106
 - staffing statistics, 53, 105-106
 - workplace diversity, 56, 105-106
 - workplace relations, 53
- Sultan, Mohamad, 17
- surveillance, 35, 39
- sweeps. *See* technical surveillance counter-measures

T

- Tamil extremism. *See* LTTE
- technical development, 5, 11, 35, 39, 42, 55
- Technical Support Unit, 37
- technical surveillance counter-measures, 4, 31, 34
- Telecommunications Act 1977*, 38
- telecommunications environment, 39
- telecommunications interception, 38-39
- terrorism. *See* politically motivated violence
- terrorist finances. *See* financial investigations
- terrorist groups, proscription of. *See* proscribed organisations.
- Thomas, Jack, 17
- threat assessments, 3, 4, 12, 20, 21, 22-23
- threat levels, 3, 12, 15, 22
- Top Secret certification, 33
- training and development. *See* staff - training and development
- travel advisories, 22

U

- UBL. *See* Usama bin Laden
- unauthorised arrivals. *See* visa checking
- Usama bin Laden. *See* al-Qaida

V

- vetting. *See* personnel security assessment
- violent protest activity. *See* politically motivated violence - Local
- visa checking, 4, 14, 24-25
- recommendations against entry, 4, 24
 - unauthorised arrivals, 25

W

- warrant operations, 35, 38
- approvals, 49
 - entry and search, 3, 15-16, 41
 - telecommunications interception, 38-39
- weapons of mass destruction. *See* WMD
- website, 48, 51-52, 105
- Wispelaere, Jean-Philippe, 36
- WMD, 19
- women in ASIO, 56, 106
- Workplace Agreement, 5, 53
- workplace diversity, 56
- workplace relations, 53

